PROCEEDINGS

OF

MAY 2021

Copyright Page

Table of Contents

Artificial Intelligence Autonomous Unmanned Aerial Vehicle (UAV) System for Remote Sensing in Security Surveillance

Ugochukwu O. Matthew
Dept. of Computer Science
Hussaini Adamu Federal Polytechnic
Kazaure, Nigeria
macdon4ru2003@yahoo.com

Jazuli S. Kazaure
Dept. of Electrical Electronics Engineering
Hussaini Adamu Federal Polytechnic
Kazaure, Nigeria
sakjazuli@gmail.com

Amaonwu Onyebuchi
Dept. of Computer Science
Hussaini Adamu Federal Polytechnic
Kazaure, Nigeria
sirlaw84@yahoo.com

Ogobuchi Okey Daniel
Dept. of Computer Engineering
Michael Okpara University of Agriculture
Umudike, Nigeria
okey.ogobuchi@mouau.edu.ng

Ibrahim Hassan Muhammed
Dept. of Computer Science
Hussaini Adamu Federal Polytechnic
Kazaure, Nigeria
ibrahimhass003@gmail.com

Nwamaka U. Okafor
School of Electrical and Electronic
University College Dublin Ireland.
Ireland
nwamaka.okafor@ucdconnect.ie

***Abstract*- Adapting artificial intelligence autonomous systems required a policy specification, policy enforcement and policy management on the key prioritized functions based on the inherent policy enforcement and self-definitive programmed knowledge by an autonomous system. In the current research, attempt was made to model an autonomous unmanned aerial vehicle (UAV) system to be able to detect humans within the thickest forest region amidst the escalating tension of bokoharam and bandits abductions within the Nigeria geographic space. The autonomous artificial intelligence UAVs was designed using laser-range detectors for location evaluation and pathway finding with very accurate precision. While the UAVs hovers in the neighborhood, it establishes an individualized 3-D map of its surrounding. The central objective of this study is to explore the scientific opportunities available for artificial intelligence unmanned aerial vehicle (Drones) modeled with machine learning (convolution neural network) on Internet of Things (IoTs) framework and adapt it to revolutionize the mission on environmental & remote sensing, security surveillance, rescue and search mission. The paper established that Nigeria security forces could adopt artificial intelligence UAV to extradite terrorists within the Lake Chad Basin where bokoharam insurgency and banditry are prevalent. The paper further highlight that UAV could be very instrumental in search and rescue mission by the security forces.**

Keywords: Artificial Intelligence, Machine Learning, Robots, Cloud Computing, Unmanned Aerial Vehicles, Internet of Thing, Autonomous System, Drones Technology

I. INTRODUCTION

In the current research, focus was directed in pursuing the vision for autonomous system management, which we viewed as being capable of societal advancement for self-governance, behavioral adaptation within the context of remote sensing and ecological surveillance that the system as a whole seek to deliver. Autonomous system generally is a form of technological advancement in which processes and procedures are performed with minimal human superintendence with negligible attendant human cost[4]. This philosophy is evidently clear in flying autonomous Drones beyond visually line of sight (BVLOS) and making sure that they succeed in the mission upon which they are assigned. To that effect, the current paper x-rayed the ongoing security challenges in the Nigerian states as the situation keep worsening, rising to an occasion of incredible dimension which had portrayed Nigeria to a likely failed state. Such insecurity challenges had presented a precarious circumstances to the national stability , therefore the authors comprehended the urgency for the adoption of artificial intelligence(AI) autonomous unmanned aerial vehicles (UAVs) or Drones system for applicable territorial surveillance, environmental monitoring and intelligence gathering for national security sustainability[5]. The continuous attacks and killings of innocent Nigerians have become an enormous task to manage by the Nigeria security forces, in that regard, the adoption of UAVs for security surveillance, ecological monitoring and intelligence gathering will provide a cost-effective approach to manage the ongoing security development. The paradigm shift will require UAVs known as Drones system, a remotely piloted vehicles (RPVs) which are small aircraft that have the potential to fly without an onboard human operative on assigned security mission beyond line of sight [6]. In that perspective, the AI autonomous UAVs modeled with convolution neural machine learning algorithm equipped with infrared cameras, sensors, communication system or other payloads will enable them sense, gather information, attack on target and avoid obstacles while on security mission. The UAVs utilization within the context of military intelligence have been acknowledged as the most effective approach to territorial surveillance, aerial intelligence gathering and security monitoring from the global military dimension[7].

The current paper reviewed the trends in the adoption of UAVs in security operations through it application in aerial surveillance from the global perspective and narrowed discussions to its potential integration within the Nigeria geographic space where susceptibility of security breaches have taken a different dimension. The research proved that UAVs could become an effective security paraphernalia for aerial surveillance, ecological monitoring, location mapping and intelligence gathering in Nigeria security engagement. While the degree of isolated killings, crimes, kidnappings, armed banditry, suicide bombings, religious motivated manslaughters, ethnic conflicts amongst others have progressively increased substantially, this phenomenon had posed dangerous precedence in the Nigeria national security[8]. However, there has never been convincing support for multi-stakeholder engagement on the Nigeria security matters except for the commander in chief of armed forces concentration on the military foot soldiers with few outdated

war planes that lacks coordinated cognizance in combating a hydra headed monsters that sprouted up in the recent time. The circumstances may not be unrelated with the emerging ethnic conquest, involving herdsmen and indigenous populace , religious bigotry, political competitiveness and a large restive citizens of the country who have perceived marginalization and political subjugation[5]. For that reason, Nigeria security forces should endeavor to strengthen the capacity for the Nigerian government in the direction of promoting its overall concentrations in containing internal and external aggressions, fight crimes, advance growth and development while improving the well-being of the citizenry which is the fundamental objectives of every responsive government[9].

II. AIMS & OBJECTIVES OF THE STUDY

The central objective of this study is to explore the scientific opportunities available for artificial intelligence unmanned aerial vehicle (Drones) modeled with machine learning (convolution neural network) on Internet of Things (IoTs) framework and adapt it to revolutionize the mission on environmental & remote sensing, security surveillance, rescue and search mission for the next generation smart and autonomous computing requiring images and videos processing, analysis, observation and law enforcement. Ultimately, these images and video transmission are essentially important for further processing to establish evidence on issues involving security observation, predatory mission and environmental monitoring. The digital paradigm captured in the entire research paper had already started taking effect in the present-day society as we look forward for more robust and advanced computing using unmanned aerial vehicles (Drones) and IoTs technologies. Among the objectives of the current paper include:

A. To provide theoretical and conceptual interpretation of invisible knowledge and logic behind the modelling of an autonomous system, its behavior, characteristics and future development in security implementation.

B. To increase the ability for modeling autonomous system to succeed on predicted and unpredicted circumstances in the event of ecological sensing, security surveillances, emergency assignment, search and rescue operations.

C. To comprehensively supervise and monitor the environmental ecosystem and validly report observations requiring immediate attention for security reason and for law enforcement by the agents of the state security service.

D. To effectively deploy a systematic surveillance device to monitor and report occurrences that might require immediate deployment based on security intelligence.

E. Crime watch and law enforcement utilization to identifying, tagging and monitoring the movement of the bandits, terrorists, robbers and tracing them to their hideout.

III. LITERATURE REVIEW

Prioritizing the security of life and properties are among the fundamental responsibilities of any responsive government to its citizens[10]. The government and the security forces represent the mechanism and machineries that governs any given state and possessed the resources to guarantee security and safety of the society from collapsing into mobocracy[11]. In that regard, security is viewed as a socio-economic dynamic that encompass the capability of a state to neutralize terrorizations and any form of intimidations arising from non interest state actor. According to Abiodun 2020, security is usually comprehended as a condition of being safe, protected and preserved of principal values and nonattendance of coercions to the extent of people values [5]. Whereas the security of a nation depends upon the protection and maintenance of the socio-economic order in the expressions of internal and external aggressions, the promotion of selected international order will moderate the risks on the fundamental values and interest of the domestic affairs which implies that security is a universal phenomenon [12]. Approaching a nation's security from a broader perspectives, it has connotation with freedom from vulnerability, including terrorizations to the nation's capacity to defend and enhance itself, promote its appreciated values and justifiable significances. According to Otieno 2019, security was viewed as the foremost human yearning because the extent of its absence renders the general public ineffective in all consciousness [13].

Contrastingly, approaching insecurity from the same direction, it portrayed the absence of security mechanism for the state governance. Insecurity connote the state of anarchy which lacks the effective control and machineries to take self-protective actions in contradiction to influences that signified detriments or dangers to an individual, community of people and the entire nation[14]. The concept of insecurity cut across every sphere of human endeavors as the state of apprehension, terror or fretfulness from agents operating within the state but does not represent the interest of the state. The phenomenon suggested physical insecurity which is the most observable form of terrorizations, fueling into countless appearances of other uncertainty such as economic trepidation and social anxiety[15]. The spate of killing in Nigeria not only constitute infringement on the fundamental human rights but it also violated the God's commandment, "Thou shall not kill". Usually, individuals are not permitted to slaughter human beings but in the absence of well-organized security architectures and a responsive government in place, religious killings, politically motivated killings and unnecessary conquest could spring up leading to loss of human lives[16]. In the recent time, the rate of kidnapping, armed robbery attacks, Fulani herdsmen killings and bokoharam bombing are on increase. In the current research, the insecurity in Nigeria was viewed as a situation where regional and national security architecture were compromised or hindered by external or internal influences based on the consequences of weak or poor economic

policy, ineffective human developmental strategy and military incapacitation. In an attempt to proffer meaningful solution to the menace, the current paper focused on the military synergy through modelling an artificial intelligence autonomous UAVs to substitute and leverage the power and proficiencies of the disruptive technologies for process modernism.

The UAVs or Drones are systems of interconnected devices carrying various degrees of sensors, infrared cameras fully autonomous and connected to the Internet, providing a perspective awareness from the air that is beyond visually line of sight [17]. The UAV device is empowered with the potential to gather a sizeable terabyte of multimedia data (information) per Drone on every transmission through the cloud infrastructure. The involvement of AI and machine learning, specifically the Convolutional Neural Networks (CNNs) in the absolute senses, represent an innovative approach to adaptive augmented reality in image & video processing for smartest autonomous Drone systems establishing a link between general feedforward neural networks and adaptive filters. Usually, two-dimensional Convolution Neural Networks are produced by one or more layers of two-dimensional filters, with the activities of the Non-linear Activation functions. The activation function employed for this purpose is usually the Rectifier Linear Unit (RELU). This is supported by supplementary convolutions such as pooling layers, completely bonded layers and regularization layers (Concealed layers) for the reason that their inputs and outputs are hidden by the activation function and conclusive convolutions[18]. The Convolutional Neural Network error minimization methods may be used to optimize Convolutional Networks optimization performances in order to implement quite powerful augmented reality (AR) for image & video processing[19]. This current research presented a description of the CNN implementation with AI autonomous sensing Drones for special visual specifications and real application to a practical image & video processing for advance mission specification beyond visually line of sight (BVLOS) on cloud infrastructure and Internet of Things (IoTs) for the autonomous smartest robots. On the merit, the research proved that Drone services could be deployed to the disaster-prone areas and images and telemetry data observed from the Drone transmission could be used to establish real estimate of events which will necessitate actions by the relevant authorities of the government. Future implementation is expected to serve the needs of governments and enterprise customers to ensure reliable real-time transmission of telemetry data, control commands, and high-definition video during flight operation.

IV. ARTIFICIAL INTELLIGENCE AUTONOMOUS UNMANNED AERIAL VEHICLES (DRONES)

The AI is a scientific evolution usually from the field of computer science, electrical & electronic engineering and mechatronics that require adaptations and programming super intelligent humans into electro-mechanical devices to work, act, behave and react like human beings under any circumstance. Scientifically speaking, AI simply implies super intelligent human in machine form without blood circulation, on the account that all the activities naturally provided and performed by biological humans are programmable into machine. On the basis of human activities, artificial intelligent systems are designed to perform some categorized functions such as:

- Speech processing and voice recognition
- Learning and Responses
- Planning, organizing and responding pre-emptively
- Problem Solving
- Behavioral modification, self-awareness, self-defense, self-understanding and self-consciousness.

In academics, researchers associated with AI are highly innovative, intriguing and technically specialized to offer solution to some difficult aspect of digital and scientific world. Among the most intriguing and innovative aspect of AI study include programming computers for certain human behavioral traits such as: knowledgeability, cognitive reasoning, problem solving, perception, learning, planning, ability to manipulate and move objects and enforcement of the sixth sense's ability. From all known indexes, knowledge engineering is a core and essential aspect of artificial intelligence research initiative[20]. Machines modelled with AI will always behave and perform as if they are humans provided, they have sufficient details regarding the exact world situation. Artificial Intelligence agent should have admittance to the generalization of knowledge engineering inherent in them to enable them to perform autonomously. However, initiating and programming general knowledge, cognitive ability, problem-solving and computational competence into the machines are usually problematic and wearisome task. Naturally, to effect Machine Learning without any kind of supervision requires the ability to identify patterns in streams of inputs (Data Set), while Machine Learning with adequate and comprehensive supervision involves classification and numerical regressions details[21]. The machine perception deals with the capability to use sensory inputs to deduce the different aspects of the real or imaginative world, whereas the computer vision is the power to analyze visual inputs like facial, object and gesture recognition, essentially required to expedite actions by AI modelled device[22].

Robotics are also another major aspect and field of scientific study revolving around artificial intelligence modelling. Robots are intelligent machines, possessing varied degree of inherent knowledge and intelligence to be able to handle tasks such as object manipulation, body adjustments, policy enforcement and navigation along with sub-problems of localization, adaptation, motion planning and environmental mapping. For clarity of purpose and to

effectively understand the slight variation in artificial intelligence, it may be equally essential to clearly understand the differences that exist between an Automated Systems (**ACs**) and an Autonomous Systems (**ACs***). An Automated system is one in which a computer reasons by the Control Logic Block from programming construct **"If–Then–Else"** rule, based on a top-level structure that are deterministic and routinely executable, which implies that for every input selection, the system output will always be relatively the same, except if something else occurred. On the other hand, an Autonomous System is extensively built on artificial intelligence to adapt and reasons probabilistically given a set of sensor inputs, implying that it makes predictions on the best possible course of actions and alternative possibilities obtained from sensor data input[23]. However, when comparing the Automated Systems when given the same input under the same condition , Autonomous Systems will not necessarily produce the exact response every time, rather such systems will produce a range of activities and behaviors[24]. Naturally, human intelligence collectively followed a pattern regarded as Perception–Cognition–Action information processing loop, in which individuals perceive something in the world around them, think about what to do, and then, once they have weighed up the options, make a decision to act through application of the cognitive senses[25]. The Artificial Intelligence is programmed into an Autonomous System to enable them to do something similar to humans, which implies that a computer absorbs and senses the world around them, and then processes the incoming information through optimization and verification algorithms with a choice of action made in a fashion similar to that of humans coordinated activities. The best approach in measuring the behavior of an Autonomous System is to enable modern artificial intelligence programmed exchanges for processing systems to coordinate each individualized attribute in the absence of human instructive interferences and superintendence. The Autonomous Processing Inventiveness (API) was developed to provide the foundation for autonomous computing paradigm so to enable systems to be programmed and modelled with AI to carry out action without human involvement[26].This is certainly true on the premise that operating UAV system beyond visually line of sight (BVLOS) required that such device should act autonomously based on the informed decision and programmed knowledge to accomplish in the mission assigned to it. This form of computing is inspired by the autonomic flight synchronization through the Internet of Things (IoTs) cloud infrastructure, permitting several unmanned aerial vehicles system to share data and communicate to each other about the situation of the operating environments.

The modus operandi and the building blocks for every autonomous system is on the peculiarity of sensing potentiality (***Sensors S_i*),** hopefully empowers the system to perceive its outward operating environment and actively coordinate the internal operating environments through the information available from the sensing device. The intrinsic abilities of the autonomous system is dependent on the knowledge of the objective (Goal) and the technicalities of self-operation with configurable knowledge and understanding of sensory data, etc., without outward participation in enabling the autonomous system identify objects, avoid collision, consider the alternative course of actions, attack on target and identify safe landing space. However, the authentic actions of the autonomous system are determined by the Logic that is accountable for the autonomous system to accomplish the rightful assessments in serving its purpose and inspiring every possible surveillance of the remote operating environments with respect to sensor data. The approach underscores the actuality that every task of an autonomous system especially the unmanned aerial vehicles are purpose-driven[27]. For instance, Unmanned Aerial Vehicle (Drones) used for search and rescue mission in advanced healthcare computing is modelled to sense and detect objects (Humans) and perform certain action. Such action may include tagging the image and transmit such image or video to the logistics station, this will certainly enable the rescue team to plan and respond to the scenario based on the information obtained from the Drone system in the remote location. In undertaking such mission, there is need for predefinition of the services for the autonomous system, the policies that defined it basic operation and the survival instinct , which implies the perception of the responses.

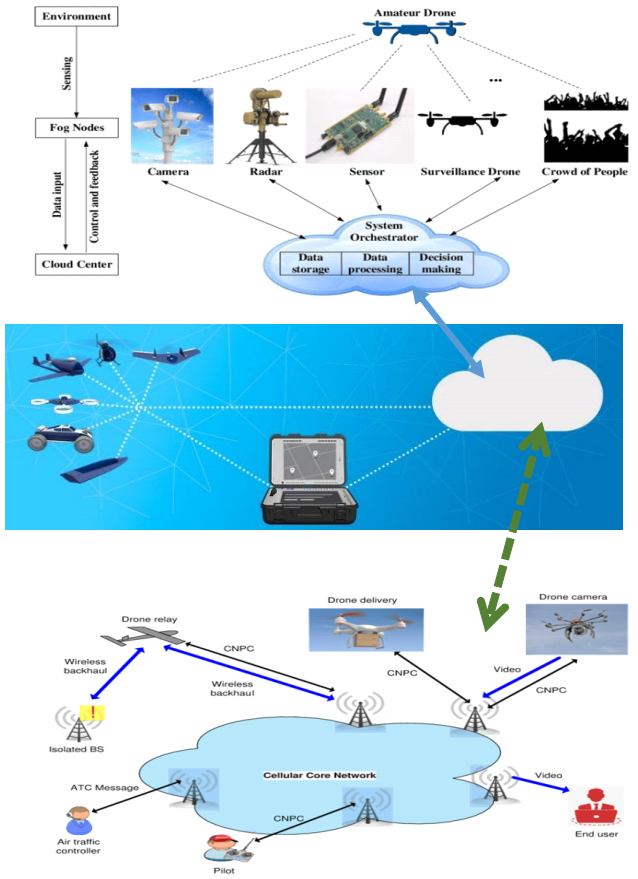


Figure 1: Drone Connective Infrastructure for Autopilot Autonomous Unmanned Aerial Vehicles navigation[2].

In the autonomous self-driving systems, the human supervisory role assumes a different dimension, instead of direct control and human superintendence, the system directly enforces the predefined accustomed schedules and conventions that influences the self-management decisions, **refer to Figure 2**. On this note, the international business machine (IBM) comprehended the four general attributes of the self-managing system as self-star also called Self-*, Self-x, or Auto-* properties for the autonomous system[28].

- **Self-Configuration**: An automatic system will usually undergo self-configuration of components to effect controls based on the perceived instances within its environment.
- **Self-Healing**: In the event of major or minor conflict rising from environmental impact, an automatic discovery and correction of faults is effected and the device is back on it prescribed mission[29]. An automatic system will always be able to resolve conflicts arising from series of interactions and inter-process communication.
- **Self-Optimization**: Every autonomous system will usually perform automatic examination and resource control self-consciousness to ensure optimality of functions with respect to the classified prerequisites. In resolving conflicts, the best case scenarios is usually employed to ensure that the result and outcome are highly optimized.
- **Self-Protection:** Taking pre-emptive actions and fortification from subjective attacks are the key operational requirements of the modern autonomous unmanned aerial vehicle system[30]. With the set of policies, the automatics system is sure to protect itself from anomaly through detect and attack mechanism or detect and escape. In some instances, self-protection requires obstacle collision avoidance and safest landing environment detection.

In the recent time, Scientists all over the world have further expanded the IBM submission of self –Star to accommodate some set of newly identifiable paradigm for Self-Regulation of the automatic systems. According to Lam et al 2018, the general policies and rules governing the automatic systems for self-management have been extended on the conventional Self-Star as required [31], which include:

A. Self-Regulation: Every autonomous system must function within the set boundary to maintain service quality and also act within a set range without external control usually governed by the set of internal policies and rules.

B. Self-Learning: The autonomous systems are required to utilize machine learning approach usually the Unsupervised Learning that does not necessarily depend on any outward command to effect inherent decisions.

C. Self-Awareness (Self-inspection and Self-decision): An Autonomous System ought to understand its internal operating environment and possibly extend its jurisdiction and boundary of operation[32]. It is important that an autonomous system should understand the degree of its own resources and the resources it is linked with, which will enable it to understand how to manage them judiciously. An autonomous system ought to be knowledgeable of its domestic inter-linkable and external linkable in the perspective of exerting influence in managing the key aspect of the operations without human interference.

D. Self-Organization: An autonomous system should maintain a spontaneous configuration capability to enable self-arrangement in a purposeful approximation within the applicable environment, devoid of the assistance from any external influences. Such autonomous systems must know and understand the nitty gritty of doing its own thing absolutely.

E. Self-Creation (Self-Assembly and Self-Replication): An autonomous system such as UAVs should be ambitious of environmental and social structure configurations with no categorical inducement or preoccupation of the external exaggerations [26].

F. Self-Management (Self-Governance): An autonomous device should have the capability to manage and govern itself through setting up of non-conflicting rules devoid of external intermediation.

G. Self-Description (Self-Explanation and Self-Representation): An autonomous computing system ought to explain and define its essence. Such system should be efficient in simplicity of understanding by humans with confirmation for expressive unambiguity.

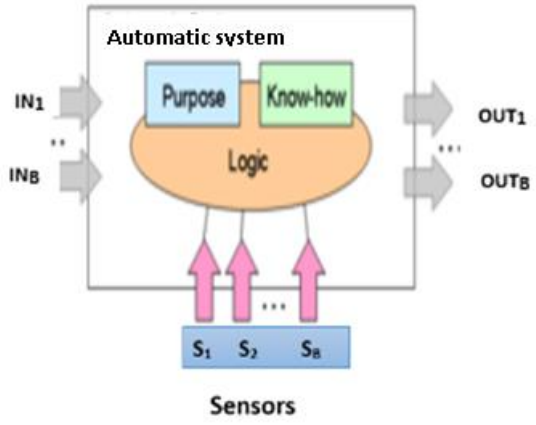


Figure 2: The Autonomous self-managing block Diagram[1].

However, the predominant objectives of autonomous computing is to comprehend hardware components, computer software systems and applications utilization which will coordinate themselves in the set priority with high-level management policy in the absence of human supervision[33]. Overcoming the well-known problems with autonomic computing systems involves scientific and technological innovations in a comprehensive and articulated fields, in addition to some novel software and system planning that promote a successful amalgamation of the constituent technologies[34]. The autonomic deployment model for implementing autonomous systems contained five distinctive policy categorizations specified below:

- Level 1 semi-autonomous policy categorization: The level 1 policy categorization is the fundamental level that describes the situation in which systems are to a large extent accomplished manually.
- Levels 2 - 4 autonomous categorization: At this level of autonomous policy categorization, systems are progressively automated with proportionate flexibility of administrative performances with less human supervisory functions.
- Level 5 perfect autonomous categorization: This policy categorization characterized the eventual perfection of every autonomous self-organizing , self-directing and self- supervising systems[35]**.**

Subsequently , the international agency regarded as "Internet Engineering Task Force (IETF)" and Distributed Management Task Force (DMTF), jointly formulated the policy-based administrative framework for the automatic systems[36]. The IEFT and DMTF administrative policy for the autonomous system consisted of four principal components:

- The Policy Management Tool (PMT).
- The Policy Repository (PR).
- The Policy Decision Point (PDP) and
- Policy Enforcement Point (PEP).

Usually, Policy Management Tool (PMT) is applied during the system administrative definition to validate the strategies to be implemented in the supervised networked information system , while all the consequential rules are warehoused in the repository in an arrangement that obligatorily conforms to the prototypical information model[37],in other to guarantee compliance along product lines from diverse manufacturers [38]. Once a novel strategies or rules are inserted in the repository or the subsisting policies are altered, the PMT copies all applicable PDP with validation and decodes the rules and corresponds the details to the PEP for considerable enforcement. The Policy Enforcement Point (PEP) is the division that absorbs all course of action with comprehensive understanding of execution (enforcement) of distinctive strategies. Implementation strategies are highly optimized because constituents of the design can interconnect among themselves utilizing multiplicity of conventions. The favourite optimal collaborative strategy for resolutions involving Policy Decision Point (PDP) and set of connective systems (PEPs) are the Common Open Policy Service (COPS) or Simple Network Management Protocol (SNMP) and Lightweight Directory Access Protocol (LDAP) for the Policy Management Tool /Policy Decision Point repository transmission [39]. Conventionally, the methodology for the strategic design is within the classification of the strategies , in which every strategy is made to assume the arrangement of an unpretentious stipulated encounter when actions are put together [40]. The Internet Engineering Task Force (IETF) strategic agenda was to implement this methodology and had contemplated strategies for regulations to validly postulate schedules to be accomplished in reaction to expressed circumstances:

if <condition(s)> then <action(s)>

However, the conditional function of the instruction may assume a very straightforward or complex demonstration, quantified in whichever order conjunctive or disjunctive standardization procedure. The executable component of the instruction can be a conjugation of proceedings that are obligatory to implementation whenever the specifications are confirmed. The Internet Engineering Task Force (IETF) did not describe any identifiable language as standard for expressing the multicomponent strategies, rather a general paradigm based concept and procedure for information framework that will demonstrate the strategic information construct [41]. This framework is a general purpose and nonspecific formulation, stipulating the composition of a conceptual strategic classifications by methods of association, consequently permitting manufacturers to put into operation their peculiarity design and performances to be used by the policy strategic evaluations. Logically, a strategically governed system must accelerate the explanation of extraordinary level managerial objectives which are straightforward for humans to unambiguously comprehend and appreciate to empower transformations into low-level strategies that will finally be mapped into instructions that readily organize the supervised systems correspondingly [40]. Even though the high-level objectives usually imitate the systems intentions for the administrative interconnections, the low-level strategies are accountable for device-level configurations. The strategies for improvement are the progression of transformation of the high-level strategic requirements into low-level implementable strategies that can be administered on the supervised devices. The fundamental responsibilities of the improvement in the perspective of course of actions are as follows:

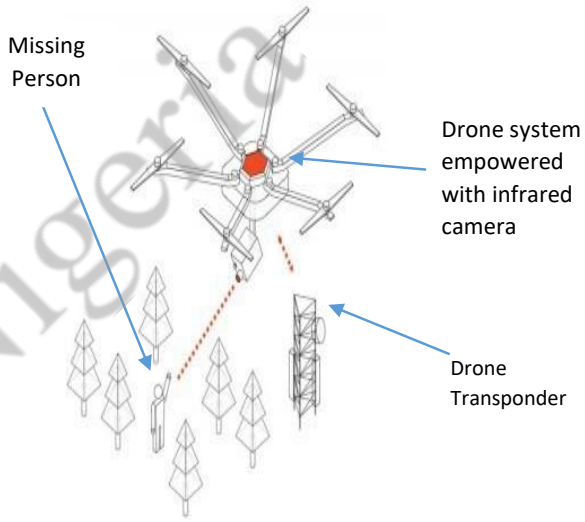
- Resolve the sources that are considered necessary to satisfying the conditions of the strategy. Ascertain the set of the criteria that best satisfied the demand of every autonomous system.
- Transform all high-level objectives into workable strategies that the system can implement with the available resources at its disposal.
- Substantiate that the low-level strategies truly intersected with the prerequisites postulated by the high-level ambitions and implement strategy.

V. RESEARCH IMPLEMENTATION

The current research was conducted to establish the latest development in the adoption of UAVs (Drones) in the 21st century mission beyond visually line of sight (BVLOS) in specific assignment with reference to IoTs framework. In doing so, attention was given to the advancement in the Drone technology to include line of sight (LOS) and beyond visually line of sight championed by IoTs, an advancement in mobile communication (4G,5G&6G) network connectivity. The Veronte Autopilot (a miniaturized, highly reliable avionics system for advanced control of UAV and Unmanned Aircraft System (UAS) embedded with a suite of state-of-the-art sensors and processors as well as a LOS and BLOS machine to machine (M2M) datalink were used to drive the mission of the current project. The cloud connectivity infrastructure via Veronte Cloud services were adopted for the integration of Drones in the Internet network to expedite airspace navigation and missions beyond visually line of sight. The initial design was focused on the use of Satellite Communications but now Veronte Autopilot had switched to Internet Connectivity with increased efficiency. The Veronte Cloud services empowers the harmonization of unmanned aerial vehicles flight data through the Cloud Server in the online flight schedule. The Internet of Things (IoTs) interconnection with the logistics location via the PC or 4G/5G Communications modem installed in the unmanned aerial vehicle switches the Veronte Cloud connectivity for an amplified adaptability in machine to machine (M2M) operative interactions.

The Veronte Autopilot is among the developers that are expecting technology improvements via the Veronte Cloud infrastructures. It describes the direction for the amalgamation of machine to machine (M2M) datalink synchronization in unmanned aerial vehicles driven by the development in end user acceptance of technology services. With the boost in the Microsoft Azure Cloud computing and Google Cloud technology, many companies will join the Space Drone technologies with different specifications and definition of operations. The global world will witness another computing paradigm characterized by IoTs enabled framework. The IoTs will either make the global world or destroy the global world completely, the two things, one is bound to happen. This innovation will further be enhanced by Cloud Technologies for Data Synchronization that will eventually link to Big Data phenomenon which will be of a greater challenge if measures were not taken preemptively. The Drones acting as sensor devices will certainly open up a large number of Internet of Things applications in the healthcare computing for emergency responses , agriculture, mining operations, security surveillance and Industrial Inspection Services[42]. The ongoing IoTs revolution in Drones industry have experienced accelerated transformation shifting from mere hobbyist play toy to become a system of complex IoTs devices. The advancement in the telecommunication world have ushered in 5G technology in an unexpected way to enhance the ability of Drones to respond to commands in real time and effect instant feedback in ubiquitously computing expeditions. The innovated IoTs Drones will assist the digital natives to perform some classified operations which will include but not limited to the current paper submission.

Figure 3: IoTs UAV system for Object Identification in Disaster Management[3]. The same is applicable to security surveillance, Law enforcement, Journalistic expeditions for news and intelligence gathering.



With reference to figure 1 & Figure 3, the cloud infrastructure became increasingly possible to stablish individual and simultaneous bidirectional communications between the control station and one or more Unmanned Aerial Vehicles (UAVs). The UAVs network was managed simultaneously to operate over large areas on hybrid IoTs Cloud Infrastructure allowing Data Synchronization through the Cloud Storage (Data Warehouse). It increases the productivity and coverage of services delivered by the provider. The systems and infrastructures permitted multiple UAVs to install Veronte Autopilot and perform flight operation simultaneously[2]. With effective compliance to the standard requirements defined in the International Standard Union, the unmanned aerial vehicles system have the capabilities to record Telemetry data , Transmit and keep log record with data recorded on every operational assignment[43]. Among several improvement recorded with utilizing Veronte Cloud Infrastructure for coordinating unmanned aerial vehicles on airspace include the increased collision avoidance, safety in UAVs flights management

and smart multimedia data acquisition by Veronte Autopilot component manipulation. These Autopilots Drone systems are empowered jointly to communicate among themselves and efficiently exchanged multimedia data ubiquitously and autonomously. The system and its infrastructure improved the algorithms for collaboration, senses avoid repulsion and as well as the flight control. This technology infrastructure allowed for analyze and coordinate with the information from transponders in the real synchronize able time management. The System allowed for synchronous configuration of events taking place in the UAVs environment managed with Veronte Cloud facilities. Performing automatic actions in unison, which include reporting the track of their current location and activities, analyzing all environmental data, sending of multimedia information (images, photos and video) through the cloud infrastructure to enable ground logistics managers take advantage for planning and coordinating responses.

VI. FUTURE RESEARCH FOCUS

From all indications, ensuring safety of Beyond Visual Line of Sight (BVLOS) flights is key factor to opening up new opportunities in flying and maintaining cost effective Military/Civilian Drones and all general purpose Drones system. Highlighting the most essential research issues, and their industrial applications, that is already receiving attention across the globe aimed at ensuring implementation of UAVs into a wider airborne ecosystem with maximum efficiency and safety for all stakeholders. Such research issues have been capture in (i.) Traffic Alert and Collision Avoidance System -TCAS (ii.) Mid-Air Collision Avoidance System-MIDCAS (iii.) Local Access Transport Areas –LATAS and other research projects supervised and sponsored by Defense Advanced Research Project Agency (DARPA), Federal Aviation Administration (FAA) and National Aeronautics & Space Administration (NASA). Specific attention should be given to the Drone industry to enable understanding of complexities in the line of flight and what steps are still needed to verify that all participants can securely guarantee the safety of a large number of Drones flight that would be conducted simultaneously in wide ranges and with no actual real time synchronization. Special agencies should steer up and engage Governments and decision makers on the state of Drones beyond visual line of sight (BVLOS) flying as well as their connectivity options either terrestrial (satellite networks control system) or IoTs cloud connectivity. The Perceive and Escape system experience, performance confrontation evasion and traffic prevention exploiting data fusion for diverse amalgamations of the integrated recognition technologies, usually the collaborative identification, friend or foe (IFF) interrogator and automatic dependent surveillance broadcast (ADS-B) transmitters and non-collaborative electro-optical, ultra violet(radar) and position finder sensors, components that assemble the signals released by other UAVs and space aircraft with information regarding location, speed and height. Every bit of these information are managed as part of administrative functions on Mid-Air Collision Avoidance (MIDCAS) that is accountable for airspace catastrophic circumvention, approximating the pathways travelled by an aircraft and resolving on whether the possibility of overlap(collision) exists and if possibilities exist then an preventive maneuvers are mandatory[44].

VII. RECOMMENDATION

The UAVs (Drones) are essentially utilized globally for advancing healthcare computing. Rwanda, Senegal, Ghana Malawi and Madagascar were countries in the Sub-Sahara Africa that had adopted the piloting of bi-directional mobility UAVs for healthcare computing and logistics management in Sub-Saharan Africa. The current paper analyzed the outcome in the most contemporary consideration to capture the Strengths, Weaknesses, Opportunities and Threats (SWOT analysis) in adoption of autonomous Unmanned Aerial Vehicles in healthcare computing as the requirement for the twenty first century extreme digital automation. In this paper, approaches for managing the autonomous unmanned aerial vehicles were presented, the regulatory considerations, supervisory issues, the feasibility requirements, the society satisfactoriness, monitoring and assessment requirements were reported to direct upcoming implementations in a more sophisticated and fundamental approaches. Recommendations for the Governments, Agencies, Key Stakeholders, Drone providers, Promoters and Funders include but not limited to:

- Designing/Developing more reliable robust technologies for AI autonomous UAVs (Drones) capable of self – performance and being able to undertake wireless recharging to ensure prolonged UAVs capabilities.
- Maintaining comprehensive vetting for UAVs (Drones) providers' capacities in providing logistical services during selection process.
- Ability to maintain in country manufactures and supply chain advantage for Drone services in locally made context. The American skeptics in adopting China made Drones are basically necessitated by fear of unknown, American President, American Congress and American people are right in that regard, please no apologies to China.
- Ability to coordinate efforts among all stakeholders and government as the key player.
- Implementing and recognizing financial support for extended period developments and investment sustainability.
- Comprehensive evaluation of impacts via standardized indicators by best standard practices. The outcome of this research should be taken a broader approach to data to include all information linkable to events. However, transmission of research findings and substantiation of UAVs potentials in ongoing healthcare automation projects is desirable for the current society advancement in the use of UAVs for healthcare computing and emergency responses. The researchers

strongly recommend future exploration on the concept of Beyond Visually Line of Sight(BVLOS) for Drones required for healthcare computing, disaster management and security surveillances in the authentic context.

VIII. CONCLUSION

Autonomous System essentially will be used globally for advancing Journalism, Healthcare Computing, Civilian Uses, Security Alertness for Law Enforcement Agencies and more advanced Military Defense Warfare in time to come. Rwanda, Madagascar, Malawi, and Senegal are among the sub-Sahara African countries that had adopted piloting the use of bi-directional mobility Drones for Journalistic and Logistic systems in sub-Saharan Africa. The outcome of this research should be taken a broader approach to date to include all information linkable to events. Sharing experiences and evidence from ongoing sector projects is needed to advance the use of Drones for Journalistic, Healthcare Computing and emergency responses. The researchers strongly recommend future exploration on the concept of Beyond Visually Line of Sight for Drones requirement for Journalistic mission and Disaster Management, News Coverages in the most authentic context.

IX. ACKNOWLEDGEMENT

The authors acknowledged the fact that the current paper does not attract any government or corporate funding and does not have any conflict of interest.

REFERENCES

[1] D. Weyns, "Towards a code of ethics for autonomous and self-adaptive systems," in *Proceedings of the IEEE/ACM 15th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, 2020, pp. 163-165.

[2] O. D. Dantsker and R. Mancuso, "Flight Data Acquisition Platform Development, Integration, and Operation on Small-to Medium-Sized Unmanned Aircraft," in *AIAA Scitech 2019 Forum*, 2019, p. 1262.

[3] C. Fan, C. Zhang, A. Yahja, and A. Mostafavi, "Disaster City Digital Twin: A vision for integrating artificial and human intelligence for disaster management," *International Journal of Information Management*, vol. 56, p. 102049, 2021.

[4] V. O. Gekara and V. X. Thanh Nguyen, "New technologies and the transformation of work and skills: a study of computerisation and automation of Australian container terminals," *New Technology, Work and Employment*, vol. 33, pp. 219-233, 2018.

[5] T. F. Abiodun, "Usage of Drones or Unmanned Aerial Vehicles (UAVs) for Effective Aerial Surveillance, Mapping System and Intelligence Gathering in Combating Insecurity in Nigeria," *African Journal of Social Sciences and Human Research*, vol. 3, pp. 29-44, 2020.

[6] H. R. Vanderhorst, S. Suresh, S. Renukappa, and D. Heesom, "Strategic Framework for Unmanned Aerial Systems Integration in Public Organisations in the Dominican Republic disaster management context," *International Journal of Disaster Risk Reduction*, p. 102088, 2021.

[7] N. Klein, "Maritime autonomous vehicles and international laws on boat migration: Lessons from the use of drones in the Mediterranean," *Marine Policy*, vol. 127, p. 104447, 2021.

[8] E. A. Nwankwo, C. Q. Omenyi-Sam, S. Uche, and L. Emeka-Aforka, "Glocalized Terrorism: A Predictive Study of Psychological Symptoms and Socioeconomic Status on Herdsmen Violent Attack in Anambra State," *Asian Research Journal of Arts & Social Sciences*, pp. 1-12, 2020.

[9] T. F. Abiodun, A. A. Asaolu, and A. I. Ndubuisi, "Defence Budget and Military Spending on War Against Terror and Insecurity in Nigeria: Implications for State Politics, Economy, and National Security," *Journal DOI*, vol. 6, 2020.

[10] E. Gordon and K. Lee-Koo, "Addressing the security needs of adolescent girls in protracted crises: Inclusive, responsive, and effective?," *Contemporary Security Policy*, vol. 42, pp. 53-82, 2021.

[11] T. C. M. Mbarga, R. Ndukwu, A. Ibochi, and F. Okeke, "Integration of Geospatial data of UAVs in Cadastral Management System and Regularization of Illegal Occupations in Informal Settlements," *African Journal on Land Policy and Geospatial Sciences*, vol. 4, pp. 76-99, 2021.

[12] N. Pasmurtseva, "Strategic Security of the Enterprise: Approaches, Features, Mechanism and Problems of Ensuring," in *SHS Web of Conferences*, 2021.

[13] F. O. Otieno, "Counterterrorism Strategies and Performance of the National Police Service in Managing Terrorism in Lamu County, Kenya Fredrick Okoth," MMUST, 2019.

[14] J. S. Odey and J. O. Ajor, "Herdsmen as the Spiritual Arm of Fulani Expansionist Quest: A Threat to Integration in Nigeria," *International Journal of Recent Innovations in Academic Research*, vol. 4, pp. 10-20, 2020.

[15] M. Lawrence, *Insurgency and Counterinsurgency in the Nineteenth Century: A Global History*: Routledge, 2020.

[16] J. M. Ramírez and J. Biziewski, *A Shift in the Security Paradigm*: Springer, 2020.

[17] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE access*, vol. 6, pp. 3619-3647, 2017.

[18] E. C. Too, Y. Li, S. Njuki, P. T. Yamak, and T. Zhang, "The Convolution Neural Network with Transformed Exponential Linear Unit Activation Function for Image Classification," in *Proceedings of the 2019 International Conference on Image, Video and Signal Processing*, 2019, pp. 55-62.

[19] M. F. Alam, S. Katsikas, O. Beltramello, and S. Hadjiefthymiades, "Augmented and virtual reality based monitoring and safety system: A prototype IoT platform," *Journal of Network and Computer Applications*, vol. 89, pp. 109-119, 2017.

[20] M. Cummings, *Artificial intelligence and the future of warfare*: Chatham House for the Royal Institute of International Affairs, 2017.

[21] M. Raissi, P. Perdikaris, and G. E. Karniadakis, "Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations," *Journal of Computational Physics*, vol. 378, pp. 686-707, 2019.

[22] T. Ko, "A survey on behavior analysis in video surveillance for homeland security applications," in *2008 37th IEEE Applied Imagery Pattern Recognition Workshop*, 2008, pp. 1-8.

[23] Y. K. Dwivedi, L. Hughes, E. Ismagilova, G. Aarts, C. Coombs, T. Crick, *et al.*, "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International Journal of Information Management*, p. 101994, 2019.

[24] J. M. Bradshaw, R. R. Hoffman, D. D. Woods, and M. Johnson, "The seven deadly myths of" autonomous systems"," *IEEE Intelligent Systems*, vol. 28, pp. 54-61, 2013.

[25] G. D. Baxter and F. E. Ritter, "28 Model-computer interaction: implementing the action perception loop for cognitive models," *Engineering Psychology and Cognitive Ergonomics: Volume 2: Job Design and Product Design*, p. 28, 2017.

[26] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1027-1070, 2019.

[27] G. Salmoral, M. Rivas Casado, M. Muthusamy, D. Butler, P. P. Menon, and P. Leinster, "Guidelines for the Use of Unmanned Aerial Systems in Flood Emergency Response," *Water*, vol. 12, p. 521, 2020.

[28] S. P. Sangani and S. Rodd, "Injecting Autonomic Computing into Legacy Systems: A Survey," *Bonfring International Journal of Software Engineering and Soft Computing*, vol. 6, pp. 230-233, 2016.

[29] R. D. Rasmussen, "Goal-based fault tolerance for space systems using the Mission Data System," in *2001 IEEE Aerospace Conference Proceedings (Cat. No. 01TH8542)*, 2001, pp. 2401-2410.

[30] B. B. Madan, M. Banik, and D. Bein, "Securing unmanned autonomous systems from cyber threats," *The Journal of Defense Modeling and Simulation*, vol. 16, pp. 119-136, 2019.

[31] A. N. Lam and Ø. Haugen, "Supporting iot semantic interoperability with autonomic computing," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 761-767.

[32] A. Silva, R. Mendonça, and P. Santana, "Monocular trail

detection and tracking aided by visual slam for small unmanned aerial vehicles," *Journal of Intelligent & Robotic Systems*, vol. 97, pp. 531-551, 2020.

[33] A. Samir, N. El Ioini, I. Fronza, H. R. Barzegar, V. T. Le, and C. Pahl, "A Controller for Anomaly Detection, Analysis and Management for Self-Adaptive Container Clusters," *International Journal on Advances in Software Volume 12, Number 3 & 4, 2019*, 2019.

[34] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, and J. Peleska, "Systems of systems engineering: basic concepts, model-based techniques, and research directions," *ACM Computing Surveys (CSUR)*, vol. 48, pp. 1-41, 2015.

[35] S. Bauk, N. Kapidani, Ž. Lukšic, F. Rodrigues, and L. Sousa, "Autonomous marine vehicles in sea surveillance as one of the COMPASS2020 project concerns," in *Journal of Physics: Conference Series*, 2019, p. 012045.

[36] Q. Hu, "Policy-based service management system," ed: Google Patents, 2016.

[37] E. Scheid, B. Rodrigues, and B. Stiller, "Toward a policy-based blockchain agnostic framework," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2019, pp. 609-613.

[38] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518-538, 2020.

[39] M. Charalambides, *Policy analysis for DiffServ quality of service management*: University of Surrey (United Kingdom), 2009.

[40] S. Lohmüller, "Cognitive Self-Organizing Network Management for Automated Configuration of Self-Optimization SON Functions," Universität Augsburg, 2019.

[41] J. Strassner and J. S. Strassner, *Policy-based network management: solutions for the next generation*: Morgan Kaufmann, 2004.

[42] Z. Qadir, F. Ullah, H. S. Munawar, and F. Al-Turjman, "Addressing disasters in smart cities through UAVs path planning and 5G communications: A systematic review," *Computer Communications*, 2021.

[43] J. R. Lehmann, T. Prinz, S. R. Ziller, J. Thiele, G. Heringer, J. A. Meira-Neto, *et al.*, "Open-source processing and analysis of aerial imagery acquired with a low-cost unmanned aerial system to support invasive plant management," *Frontiers in Environmental Science*, vol. 5, p. 44, 2017.

[44] D. A. Haessig, R. T. Ogan, and M. Olive, "“Sense and Avoid”-What's required for aircraft safety?," in *SoutheastCon 2016*, 2016, pp. 1-8.

Beyond Fear: Thinking sensibly in the Age of Emerging Cyber security Threats and Attacks

Abasiama G. Akpan[1], Mmeah Shedrack[2], Kings - Wali, Chisaa Ndidi[3]

[1]Department of Computer Science & Mathematics, Evangel University, Akaeze Nigeria
[2]Department of Computer Science, Ken Saro Wiwa Polytechnic, Bori Nigeria
[3] Department of Computer Science, University of Port Harcourt, Port Harcourt Nigeria

Abstract: The rapid growth of the internet has led to a significant growth of cyber threats and attacks incidents with disastrous and grievous consequences. Malware is the main weapon to carry out malicious intents in the cyberspace, either by exploration into existing vulnerabilities or utilization of unique characteristics of emerging technologies. The design of an innovative and effective malicious code (malware) defense mechanism has been regarded as an urgent requirement in the cyberspace. In this paper, we present a survey of the most exploited vulnerabilities in existing hardware, software, and network layers. We also discuss different types of emerging Cyber threats and new attack patterns in emerging technologies such as deep fakes, disinformation in social media, cloud jacking, ransomware, SQL injection attack, cross-site scripting, birthday attack and critical infrastructure. It has been established that these Cyber criminals are exhibiting common level of sophistication and advancement as the advances in Computer and mobile technologies. The available countermeasures are found to be satisfactorily effective, yet Cyber criminals are creating new measures to overcome security mechanisms. This paper has proposed several recommendations including the fact that the National Orientation Agency should shift focus to national re – orientation of the psyche of the whole population and particularly the youths in post – primary and tertiary institutions and to parents, towards raising crop of children with strong religious training, brief and trust in God as well as the infusion of religious training in the curriculum.

Keywords: Cyber Security, Cyber Attacks, Cyber Threats, Malware, Vulnerabilities.

I. INTRODUCTION

Our society, economy, and critical infrastructures have become largely dependent on computer networks and software solutions. We use cyberspace to exchange information, buy, sell product and services and enable various online transactions across a wide range of sectors, both nationally and internationally. Cyber attacks become more attractive and potentially more disastrous as our dependence on information and communication technology increases. Hence, a secure cyberspace is critical to the heath of the Nigerian economy and to the security of the global economy [1]. According to Symantec [2], a cyber attack is any type of offensive action that targets computer information systems, information system infrastructures, computer networks or system devices using various techniques to steal, alter or destroy data or information systems. Cyber attacks become lucrative because attacks are cheaper, convenient and less risky than physical attacks [3]. As discussed by Tatum [4], Cyber Attack can be defined as an attempt to undermine or compromise the function of a computer-based system, or attempt to track the online movements of individuals without their permission. Attacks of this type may be undetectable to the end user or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks [5].

Cyber criminals only require a few expenses beyond a computer and an internet connection. They are unconstrained by location and distance; they are difficult to identity and prosecute due to anonymous nature of the internet. Given that attacks against information and communication technology systems are very attractive, it is expected that the number and the sophistication of cyber attacks will keep growing. In the other hand, cyber security threats is a malicious act that seeks

to damage data, steal data, or disrupt digital life in general.

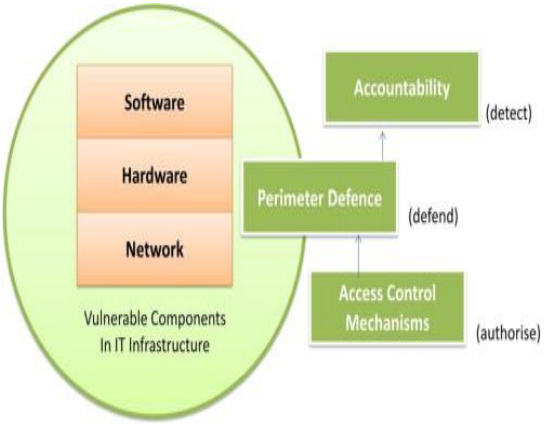


Figure 1: Vulnerabilities and defense strategies in existing systems [6]
Source: Julian jang – Jaccard *et al.* (2014)

Cyber security encompasses industry and government defense strategies adopted to curb cyber criminality in the super highway. It also involve the understanding of surrounding issues of diverse attacks and devising defense strategies (i.e. countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies [7].

- *Confidentiality:* It is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- *Integrity:* It is the term used to prevent any modification/deletion in an unauthorized manner.
- *Availability:* It is the term used to assure that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

In the words of Kosutic [8], Cyber security is the body of technologies, practice with coordinated series of actions, designed to defend networks, computers, system application programs and data from an attack, damage or unauthorized access. Cyber Security professionals classified Cyber emerging threats as malicious attacks, network attacks, or network abuse. Malicious attack is any effort to exploit another person computer and infect the system resources through Virus, Trojan horses, Spyware etc. Network attacks are intended actions meant to damage or disturb data flow of the computer system on a network service, which causes effects such as Denial of Service (Dos), Session Hijacking, Email Spoofing, etc [7]. Network abuse is fundamentally an exploit to the point of interaction of a network, and it could be utilized by actions such as spam, phishing, pharming, etc [8]. Cyber attacks are widely viewed as criminal action led by means of the Web. These exploits can incorporate taking an Organization's intelligent property, seizing online bank accounts, designing and circulating Viruses on different Computers, posting secret Business Data on the Web and destroy a nation's basic national Infrastructure. Internet threats are seen as the highest failure to business and revenue loses of all Organizations [9].

A lot of cyber security professionals believe that malware is the key alternative to carry out malicious intends to breach cyber security efforts in the cyberspace [10]. Malware refers to a broad class of attacks that is loaded on a system, typically without the knowledge of the legitimate owner to compromise the system to the benefit of an adversary. Some exemplary classes of malware include viruses, worms, Trojan horses, spyware, and bot executables [11]. Malware infects systems in a variety of ways, for examples, propagation from infected machines, tricking user to open tainted files, or alluring users to visit malware propagating websites. More concrete example of malware infection is that malware may load itself onto a USB drive inserted into an infected device and then infect every other system into which that device is subsequently inserted. Malware may propagate from devices and equipments that contain embedded systems and computational logic. In short, malware can be inserted at any point in the system life cycle. Victims of malware can range anything from end user systems, servers, network devices (i.e., routers, switches, etc.) and process control systems such as Supervisory Control and Data Acquisition (SCADA). The proliferation and sophistication of fast growing number of malware is a major concern in the Internet today [12].

II NATURE OF CRIME IN THE CYBER SPACE

Cyberspace refers to the interdependent network of information and communication technology components that underpin many of our communication technologies in place today. This component is a crucial entity of the Nigeria's and

global economy critical infrastructure. We use cyber space to exchange information, buy, sell products and services, and enable many online transactions across a wide range of sectors, both nationally and internationally. The primary targets of cybercrimes are on data, network, and access [5, 13]. Cybercrimes under the heading of data crimes include *data interception, data modification, and data theft*. Data interception is the interception of data on transmission. Data modification is the alteration or destruction of data on transmission [14]. Data theft is the taking or copying of data, regardless of whether it is protected by other laws such as US copyright and privacy laws, Health Insurance Portability and Accountability Act (HIPAA) or the Gramm Leach - Billey Act (GLBA) (Electronic Privacy Information Centre, 2004). Cyber crimes include access crimes such as unauthorized access and virus dissemination. Unauthorized access is the hacking or destruction of a network of system [14].

A. Demography and characteristics of Cyber Criminals

According to a study by ChiChao Lai *et al.* [15], the demographic characteristics of cybercriminals is revealing as well as disturbing and calls for concerted effort by all to avoid an impending catastrophe. The report findings show that 81.1% were male; 45.5% had some senior high school; 63.1% acted independently; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age bracket, which was the majority group. For those enrolled student cybercrime suspects, the findings show that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects in their respective years. The high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern. The following groups of people easily fall prey or perpetrate cyber- criminality is:

- Disgruntled employees
- Teenagers
- Political Hacktivist
- Professional Hackers
- Business Rival
- Ex-boy or Girl friend
- Divorced Husband or Wife
- Political enemies

The victims are gullible, desperados and greedy people, unskilled and inexperienced and perhaps unlucky people too can fall victim [16].

B. Top 20 Countries with the highest rate of Cybercrime

Symantec [2] has ranked 20 countries that cause the most cyber threats and attacks. In compiling such list, Symantec was able to quantify software code that interferes with a computer's normal functions, rank zombie systems, and observe the number of websites that host phishing sites, which are designed to trick computer users into disclosing personal data or banking account information [17]. Symantec was also able to obtain data including the number of bot-infected systems which are those controlled by cybercriminals, rank countries where cyber attacks initiated and factor in a higher rate of cybercrime in countries that have more access to broadband connections. The highest rate of cybercrime was found to be in the United States which contributes to the broad range of available broadband connections, which are those that allow uninterrupted internet connectivity [18].

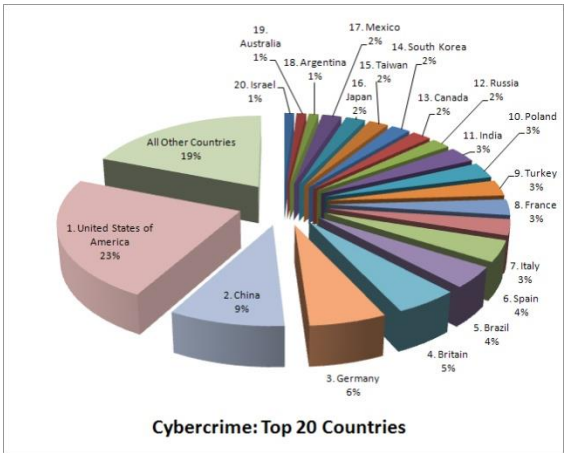


Figure 2: List of Top 20 Countries with the highest rate of Cybercrime
Source: Business Week/ Symantec

C. Top list of countries with lowest malware infection rates in computers

Sweden - 19.88%, Finland - 20.65%, Norway - 21.63%, Japan - 22.24%, Belgium - 22.78%, United Kingdom - 23.38%, Switzerland - 23.94%,

Germany - 24.12%, Denmark - 24.34%, Netherlands - 24.86% [18].

D. Corporate security Concerns

Denis [19] reported top three computer security concerns as:
(a) Embezzlement 30% (92), (b) intrusion or breach of computer systems 22% (67), and (c) computer viruses and denial of service attack 11% (33). These top three computer security concerns reflect the thinking of 63% of the organizations reporting. Figure 2 depicts in ranking order all the variables identified.

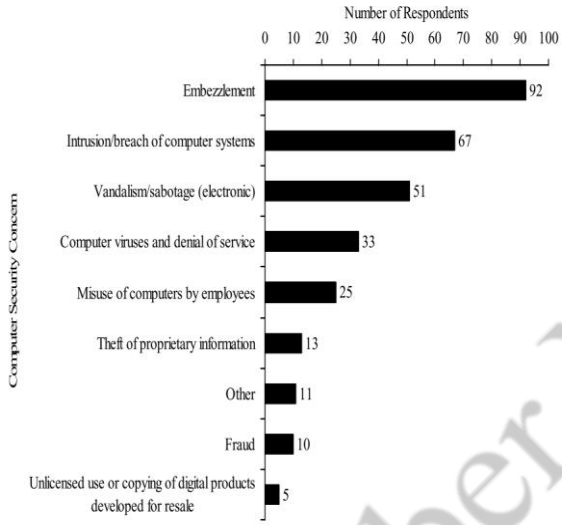


Figure 3: Ranking of computer security concerns by organizations [1].

E. Malware as attack took

In early days, malware was used to underline security vulnerabilities or in some cases to show off technical abilities [20]. Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. For example, malware is often used to target government or corporate websites to gather guarded information or to disrupt their operations. In other cases, malware is also used against individuals to gain personal information such as social security numbers or credit card numbers. Since the rise of widespread broadband Internet access that is cheaper and faster, malware has been designed increasingly not only for the stealth of information but strictly for profit purposes. For example, the majority of widespread malware have been designed to take control of user's computers for black market exploitation such as sending email spam or monitoring user's web browsing behaviors and displaying unsolicited advertisements [21]. Based on Anti-Phishing group report, there was a total of 26 million new malware reported in 2012. Figure 4 describes relative proportions of the types of new malware samples identified in the second half of 2012 reported by the Anti-Phishing group [22].

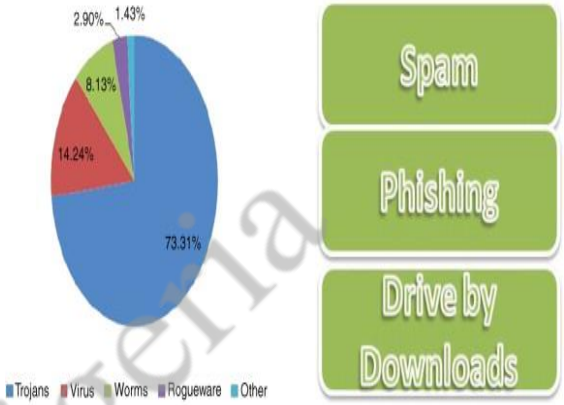


Figure 4: Types of malware and medium to spread them
Source: Julian jang – Jaccard *et al.* (2014)

III. RESEARCH METHODOLOGY

The data for this research were resultant of secondary sources, previous researches and analyses of scholars, books, Journals, Conference proceedings, white papers and Government publications on cyber security that are related to the current trend of cyber emerging threats and attacks. The study involved an extensive literature review which critically analyzed the present state of cyber security. It lay policies to enhance cyber security and the critical steps in acquiring the techniques on how to deal with the emerging cyber threats and attacks through content analysis approach.

IV. EMERGING CYBER SECURITY THREATS AND ATTACKS

Cyber threats and attacks have become routine as the internet itself. Each year, industry reports, media outlets and academic articles emphasize this increased occurrence, spanning both the amount and variety of threats and attacks [23]. In this study, we seek to further advance discussions on

some of the emerging cyber threats and attacks as follows:

- **Deepfakes:** Is a combination of the words "deep learning" and "fake". Deepfakes happen when artificial intelligence technology creates fake images and sounds that appear real. Examples of deepfakes are: creating a video in which a politician's words are manipulated, making it appear that the politician said something he never did. To minimize the risk, have strict verification procedures enforced.

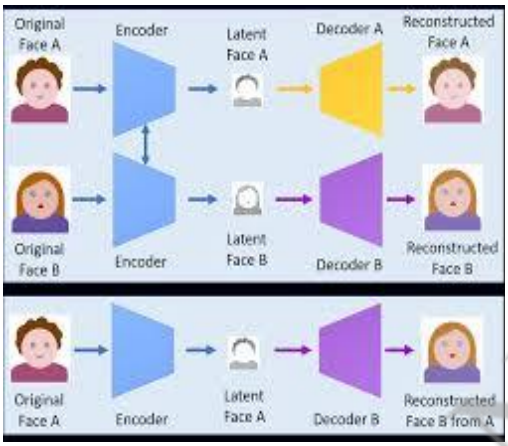


Figure 5: Deepfakes attack

- **Synthetic identities:** They are forms of identity fraud in which scammers use a mix of real and fabricated credentials to create the illusion of a real person. Example, a criminal might create a synthetic identity that includes a legitimate physical address. The social security number and birth date associated with that address, though, might not be legitimate. To minimize risks, ensure that your social security number, both physical and digital, is safe from thieves. Shred old documents that contain personal information.

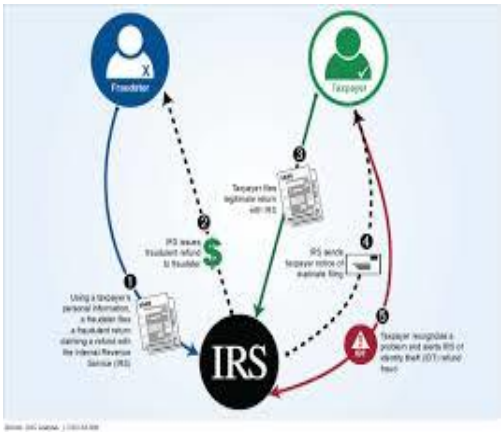


Figure 6: Synthetic identities

- **AI - Powered Cyber attacks:** Uses artificial intelligence. Hackers are able to create programs that imitate known human behaviors. These hackers can then use these programs to trick people into giving up their personal or financial information. To minimize the risk, machine learning algorithms is use to learn from historical data and detect anomalies to enable organizations to prevent and manage cyber attacks effectively and efficiently.

Figure 7: AI - Powered Cyber attacks

- **Poisoning attacks:** Artificial intelligence evolves. In these attacks known as poisoning attacks, cybercriminals can inject bad information into AI program. This bad information can cause the AI system not to function appropriately. Example, getting around spam detectors. To minimize the risk, DNS servers are subject to vulnerabilities. Staying on top of the latest patches can safeguard against attackers looking to exploit these well-known vulnerabilities.

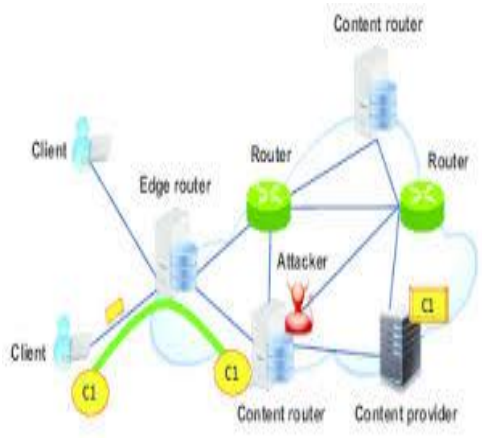


Figure 8: Content poisoning attacks

- **Disinformation in Social Media:** This is also known as disinformation, the deliberate spreading of news stories and information that is inaccurate and designed to persuade people - often voters - to take certain actions or hold specific beliefs. Examples, social disinformation spread through social media such as facebook, twitter, etc. To minimize the risk, limit profile information shared.

- **Advances in quantum computers pose a threat to cryptographic systems:** The threat is that quantum computers can decipher cryptographic codes that would take traditional computers far longer to crack if they ever could. To minimize the risk, implement strong cryptosystems with redundant encipherment and implement long key spaces.

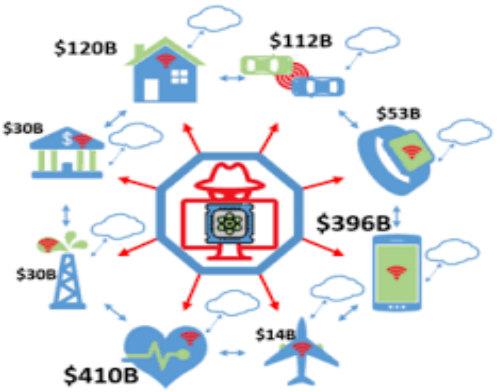


Figure 9: Quantum Attacks on Cryptographic

- **Vehicle cyber attacks:** As more cars and trucks are connected to the internet, the threat of vehicle-based cyber attacks rises. The worry is that cybercriminals will be able to access vehicles to steal personal data, track the location or driving history of these vehicles, or even disable or take over safely functions. To minimize the risk, a risk-based prioritized identification and protection process for safety-critical vehicle control systems should be put in place.

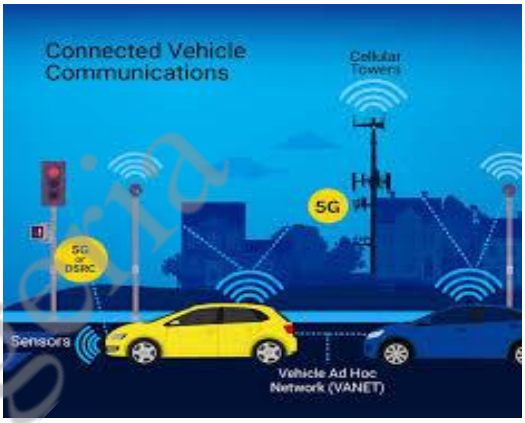


Figure 10: Vehicle cyber attacks

- **Cloud Jacking:** Is a form of cyber attack in which hackers infiltrate the programs and system of businesses, stored in the cloud, and use these resources to mine for crypto currency. To minimize the risk, restrict the IP addresses allowed to access cloud applications. Some cloud apps provide tools to specify allowable IP ranges, forcing users to access the application only through corporate networks or VPNs.

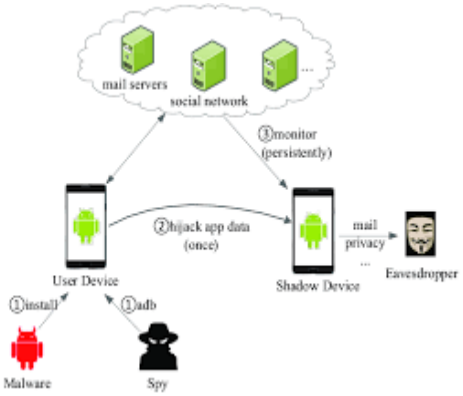


Figure 11: Cloud Jacking Attacks

- **Ransomaware attacks:** In a ransomware attack, the attacker infecting a victim's systems with a piece of malware that encrypts all of their data. The victim is then presented with an ultimatum – either pay the ransom or lose their data forever. To minimize the risk, strong perimeter security, such as firewalls to prevent malware from uploaded to your systems.

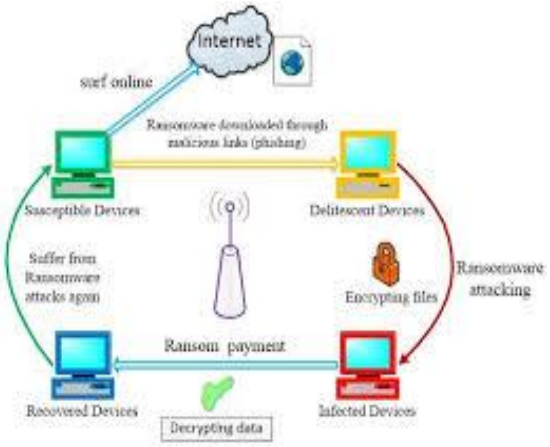


Figure 12: Ransomaware attacks

- **IOT – Based Attack**s: Is any Cyber attack that leverages a victim's use of internet – connected smart devices (Such as Wi – Fi enabled speakers, appliances, alarm clocks, etc) to sneak malware onto a network. To minimize the risk, keep the firmware for these devices up – to – date, as this can help resolve exploits that have been patched by the manufacturer.

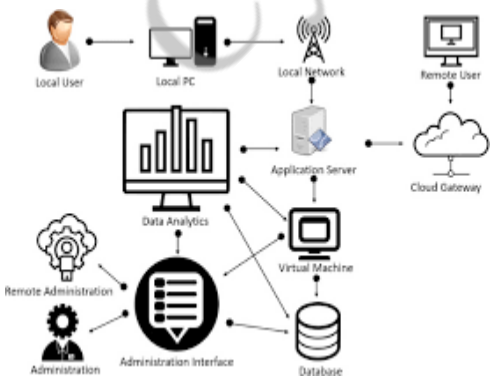


Figure 13: IOT – Based attacks

- **Denial-of-Service (DOS) and Distributed denial-of-service (DDOS) attacks:** A denial-of-service attack overwhelms a system's resources so that it can not respond to service requests. A DDOS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker. Examples are, TCP, SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and bonnets. To minimize the risk, blacklist IP addresses that are identified as being part of a DDOS attack.

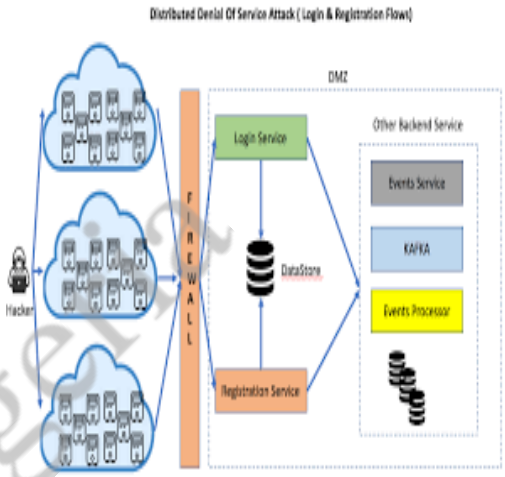


Figure 14: Distributed denial-of-service (DDOS) attacks

- **Man-in-the-middle (MitM) Attack:** A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Examples are session hijacking, IP Spoofing and Replay. To minimize the risk, don't allow employees to use public networks for any confidential work, or Implement virtual private networks (VPNs) to secure connections from your business to online applications and enable employees to securely connect to your internal private network from remote locations.

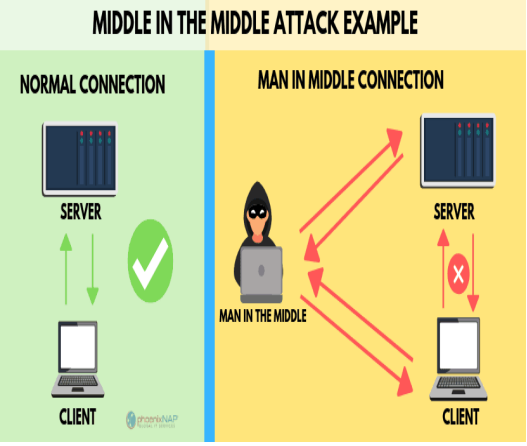


Figure 15: Man – in – the – Middle

Source: Google (2020)

- **Phishing and Spear phishing attacks:** Phishing attack is the practice of sending, emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering technical trickery.

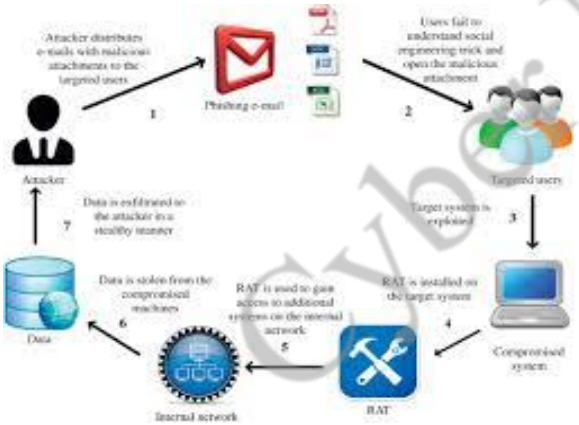


Figure 16: Phishing Attack

- Spear phishing is a targeted type of phishing activity attackers takes the time to conduct research into targets and create messages that are personal and relevant. To minimize the risk, develop a security policy that includes but isn't limited to password expiration and complexity and deploy a web filter to block malicious websites.

Countries	Number of Phishing Sites
Korea	87
China	75
India	25
Thailand	25
Japan	9
Chinese Taipei	18
Australia	4
Hong Kong	5
Malaysia	3
Singapore	2

Figure 17: Countries with phishing sites
Source: eBay

Figure 18: Ten Top Phishing Sites Hosting Countries
Source: Anti – Phishing Working Group

- **Drive-by Attack:** Drive by download attacks are common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP codeon one of the pages. To minimize the risk, one additional security control for preventing a drive-by virus infection is using different Web browsers, and only using vulnerable versions of IE on the specific applications that require it. General purpose Web browsing could be done using an alternative Web browser like Firefox, Chrome, Opera, etc. All of these browsers usually have different security vulnerabilities than IE, and will also require periodic security updates.

Figure 19: Drive - by Attack

- **SQL Injection attack:** SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the data base via the input data from the client to server SQL commands are inserted into data-plane input (for example, stead of the login or password) in order to run predefined SQL commands. To minimize the risk, input validation, parameterized queries, stored procedures, escaping and web application firewall should be apply.

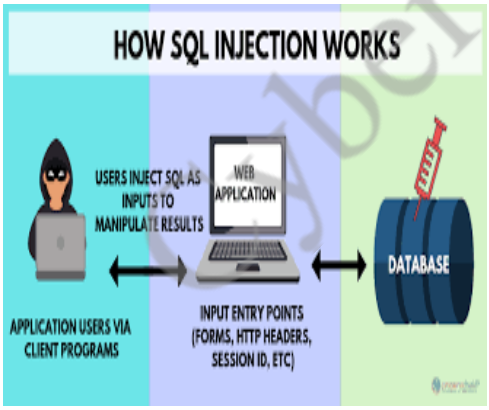


Figure 20: SQL Injection attack

- **Cross-site scripting (XSS) Attack:** XSS attacks use third-party web resources to run scripts in the victims' web browser or scriptable application. Specifically, the attacker injects a play load with malicious JavaScript into a website's database. When victim requests a page from the websites, the web site transmits the page, with the website transmits the page, with the attacker's play load as part of the HTML body, to the victim's browser, which executes the malicious script. To minimize the risk, an effectively preventing XSS vulnerabilities is likely to involve a combination of the following measures filter input on arrival, encode data on output, content security policy and Using appropriate response headers.

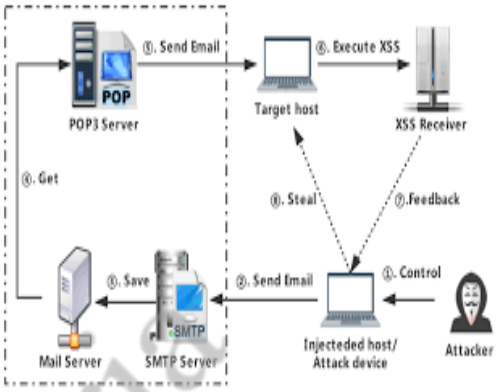


Figure 21: Cross-site scripting (XSS) Attack

- **Eavesdropping Attack:** Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. To minimize the risk, Eavesdropping attacks can be prevented by using a personal firewall, keeping antivirus software updated, and using a virtual private network (VPN)

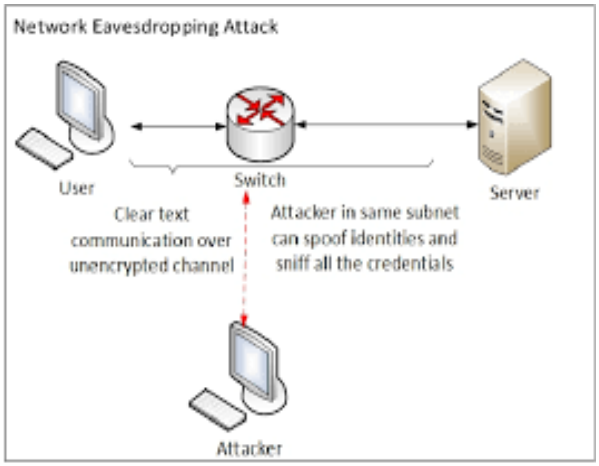


Figure 22: Eavesdropping Attack

- **Birthday Attack:** Birthday attacks are made against hash algorithms that are used to verify the integrity of a message

software or digital signature. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. To minimize the risk, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computationally infeasible, i.e. about twice as many bits as are needed to prevent an ordinary brute-force attack.

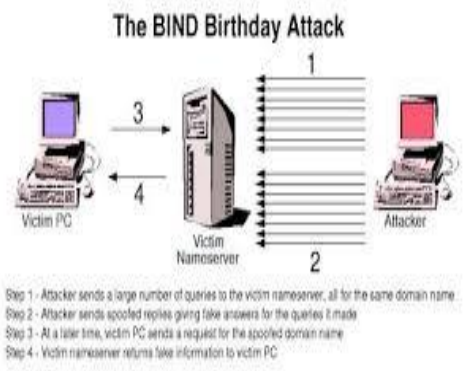


Figure 23: Birthday Attack

- **Malware Attack**- malicious software can be described as unwanted software that is installed your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the internet. Examples are, macro viruses, file infectors, system or boot record infectors, polymorphic viruses, stealth viruses, Trojans, logic bombs, worms, droppers, ransomware, adware, spyware. To minimize the risk, Malware attacks can be prevented by using a personal firewall and keeping antivirus software updated.

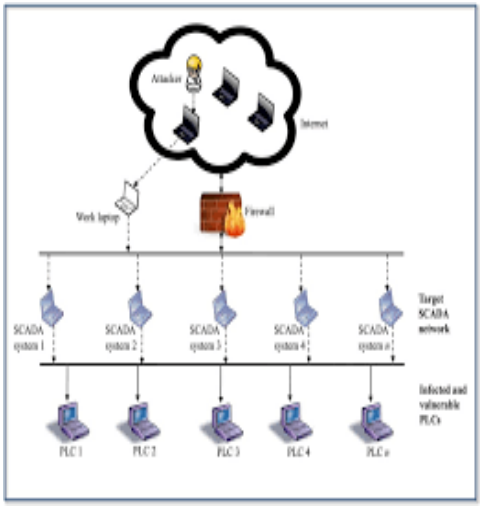


Figure 24: Malware Attack

A. *Security measures in place: industry security initiatives for the cyber space:*

Firewalls, Antivirus, Anti-Malware, Pass-Wording, Encryption, Biometric Authentication Systems, Intrusion Detection and prevention Systems, etc.

B. *Some Tested Palliative solutions in place*

If correctly installed, the following technologies can help to block attacks: (These will be explained further in the following pages).

- **Firewalls:** Firewalls are hardware or software devices that block certain network traffic according to their security policy.
- **Software solutions:** It exist to identify and remove malware and to help manage spam email. Many must be paid for but free versions are also available.
- **Authentication:** It involves determining that a particular user is authorized to use a particular computer. This can include simple mechanisms such as passwords, to more complex methods using biometric technology.
- **Hardware cryptography:** It uses computer chips with cryptographic capabilities intended to protect against arrange of security threats.
- **Patches:** They are programs designed by software manufacturers to fix software security flaws. Patching is often installed automatically. This reduces end-user participation and increases ease of use

VI. CONCLUSION

Cyber crime is real! The internet is the nervous centre of world economy. Cybercrime is conducted remotely and anonymously to take advantage of flaws in software code. Cyber crime has created major problems and has continued to increase at institutions of higher learning. The academia is emerging as a particularly vulnerable for internet crime. Organizations and individuals have suffered losses at the hands of cyber- criminals with only nine percent of such incidents reported to the security operatives. There is need for consistent training of the Nigerian Police in Cyber Crime Prevention and Forensic science for cyber crime policy and control. There is urgent need to develop a single national database to gather and compile cybercrime data. The National Assembly should consider enacting a legislation that encourages incident reporting while reducing the risks associated with reporting and provide policies that provide stronger sentences for those found guilty of committing a cybercrime.

REFERENCES

[1] Akpan, A. G., Mmeah S. and Baah Barida (2018). Cybercrime and Cyber security: A painted scenario of a new type of war. *Journal of Scientific and Engineering Research*, 5(10):185-197.

[2] Internet security Threats Report. Symantec, http://symantec.com/threatreprot/,last accessed: August, 2020. http://www.maawg.org/ last accessed: August, 2020.

[3] Goodman, S. E. and Lin, h. S. (2007). Toward a safer and more secure Cyberspace. The National AcademicsPress. Anti-phishing group tech report, http://www.antiphlishing.org/phishreports Acrhive.html, last accessed: September, 2020.

[4] Tatum, Malcolm (2010). "What Is a Cyber-attack?" Available on-line from: http://www.wisegeek.com/what-isa- cyberattack.htm (Accessed 29th September, 2020).

[5] Alhaji Idi Babate, Maryam Abdullahi Musa, Aliyu Musa Kida, Musa Kalla Saidu (2015). State of Cyber Security: Emerging Threats Landscape. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, Vol. 3, Issue 1, pp. 113 – 119.

[6] Julian jang – Jaccard and Surya Nepal (2014). A survey of emerging threats in Cyber security. *Journal of Computer and System Sciences*. Volume 80, Issue 5, pp. 973 – 993.

[7] Whitney, S. (2004). Trend turns more purchase coverage for cybercrime. Best's review, 105(8): 90. Oldwick, NJ: AM. Best Co. Inc.

[8] Kosutic, D 2007, what is Cyber security and how can ISO 271001 help? Blog. Accessed 5 September, 2020 < http://blog. iso27001standard.com/2011/10/25/what- is- cyber security and - how-can-iso- 27001- help/#

[9] Williams, P. (2002). Organized crime and cyber crime: implications for business. Retrieved on September, 2020.

[10] Canty, D. (2012). Digital Danger Zone: tackling cyber security. Arabian Oil and Gas, http://www.arabianoilandgas.com/article-9868-digitaldanger-zone-tackling-cyber security/ last accessed September, 2020.

[11] Justin, M. Rao (2011). The economics of spam email metric MAAWG report Microsoft research. Available at: http://www.maawg.org/system/ les/news/ MAAWG 2013

[12] Ponemon, (2012) Cost of Cyber Crime Study: United Kingdom benchmark Study of UK Organizations, Ponemon Institute Research Report October.

[13] Australian Parliament the report of the inquiry into Cyber Crime

http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

[14] DHSS & T Roadmap for cyber security research, Jan. 2009 http://www.cyber.st.dhs.gov/docs/DHS - Cybersecurity-Roadmap.pdf (Accessed: September, 2020).

[15] ChiChao Li, Wen Yuan Jen & Weiping Chang, Shihchieh Chou (2006), *Journal of Computers*, Vol. 1, No. 6, Sept. 2006, Academicy Publisher, USA.

[16] Osuagwu O.E., Anyanwu E. (2003) Management of Information Technology at Periods of Technological Discontinuity, OIPH, Owerri, Nigeria, p. 23.

[17] Top 20 Countries found to have the most Cybercrime: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ (Accessed September 10th, 2020)

[18] List of countries with lowest malware infection rates in computers: https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/ (Accessed September 16th, 2020)

[19] Denise Marcia Chatam (2007). The Study on Cybercrime's Impact in the Workplace, Campus Technology, USA.

[20] McConnel, B. W. (2001). Hearing on Cybercrime, Committee on legal affairs and Human nights, parliamentary assembly of the Council of Europe, Paris, France: McConnel International.

[21] E.E. Schultz (2006). Where have the worms and viruses gone? New trends in malware Computer. Fraud Secure (7) (2006), pp. 4- 8

[22] Anti-phishing group tech reports: http://www.antiphishing.org/phishReports Archive.html (Accessed August 13th, 2013)

[23] G. Cluley (2010), Sizing up the malware threat-key malware trends for 2010. Netw. Secur. (2010), 10.1016/S1353-4858(10)70045-3

A CYBERSECURITY & DATA PRIVACY MATURITY ASSESMENT FRAMEWORK FOR NIGERIAN PUBLIC AND PRIVATE ORGANIZATIONS

Aliyu Aliyu
PhD Student, Cyber Technology Institute.
De Montfort University
Leicester, UK.
p17243308@my365.dmu.ac.uk

Ibrahim Abdullahi
Assistant Lecturer, Software Engineering & IT
Nile University of Nigeria
Abuja, Nigeria.
ibrahim.abdullahi@nileuniversity.edu.ng

Sagir Muhammad Yusuf
PhD Student, School of Computer Science
University of Birmingham
Birmingham, UK.
smy870@student.bham.ac.uk

Adamu Bappi
Assistant Lecturer, Computer Science Department.
Federal College of Education (Technical)
Abuja, Nigeria.
bappiadamujauro@gmail.com

Abstract **Public and private organizations in Nigeria can utilise Capability Maturity Models to determine their maturity levels against best practices. Indeed, a need for a model that integrate both local and international regulations and standards exists. This article presents a model that can be used as a cybersecurity standard compliance monitoring tool for all organizations that are involved in the storage and processing of personal data conducted in respect of Nigerian citizens and residents; in line with the Nigeria Data Protection Regulation (NDPR) and other standards. The novel Maturity Assessment Framework incorporates the security regulations, privacy regulations, and best practices that organizations must be compliant to, and can be used as a self-assessment or a cybersecurity audit tool.**

Keywords— NDPR, CMM, cybersecurity

I. INTRODUCTION

Cyber-attacks are on the rise, with threats such as malware, phishing, ransomware, and spyware increasingly prominent, protecting organizations has never been more important. The Ponemon Institute's Cost of a Data Breach Report 2020 [1] recently revealed that the cost of data breach to organizations has never been this high, as organization spend a tremendous amount of money on four activities as they respond to data breach in terms of: Detection and escalation, Lost business, Notification, and also Ex-post response. Furthermore, with the advent of the global pandemic, Coronavirus has led to a fivefold increase in cyber-attacks [2] and is likely to leave organizations at a higher risk of attack for months, if not years, to come. And indeed, Nigerian organizations are not free from such attacks as studies by the Kaspersky Lab [3] showed that over 90% of organizations surveyed worldwide reported their IT infrastructure had been attacked at least once within the period of a year. The report also highlighted the danger corporate IT infrastructures are facing due to deficiency in terms of security and being constantly targeted by adversaries.

Public and private organisations can adopt from a wide range of off-the-shelf frameworks in order to improve their cyber security readiness. As most of these commercial frameworks have support both at an individual and organizational level. However, a research by Aloul [4] highlights that organisational program for security improvement are mainly successful when staff are given adequate custom training and education in cyber security awareness. The research also found that it is essential for the programs to be made part of the risk/security assessment plan adopted by all various departments and levels within the organisation, especially the administrative staff. This is because the administrative staff are the first line of defence of the organisation against adversaries as they are most the first point of contact when interacting with any organisation [5]. Hence, to ensure a secure environment within the organisation, it is essential to provide relevant security awareness program for the organizational staff. Ideally, constant training and education should be provided to equip both in-house and remote staff and employees to deal with ever evolving cyberthreats and be educate on the available modern prevention methods [6]. Overall, most importantly for the organisation, there should be an effective and efficient metric to measure and monitor compliance with standards. One such approach is through the method of changes to the organisational management and audits processes to strengthen the level of cybersecurity [7]. Thus, one such important set of tools is maturity models [8].

A maturity model can be defined as "a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline" [9]. The artefacts that make up the model are typically agreed on by the domain or discipline, which validates them through application and iterative recalibration. Maturity models are effective due to the measurable transitions between its levels as it validated based on practically empirical data. As a result of this validation, each level in the model is practically more mature than the previous level. Hence, what is considered as matured behaviours needs to be characterized and validated. However, this takes tends to be challenging and unambiguously in many maturity models.

Our proposed Cybersecurity Maturity Assessment Framework follows the Capability Maturity Model (CMM) [10] methodology. The process methodology was developed by the Software Engineering Institute of Carnegie Mellon University for the purpose of improving the management of software development. Over the years, this process was adopted in various other domains, including cybersecurity. Organisations can measure their standards competency and maturity by adopting maturity model as it encompasses a set of recognized best practices, skills, or standards. Performance scale as used to quantify and categorise Metrics. Thus, organizations can measure their performance against these maturity levels.

This paper makes the following contributions:

- It proposes a novel Cybersecurity Maturity Assessment Framework for public and private organisations in Nigeria that can be used to conduct standardised checks against 15 security requirements.
- The proposed framework incorporates necessary local and international regulations and security best practices.
- It is scalable as it can be adapted and extended to be used on other critical sectors of Nigeria.

II. PROPOSED FRAMEWORK

Our proposed Cybersecurity Maturity Assessment Framework (CYMAF) is based on an Appraisal methodology. An appraisal is an activity that organisations can adopt in order to identify the strengths and weaknesses of the organisational processes and also identify and compare to security best practices. Our proposed model can be used as a tool to check for organizational compliance and also gap-analysis identification. The CYMAF is established based on the following:

- A review of security requirements that Nigerian organisation must follow in order to demonstrate compliance mainly with the Nigeria Data Protection Regulation (NDPR) and other regulations that may apply to them such as the Consumer Protection Regulation (CPR), Data Protection Bill (DPB) etc.
- A literature review of existing research on cybersecurity appraisal and maturity models.

This paper, entitled "A Cybersecurity Maturity Assessment Framework for Nigerian Public and Private Organizations", aims to propose a framework that all public and private organizations in Nigeria can adopt as a self-assessment tool in order to determine their security level and also to highlight their weaknesses and mitigation plans as an organisation. It incorporates the local regulations that public and private organizations in Nigeria must comply with, such as the NDPR.

The framework has six different levels of maturity that organizational performance can be measured. Public and private organizations in Nigeria will benefit from the framework as they will be able to assess their security level, conduct a gap analysis, and create appropriate mitigation plans. The framework can also indicate whether the Public and private organization is compliant with the expected regulations, overall aiding in self-assessment and improvement through the output of its relevant compliance reports.

A. Security Requirements

The proposed framework consists of 15 requirements. The 15 requirements were created based cybersecurity best practices such as the CIS Controls, NIST Framework, etc. The 15 requirements were categorised into three groups as illustrated in Figure 1:

1. IDENTIFY (I)
2. PROTECT & DETECT (P)
3. RESPOND & RECOVER (R)

The first set of requirements, category Identify (I) consists of Requirements I1 − I4. The second set of requirements, category Protect & Detect (P) consists of Requirements P5 − P13. The third set of requirements, category Respond & Recover (R) consists of Requirements R14 − R15. Category Identify (I) consists of all the requirements that would enable an organisation to understand its business and operational ecosystem. Category Protect & Detect (P) consists of all the requirements that would enable an organisation to detect incidents and protect all its assets that supports the organizational services i.e., (people, procedures, and technologies). Lastly, category Respond & Recover (R) consists of all the requirements that would enable an organisation to respond and manage information security incidents that have the potential to affect the provision of organizational services. It should also be noted that all categorises have its main requirements and also sub-requirements as illustrated in Figure 1 below.

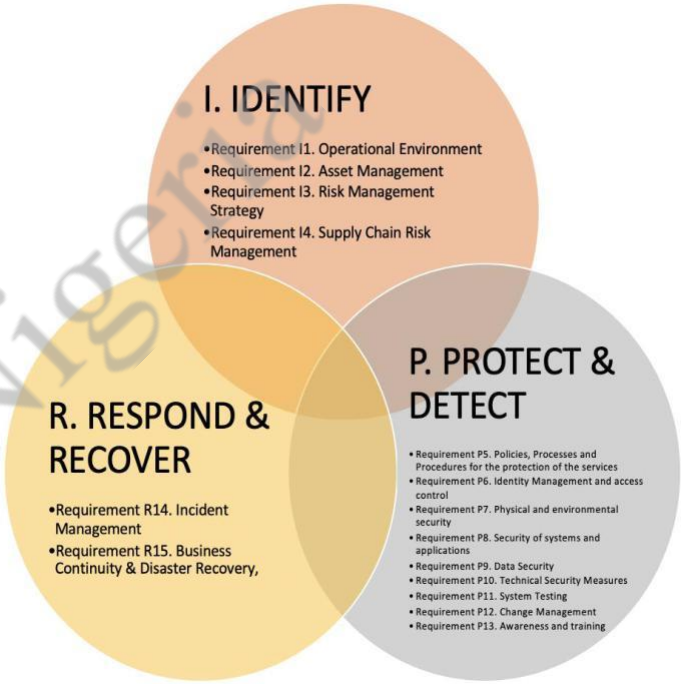


Figure 1: CYMAF General Security Requirements

B. Mapping of Regulations

It is worth stating that we incorporated our chosen regulation requirements of the Nigeria Data Protection Regulation (NDPR), Consumer Protection Regulation (CPR), and considered a draft of the Data Protection Bill (DPB) into our General Security Requirements. However, for this paper, we focused mainly on directly breaking down and mapping of the NDPR's principles. The mapping of the different regulations into the CYMAF was done accordingly. By focusing on each individual local regulation and mapping it into one of our requirements. For example, in terms of NDPR, we focused on the 9 principles of NDPR—and mapped each of the principles into one of our requirements. For example,

the first principle of NDPR is Clarity of Privacy Policy. This was mapped into Sub-Requirement P5.1: NDPR Compliance. The second principle, which is Rights of Data Subject, was mapped into Requirement P5: Policies, Processes, and Procedures for the protection of the services. The third principle, which is Data Security, was mapped into Sub-Requirement P.9.1: Encryption. The fourth principle, which is International Data Transfer, was mapped into Requirement I1. Operational Environment. The fifth principle, which is Third Party Processing, was mapped into Requirement I4. Supply Chain Risk Management. The sixth principle, which is Lawful Processing, was mapped into Requirement P5: Policies, Processes, and Procedures for the protection of the services. The seventh principle, which is Explicit Consent, was mapped into Sub-Requirement P5.1: NDPR Compliance. The eighth principle, which is Prohibition of Improper Motives, was mapped into Requirement P5: Policies, Processes, and Procedures for the protection of the services. The ninth principle, which is Data Integrity and Storage Limitation, was mapped into Sub-Requirement P.9.2: Data Classification.

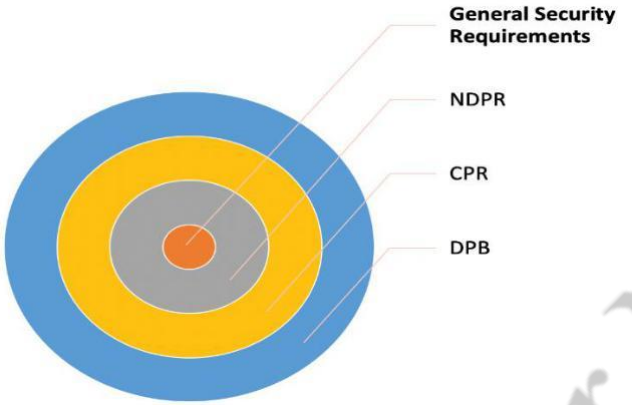


Figure 2: Overview of our maturity model standards

Figure 2 above shows the proposed regulations that would be incorporated into the maturity model. However, for this paper focus was given on the NDPR. This is to show the viability of the idea. Indeed, our chosen industry standards that make up the model, like the Nigeria Data Protection Regulation (NDPR), Consumer Protection Regulation (CPR), and Data Protection Bill (DPB) would make for an adequately sound cybersecurity maturity model.

C. Maturity Levels

Our proposed framework use maturity model with levels called maturity levels. These maturity levels are inbuilt in each of the main requirements and sub requirement. The maturity levels range from 0 to 5 i.e., it has 6 levels, with 0 being the lowest while 5 being the highest. Each maturity level and its meaning and also each maturity level builds on the previous maturity levels by adding new requirements. An example of such a scale is shown in Figure 3. The description of each level is presented below:

- Level 0: represents Incomplete.
- Level 1: represents Initial.
- Level 2: represents Managed.
- Level 3: represents Defined.
- Level 4: represents Quantitatively Managed.
- Level 5: represents Optimising.

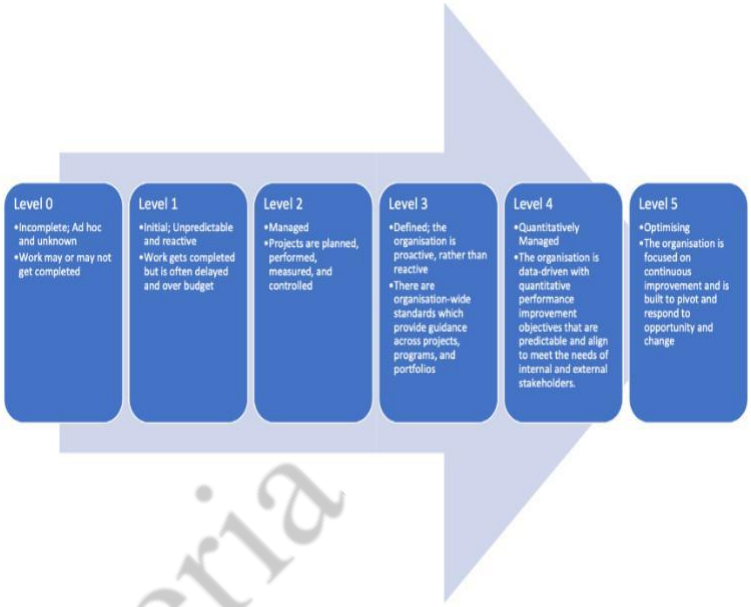


Figure 3: Maturity Levels

III. DISCUSSION

Our proposed framework defines a set of metrics that public and private organizations in Nigeria can adopt as a maturity assessment tool with regards to a set of recognized best practices, or standards. It incorporates the Nigeria Data Protection Regulation (NDPR), Consumer Protection Regulation (CPR), and Data Protection Bill (DPB) and can be used to conduct a gap analysis against 15 security requirements. The metrics are organized into categories and quantified on a performance scale. By applying the proposed framework, public and private organizations in Nigeria can achieve progressive improvements in their cybersecurity maturity by first achieving stability at the project level, then continuing to the most advanced-level, organization-wide, continuous process improvement, using both quantitative and qualitative data to make decisions. For instance, at maturity level 3, the organization has been elevated and transformed. It is proactive, rather than reactive. The organisation would have organisation-wide standards which provide guidance across projects, programs, and portfolios. As a public or private organization achieves the generic and specific goals at a maturity level, it is increasing its cybersecurity/standards maturity and at the same time achieves compliance with relevant international and local regulations and national laws.

IV. CONCLUSION

There have been several cyberattacks upon public and private organizations in Nigeria as well as around the globe, and the global pandemic has shown that organizations are not safe as it has been reported a global increase in cyberattacks have increased targeting organizations. Capability Maturity Models can enable public and private organizations in Nigeria to scale current maturity levels against best practices. To the best of our knowledge, there are no model that integrates several international and local regulations for public and private organisation in Nigeria to use or adopt. Hence, based on this finding, in this paper we present a model that can be used as a cybersecurity assessment tool for public and private organizations in Nigeria, as it incorporates security and privacy regulations and best practices.

The proposed model consists of 15 security categories, six maturity levels. In the future, we aim to conduct an in-depth mapping of the two other regulations (CPR and DPB) and also implement the model as an online platform that can be used both as a self-assessment and audit tool. Information that will be collected from the platform can be used in order to identify current security problems for both public and private organisations in Nigeria and prioritize future security plans and funding actions both by the individual organizations and the government of Nigeria in order to achieve of the mandate of the government; Digital Nigeria.

REFERENCES

[1] "Cost of a Data Breach Study", Ibm.com, 2020. [Online]. Available: https://www.ibm.com/uk-en/security/data-breach. [Accessed: 27- Sep- 2020].

[2] "WHO reports fivefold increase in cyber-attacks, urges vigilance", WHO, 2020. [Online]. Available: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. [Accessed: 27- Sep- 2020].

[3] Kaspersky, G.C.I. Global Corporate IT Security Risks: 2013; Kaspersky Lab: Moscow, Russia, 2013.

[4] Aloul, F.A. The need for effective information security awareness. J. Adv. Inf. Technol. 2012, 3, 176–183.

[5] Evans, M.; He, Y.; Maglaras, L.; Janicke, H. HEART-IS: A novel technique for evaluating human error-related information security incidents. Comput. Secur. 2019, 80, 74–89.

[6] Cook, A.; Smith, R.; Maglaras, L.; Janicke, H. Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure; BCS: Belfast, UK, 2016.

[7] Rajewski, J. Cyber Security Awareness: Why Higher Education Institutions Need to Address Digital Threats. 2013. Available online: https://www.huffpost.com/entry/cyber-security-awareness-_b_4025200 (accessed on 22 May 2020).

[8] Maglaras, L.; Ferrag, M.A.; Derhab, A.; Mukherjee, M.; Janicke, H.; Rallis, S. Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. arXiv 2019, arXiv:1901.03899.

[9]. Butkovic, M.J.; Caralli, R.A. Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale. 2013. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187 (accessed on 22 May 2020).

[10] Humphrey, W. Characterizing the software process: A maturity framework. IEEE Softw. 1988, 5, 73–79.

USERS' PERCEPTION IN HANDLING OF DATA SECURITY, CONFIDENTIALITY, AND PERFORMANCE OF CLOUD COMPUTING SERVICES IN NIGERIA

Adamu Bappi
Computer Science Department.
Federal College of Education, Gombe.
Gombe, Nigeria.
bappiadamujauro@gmail.com

Ibrahim Abdullahi
Assistant Lecturer, Software Engineering & IT.
Nile University of Nigeria
Abuja, Nigeria.
ibrahim.abdullahi@nileuniversity.edu.ng

Aliyu Aliyu
PhD Student, Cyber Technology Institute.
De Montfort University
Leicester, UK.
p17243308@my365.dmu.ac.uk

Sagir Muhammad Yusuf
PhD Student, School of Computer Science
University of Birmingham
Birmingham, UK.
smy870@student.bham.ac.uk

Bala Modi, PhD
Senior Lecturer, Computer Science Department.
Gombe State University
Gombe, Nigeria.
bmodi@gsu.edu.ng

Abstract— **The problem of data protection and security became worriment for most of the businesses in developed and underdeveloped countries all over the world. However, the problem is raising more concern to the businesses in developing countries due to the lack of storage infrastructure, data protections laws and enforcement, and poor knowledge of handling the data. This paves a way for huge subscription to data storage cloud services. In this paper, we analyses the Nigerian business firms' views over the level of trust they have on their cloud service providers and suggested the wayout. Security and privacy were marked as the worriment focal points in addition to the level of awareness.**

Keywords—Cloud computing, Data Security, Cyber Security

I. INTRODUCTION

The aspect of data storage is very important in every industry due to the role it plays in business analysis, record management, and so on(Okai et al., 2014; Uma Pavan Kumar Kethavarapu and S. Saraswathi, 2016). It is even considered as the most valuable asset of running business. Therefore, its security and privacy in all situations is very important because exposure may lead to a business crash due to competitors interruptions, records crashes, patents exposure, and so on. However, the demand for secured storage varies from country to another base on the level of development and technological progress. In developed countries, both private and public organizations respects the designated laws to protect businesses data both on cyberspaces or local records. Severe punishments were designed to punish law breakers. So, data storage rendering services were put into compulsory protection of client data. Additionally, those developed countries have designated storage architectures and stable power supply with steady building protections, these features makes them more likely to excel in data storage services for both their citizens and the under developed and developing countries.

However, in developing and under developed countries, the case is very different. Due to poor storage services, users have to use the inefficient local storage or subscribe to international cloud storage services (a designated online-based mass storage services). This makes most of the business skeptical about the security and privacy of their stored data in the cloud in addition to the cost. For example, let assume a shopping mall in Abuja which generate a daily transactions worth millions of naira and a combined transactions data and security videos of average 1gigabytes per day. To reduce, the storage cost will it going to be deleting its information everyday (mostly the videos)? That option subjected it to security and business analysis problem. Thus, a great solution is to subscribe to a well-trusted cloud computing services to protect its data.

While cloud computing is a viable solution, it encounters challenges interms of trusted communication link, users knowledge on data security, persist maintenance process, and synchronisation challenges. We all know that malwares are the major drawbacks of using an internet all over the world. Unfortunately, cloud services are only accessible via the internet, therefore, the security problem may not only be viewed at the cloud service providers perspective but also the communication link.

The use of cloud computing by such industries is still putting the question of: how secured by data is, in the hand the hands of the cloud service provides? The view is very different from the users of developed countries than the under developed countries. So, we decided to analyse the level of trust Nigerians business have over their cloud services providers. We run a survey on different businesses from different sectors and areas of the country. We then analyses all the suspected problems and suggested the way forwards.

This paper is organise as follows, section two discusses the roles and need of cloud computing services in developing countries by taking Nigeria as the use case. Section three outlined the procedure for data collections (survey), participant selections procedure, and results. The final section, discusses the result and the way forward.

II. Cloud Computing as the Revolutionary Technology to the Nigerian Industry

It is beyond any reasonable doubt that the issue of data security in Nigeria is facing various challenges due to poor laws on data protection, laws existing laws enforcement, and poor storage architecture. The Nigerian National Information Technology (NITDA) proposes the National Data Protection Regulation (NDPR) in 2019 that outlined all the necessary data safeguarding laws as prescribed in Nigeria constitution (Ekweozor, 2020). This is a step forward to towards securing the citizens' data as well as ensuring a transparent information technology services in the country. Despite the designated laws breaches, we outlined the following challenges as the main reasons for implementing secured and reliable cloud computing services in Nigerian industry

- Improper awareness: most of the data security staffs in Nigerian IT industries have poor knowledge on ethics of handling the collected users' information. Base on our survey, most of the staffs are not aware of the constitutional roles governing their roles of data collection and protection. Additionally, very few know the value of the data they are handling, some even expose the data for academic research without the consent of their users. We suggest that, this problem can be addressed by organizing orientation workshops by various governmental and non-governmental industries as well as suggest those industries to the cloud computing services whose terms and conditions are impose automatically and protected using international laws.
- Lack of proper storage architectures: most of the industries store their data on portable memory chips which are vulnerable to lost or get stole. Few of them uses back up servers in their offices, while this is a good idea, but their offices lack safety and security measures. For example, most of the offices lack fire extinguishing tools and protective doors.
- Poor update capacity: the firms mostly use 500gigabytes storage device to store their data. Consequently, this gets filled quickly and triggered the deletion of part of the data. Unknowingly to them, this has caused a lot of losses to their business as they can not trace back the history of their transactions.

- Law enforcement issues: enforcement of the data protection acts violation is poor in most part of the country; as a result, cyber crime and other related data protections laws violation become rampant.

The outlined challenges can simply be addressed by implementing an effective cloud computing services from first-class industries like Google, IBM, Microsoft, etc., their services provides a standard, affordable, and secured storage services safeguarded by international protection laws. Interestingly, all the laws governing their services were implemented automatically via the service terms and conditions; and the service providers are reliable base on their security and privacy history. The next section of the paper describes how we obtain the summary of the outlined challenges.

III. METHODOLOGY

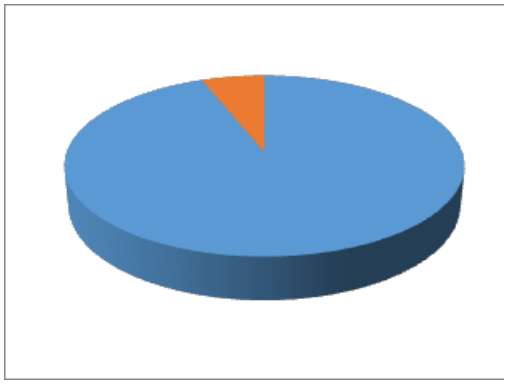
Challenges and solutions of cloud computing security were identified by this paper through critical reviewing of related literatures. Furthermore, survey was conducted to find out solutions/practices used in organizations for the Cloud computing security challenges.

When Data on phenomena cannot be directly observed, then Survey is applied by researchers to collect data, as the situation in our case. The survey conducted was non-experimental and descriptive. It aimed to investigate the research question. Variables such as knowledge and concept about cloud computing, the risk factors such as availability, performance, security, data portability/interoperability issues were examined.

By conducting the survey, the work will provide the driving reasons for Nigerian enterprises to adopt cloud computing platform and also provide suggestions for mitigating those risks and how to eliminate those barriers. In addition, the survey will provide an insight about enterprises perception of the available service and deployment models provided by the cloud computing vendors. To obtain the best outcome, the questionnaire was structured in two thematic areas as follows:

Users Perception on Security and Outlined Questions

These set of questions mainly evaluate the Cloud-security threats and threat agents facing SMEs. The questions are meant to look into the likelihood of threats and the SMEs preparedness or otherwise in respect of susceptibility to attacks, and to measure the reliability of cloud users to their Cloud Service Providers, with respect to securing their data. It also looks at the possible recommendations from the cloud users on how to hypothesize efficiently and effectively the security policy while using cloud. On the other hand, it also discusses the effort of government or organizations in terms of securing users data in the clouds.



Business Profile

These set of questions sought to profile the SME businesses aimed at documenting SME products and services, and their sectors of operations, e.g. banking and finance, ISP, public sector, etc. The set of questions gauged the level of compliance, ICT governance and ultimately, the risk impact associated with Cloud-security policies and procedures.

Sampling Procedure

By sampling, every participant has an equal chance of being selected. This method is one that gives every unit in the population a chance of being selected in the sample. In terms of this research, the chance of been selected as a participant depend directly on the knowledge of IT (Information Technology) with more emphasis on cloud computing. And the probability of been chosen as a participant is inversely proportional to the knowledge of cloud computing, non-updates on cloud computing practices. There are two basic types of sampling procedures adopted during this study. These include simple random and cluster.

There is no design without disadvantages, some of the challenges mainly faced are: It might not reflect on diversity of the community, other elements in the same cluster may share similar characteristics. It provides less information per observation than an SRS of the same size (redundant information: similar information from the others in the cluster), standard errors of the estimates are high, compared to other sampling designs with the same sample size. Furthermore, this research sampling procedure was adopted due to its reliability, distribution of the sampling places and its economic orientation. This survey is conducted on IT administration and IT staff of the below listed places in and outside Nigeria where more than 50 prospective IT practitioners participated. Survey included thirty one questions. The questionnaire including its rating scale is designed to evaluate the user's perception and security issues of cloud computing. An inquiry tool was developed to access this questionnaire. Questions were being rated by users from the given value for evaluation and to promote the cloud computing security and threat concepts. This design method is selected due to its security, easiness and manageability. The work involved survey from a range of relevant industry users of cloud computing services and universities. The following groups were targeted for the study:

1. Technical officers in department of Information Technology (IT) in universities
   The following universities were used: Nile University of Nigerian, Baze University, Gombe State University, Federal University Kashere, and Cavendish University Uganda.
2. Technical officers in department of Information Technology (IT) in the private and public industries.

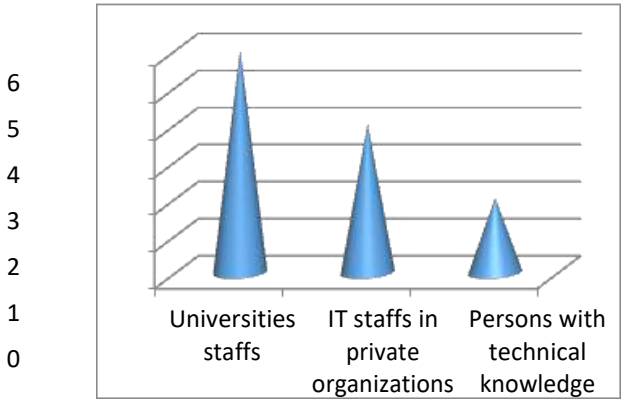


Figure 1.0 Survey responses bar graphs.

IV. RESULTS

From the analysis, several security challenges were identified during the survey that appeared as a great obstacle to the cloud user's level of trust. The list of identified challenges are: Lack of trust, Physical security, WLAN's security, Direct attacking method, Client monitoring, Perceived lack of reliability, Auditing, Password guessing, Trojan horses, Completeness, lack of fairness, Data leakage, Computer network attack, Data security, Network security, data locality, Backup and Data integrity. In part of the analysis, it was discovered that some of the attributes give greater threats to Cloud Computing, they are
Confidentiality, Integrity, Availability, Security, Accountability, Reliability, performance, and Auditability. The records of the most threaten attributes in figure 2. shows that Security 31%, Confidentiality 14% and Integrity and performance 0%, auditability and backup 28% each.

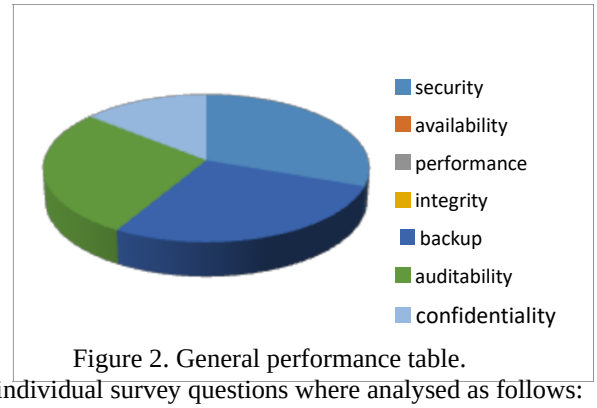


Figure 2. General performance table.

The individual survey questions where analysed as follows:

1. Does the Cloud Service Provider (CSP) allow a customer to select a specific location for the use or storage of the customer's data

No
6%

Figure 3. Survey question 1 response depicted in pie chart.

1. Does the Cloud Service Provider (CSP) provide a capability to locate and search all of a customer's data?

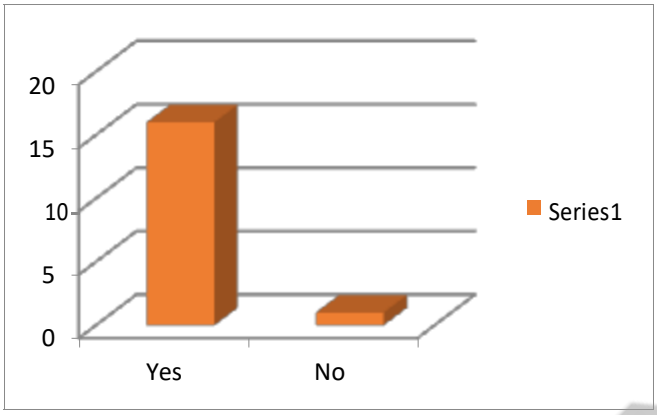


Figure 4. Survey question 2 response depicted in Bar graph.

1. Access to critical data is better controlled in a private cloud environment?

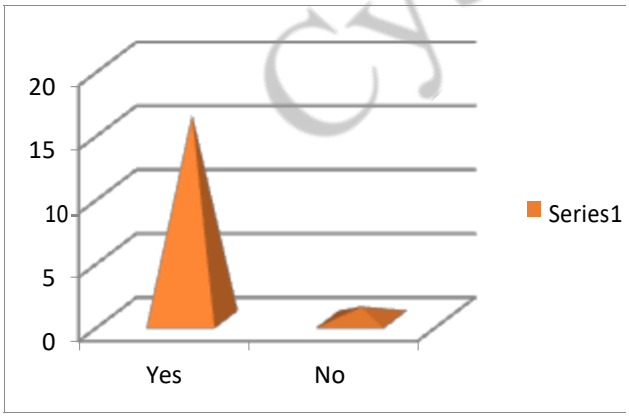


Figure 5. Survey question 3 response depicted in bar graph.

1. Does your CSP provide data masking to prevent data from potential hacks?

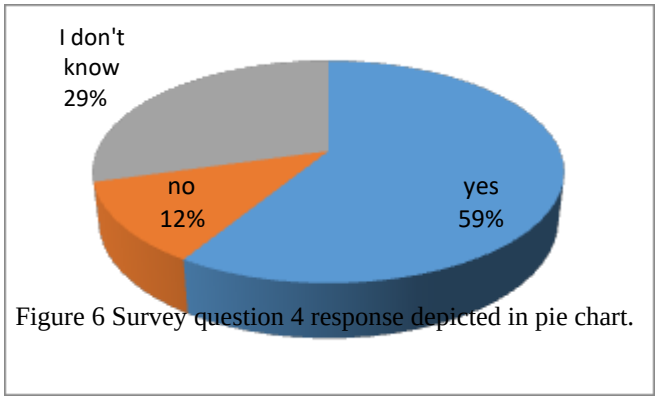


Figure 6 Survey question 4 response depicted in pie chart.

5. What functionality is provided by your CSP Security Network Intrusion Prevention System Virtual Appliance(NIPVA) for a cloud environment?

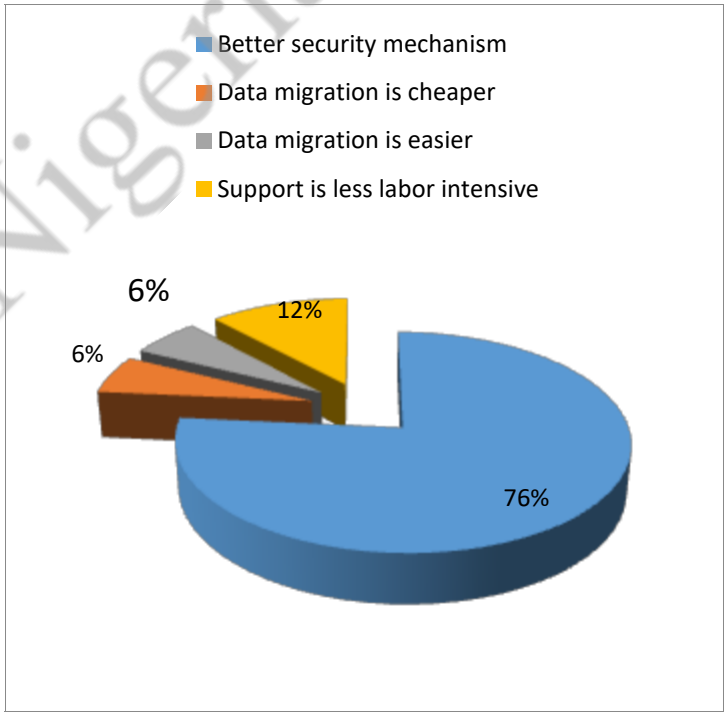


Figure 7. Survey question 5 response depicted in pie chart.

Reported challenges.

In the part of the Survey, a totally 13 Security challenges bedeviling perception of Cloud Computing users' level of trust were identified. A summary of these future security challenges based on the opinions from experts. The results

are as follows: (i) malicious insiders (ii) hypervisor viruses (iii) legal Interception point (iv) virtual machine security (v) trusted transactions (vi) Risk of multiple Cloud tenants (vii) Insecure application programming interfaces (viii) Privacy – Personal information about many people will be handled by Cloud Service Providers(CSP) all over the world. No one will know who is accessing user's data. From the results analysis of the results, the following security threat techniques were: (a) SSL (Secure Socket Layer) Encryption: Encryption between browser and web server. It usually provides enough security from the workstation to the browser. The use of SSL does not require Cloud service provider for any functionality (b) VPN (Virtual Private Network): VPNs are most commonly used for home based or mobile applications. When users connect to the internet from home or any public place like airport, hotel etc., then he will be signed into his VPN and get secure communication. Many Cloud Service Providers offer VPNs to cover the area from the work station in user facility to user connection to the internet and across the internet.

V. DISCUSSION AND CONCLUSION

The result of the conducted surveyshows that most of the cloud users have worried about the level of confidentiality, backup, auditability, integrity and security of their data which is stored by the local data storage infrastructure and the local cloud computing services. The results shows that security is the most factor which hinder the level of trust of the cloud user, most of the respondents worried about their business security as competitors may hijack their information. Most of the respondents suggested that Government agencies should be in charge of securing their cloud transactions. The identification of cloud users security perceptions in Cloud Computing is challenged by considering the large number of services. Most of the responses from the survey, noted that Cloud Computing is use by many users in handling their confidential information. As such, we suggest the use of soft and hard tokens to authorise access to the appropriate data.

It's solely recommended that, since many people are accessing and sharing their software applications online and access information by using the remote server networks instead of depending on primary tools and information hosted in their personal computers because of flexibility in Cloud Computing. From the perspective of this paper, It's also suggested that to find an optimum and appropriate security solutions for the specific services in the Cloud that will be highly transparent to the users, There is a scope to propose the guidelines to overcome the future challenges like physical security, espionage, transparency, data ownership, hypervisor viruses and malicious insiders in Cloud security. To concentrate on more specific areas like government intervention, regulatory and compliance issues, jurisdiction laws, etc.

REFERENCES

Ekweozor, E., 2020. An Analysis of the Data Privacy and Protection Laws in Nigeria (SSRN Scholarly Paper No. ID 3639129). Social Science Research Network, Rochester, NY. https://doi.org/10.2139/ssrn.3639129

Okai, S., Uddin, M., Arshad, A., Alsaqour, R., Shah, A., 2014. Cloud Computing Adoption Model for Universities to Increase ICT Proficiency. SAGE Open 4, 2158244014546461. https://doi.org/10.1177/2158244014546461

Uma Pavan Kumar Kethavarapu, S. Saraswathi, 2016. Concept Based Dynamic Ontology Creation for Job Recommendation System. Procedia Computer Science 85, 915–921. https://doi.org/10.1016/j.procs.2016.05.282

Tharam D. (2010) Cloud Computing: Issues and Challenges, 19-21 Dec p43.

Vaquero et al, (2008) A Break in the Clouds: Towards a Cloud Definition pp1-6

Ruoyu et al, (2010) Advent Of Cloud Computing Technologies In Health Informatics, pp. 32-39.

Tanzim et al, (2012) Securing Cloud from Cloud Drain, pp.1-4. Hof. R.D,(2006) Cloud computing as a facilitator of SME entrepreneurship pp.1-6.

Mell and Grance, (2011) NIST Computer Security Special Publication, pp.1-7.

James et al, (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, pp.1-18.

National Institute of Science and Technology, Special Publications (2011) pp.1-7.

Kresimir and Zeljko, (2010) Cloud computing security issues and challenges, pp.1-3

Jaydip, (2013) Enterprise Security and Privacy in Public Cloud Computing Environment -The African Case., pp.2-13.

Ramgovind et al, (2010)Tackling Cloud security issues and forensics model', High Capacity Optical Networks and Enabling technologies (HONET) , 19-21 Dec, pp. 190-195.

Ahmed S, Raja M. (2010) 'Tackling Cloud security issues and forensics model', *High Capacity Optical Networks and Enabling technologies (HONET)* , 19-21 Dec, pp. 190-195.

Ahuja R. (June 2011) SLA Based Scheduler for Cloud storage and Computational Services', International Conference on Computatonal Science and Applications (ICCSA), pp.258-262.

Albeshri A, Caelli W. (Sept 2010) Mutual Protection in a Cloud Computing Environment', 12th IEEE International Conference on High performance Computing and Communications (HPCC), 641-646.

Almulla S, Chon Yeob Yeun. (March 2010) Cloud Computing Security management , 2nd International Conference On Engineering Systems Management and Its Applications , pp.1-7.

B. lagesse. (Mar.2011) Challenges in Securing the Interface between the cloud and Pervasive Systems', 2011 IEEE International Conference on Pervasive Computing and Communications Workshops, pp.106-110.

Brenner M., Wiebelitz J. (may 31, 2011) Secret program execution in the Cloud applying homomorphic encryption', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference 2011, pp. 114-119.

C. C Ragin. (1997) Turning the tables: How case - oriented research challenges variable oriented research', Comparative social research, vol. 16, pp. 27-42.

Chang Lung Tsai, Uei –Chin Lin. (Aug 2010) Information Security issue of enterprises adopting the application of Cloud Computing

Applicability of Distributed IoT-powered Triage Units in the Management of Infectious Diseases in Developing Countries: The COVID-19 case

Reginald Ekene Ogu
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
reginald.ogu@futo.edu.ng

Lazarus O. Uzoechi
Dept. of Electrical and Electronic Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
lazarus.uzoechi@futo.edu.ng

Yusuf U. Mshelia
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
yusuf.mshelia@futo.edu.ng

Izuchukwu Azubuike Erike
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
azubuike.erike@futo.edu.ng

Chinomso D. Okoronkwo
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
chinomso.okoronkwo@futo.edu.ng

***Abstract*—Medical pandemics disrupt human activities and threaten the existence of man. Oftentimes, health care delivery services and personnel become overwhelmed by health interventions in the context of pandemics. Currently, the COVID-19 respiratory health pandemic has troubled the world economy. This paper presents the Phase One of a health care delivery architecture based on the Internet of Things (IoT) technology. The architecture proposed herein comprises of three layers: physical, communication and cloud. The architecture considered the peculiarity of developing countries like Nigeria, where there is inadequate electricity and limited communication bandwidth with poor Quality of Services (QoS) of the Internet. The IoT triage architectural model developed in this work aims to address priority on assignment of the limited health facilities such as bed spaces, ventilators, medical professionals, etc., based on comparative analytics on vital health signals updates from IoT devices of patients. In this work, much emphasis is placed on the physical layer of the architecture. By this, a use case diagram for the physical triage outfit is developed in addition to the architecture. It is expected that the proper implementation of this architecture in health care delivery services across the globe will go a long in managing and minimizing the effects of pandemics like the COVID-19.**

Keywords— automation, distributed databases, Network architecture, public healthcare, wireless application protocols

I. INTRODUCTION

Presently, the entire world is making frantic efforts to halt the fast speeding spread of COVID 19 disease because of the death rate of approximately 21% of the total outcome of the virus infection [1]. Within a period of four months from the date of its discovery in November, 2019 to April , 2020, COVID 19 has transited from an epidemic to a pandemic with over 2 million persons, reportedly infected by the Corona Virus infection [1].

COVID-19 is a novel disease related to respiratory infection like pneumonia, flu, etc. It was first detected in Wuhan, China around December 2019 with symptoms that include fever, cough, shortness of breath, difficulty of breathing, among others [2]. Within one month of its detection, it seriously threatened the existence of humans on earth. This raised alarm and made the World Health Organization to declare it a Public Health Emergency that requires the attention of everyone [3], [4]. According to [5], this virus has never been detected on human prior to this time.

The need to halt the spread of this disease is based on its negative effect on the economy of the world. According to [6], COVID-19 is already affecting the economy of the entire world but for developing economies like Nigeria, the probability of recession is inevitably high. For Nigeria, a country that is still recovering from the recession of 2016, a lingering COVID-19 pandemic can lead to unpredictable economy.

According to [7], health pandemics are characterized by a mismatch between the number of infected persons and available healthcare infrastructure and personnel. This is evident as the healthcare delivery of developed countries have been overwhelmed by the COVID-19 pandemic. In the case of the overwhelm of health care systems, the triage become so important in harmonizing patient needs and available resources [8].

A triage involves carrying out a comprehensive assessment on the sick or injured to determine the urgency for medical attention thereby prioritizing patients for treatment. The triage is an important part of the healthcare delivery system, it has become a critical process in health emergencies [9]. Errors during triage leads to increase in the probability of death of patients [8], [10], [11]. Thus, the need for an efficiently designed triage.

The triage is ever evolving [12]. From observations, the infrastructure and mode of operation of triage mechanisms in healthcare delivery in Nigeria are not working with the current day information technology (IT) and computing technologies. This makes the rich seek medical help overseas while the poor are left at the mercy of old, dilapidated, non-functional healthcare system. World-wide, healthcare facilities are highly overwhelmed by the novel COVID-19 pandemic that international boarders have been closed, even to the elites of developing countries for medical tourism.

In order to improve the quality of healthcare delivery, there is the need to have a functional triage system. This will go a long way in improving the quality of the healthcare

system and Nigeria will be in a better position to achieve the Goal Number 3 of the Sustainable Development Goals – Good Health and Well-being [13].

There is every need to employ some of the current technologies to combat this dreadful disease. As a matter of fact, the first country to experience COVID-19 (China) was able to relatively contain the spread of the disease using technology [14]. The ability of China to fight this disease has been identified in their ability to employ various emerging electronic and computing technologies. Among the notable technologies are 5G, big data and cloud computing. With these technologies, data such as facial recognition within the interaction networks of infected persons were traced and potential infected patients were notified before symptoms became obvious. The amalgamation of these technologies (Industrial Internet) empowered the Chinese to effectively wage war against and curtail the spread of COVID-19 [14].

Just like many developing countries, the quality of health care system in developing countries like Nigeria is poor. According to a report by the World Health Organization (WHO), life expectancy in Nigeria is less than 60 years [15]. Emphatically, developing countries cannot boast of state-of-the-art healthcare facilities. Nigerians are faced with stressful and undesirable scenarios while trying to get medical attention. Furthermore, there is no existing central medical database for the Nigerian citizens. When patients on triage have been profiled for treatment, the inaccessibility of their medical history impedes the treatment rate. According to [16], there is need for the development of a framework that will aim at improving the quality of life of citizens through a working healthcare system; hence, this research.

This research seeks to develop an Internet of Things (IoT) based functional triage model that can also access patients' medical history to aid in dispensing medical care for effective healthcare delivery in developing countries with Nigeria as a case study. Recently, the highest profiled COVID-19 victim in Nigeria, though later died, who used to treat previously underlying health conditions in London had to request for the medical records from the hospital in London to enable him to be treated in Nigeria as a result of the closure of the international boundaries [17]. This distributed IoT triage systems are meant to be set-up as an emergency response unit for the control of any epidemic in such developing societies to help curb the spread of any form of disease and not just COVID-19. The medical triage units are meant to detect and profile disease diagnosis in the order of their gravity using an estimated weighted value for each disease.

The Internet of Things (IoT) is a technological concept concerned with connecting things to the Internet for data exchange. Currently, IoT is applied to various areas of human activities such as transportation, energy management, etc. While IoT makes use of the ubiquitous capability of the Internet, edge computing is primarily concerned with actualizing data computation on distributed sensory units. It aims at reducing the time taken for data to be transmitted and received to/from the Internet by increasing the speed of sensing, data transfer, computation and actuation. It is envisioned that by applying IoT to Triage systems, a smart and reliable healthcare delivery system will be created for the management of COVID-19 pandemics. The IoT triage seek to effectively manage the relationship between patients' response and treatment.

II. Literature Review

The continuous measurement and analysis of patients' health status remotely can only be attainable by deployment of mobile computing, wireless communications and network technologies in telemedicine. In [18], categorized remote health monitoring into tier 1, tier 2 and tier3. Tier 1 is designated as the wearable sensor, tier 2 is the mobile application and tier 3 is the server.

A local triage algorithm, which has a fault-tolerant framework on mHealth, to elimination of single medical centre server to the adoption of a distributed hospital servers was proposed in [18]. In addition, the authors presented a philosophy behind the development of a framework to impede downtime issues related to mHealth, due to congestion issues in tier (3). By this, the authors added a fourth layer IoT telemedicine architecture. These four architectural parameters were applied, to realise a fault-tolerant framework in a triage medical system. This comprises of interaction, things, process, and data. The evaluation of this architecture was focused on the process layer. Thereafter, a developed risk-level localization triage (RLT) system algorithm was implemented to detect patients' emergency case, towards identification of the healthcare service package risk level in consideration to patients' time of arrival at hospital (TAH) and also recommend hospitals that offer these services based on information returned from a multi-criteria decision making (MCDM) system.

Existing IoT- based medical data transfer transmission was compared with the cellular network with regards to its efficacy in the medical triage system in [19]. The implementation of cellular based communication is more efficient because of its support for large emerging IoT applications according to[20]. The researchers identified the need of such communication technology to be employed in medical ambulances as a disaster management approach in crowded facility, whereby victims' chances of survival are dependent on first responders medical care before arrival to the hospital. Hence, the researchers developed an IoT-based prototype on MySignals HW v2 medical sensor board that supports various vital health signal evaluations, such as blood pressure, pulse, blood oxygenation, and respiration and additional diagnostic medical data.

A remote monitoring system of vital health signs for triage and detection of anomalous patients states in the emergency room was developed in [21]. The automation of the triage process was necessary to determine the level of attention based on a patient's health status. This paper took into consideration the development of a remote health monitoring system that could perform the triage process by continuous monitoring of the patient's vital signs in real-time.

A wearable health monitoring system was developed in [22]. The system comprises of a monitoring device (bracelet) that measures vital signs of patients and an information system (server) where signals received are processed to visual data format. This can be viewed as a graphical user interface at the client's device, in real-time. A 98 % and 100% data transmission evaluation results were observed after testing of the developed system on four (4) people of ages between 30 and 40 years, although the authors indicated these results were highly dependent on the wireless network availability [22]. This may not be applicable in a developing country with poor wireless network availability.

An automated triage system was to limit the time and human error experience in manual measurement and vital sign medical records by assistant medical officers was developed [23]. The system automates the triage process by use of a developed triage making decision algorithm. The algorithm is made up of machine learning technique and signals processing attributes that were developed using the MATLAB software. The automated triage system makes its decision based on vital sign inputs received from multiple sensors which are interfaced with an e-health kit v2.0 and an Arduino platform.

The triage process was classified into primary and secondary categories in [24]. The primary triage process occurs at the scene of incidents that intends to assign transport and treatment to most critical victims. Whereas secondary triage process is performed as victims await transport and while on their way to the emergency department of the hospital. The researchers were focused on the implementation of augmented reality technology for the secondary triage process.

Of special interest to our work is the layered architecture by [25]. The Distributed Internet-like Architecture for Things (DIAT) is scalable and accommodates heterogeneous objects while providing support for interoperability. In addition to the work above, a cost effective architecture platform, WAZIUP IoT architecture was proposed by [26], for developing countries to improve productivity. Their work was focused on enabling the rapid and cost-effective deployment of advanced and real-time monitoring. Among the key features, the systems support low cost, low power, low bandwidth, and intermittent Internet.

English researchers are testing a new mobile diagnostic system which comprises of a handheld lab-on-a-chip device that is integrated into a cloud network through smartphones [27]. Early studies have shown that the mobile diagnostic system can provide early detection of infectious disease outbreaks, even in remote areas. The duration of testing a patient is approximately 30 minutes. Whenever a patient tests positive, a report is sent to the central cloud platform [27].

As can be seen from the review above, there is paradigm shift in communication technologies deployed in development of eHealth systems. Integration of IoT, Edge computing, 5G Cellular network and AI technologies has become an important task in telemedicine.

III. Proposed IoT based Medical Triage Model Architecture

An IoT-Edge Medical Triage is necessary for the management of health pandemics. Therefore, the architecture comprises the union of factors unique to infectious diseases such as COVID19 as in our case study and developing countries' peculiarities. The proposed IoT medical triage architecture is shown in Fig. 1. The key peculiarity is the fact that there is unavailability of reliable Internet service in most rural towns in Nigeria.

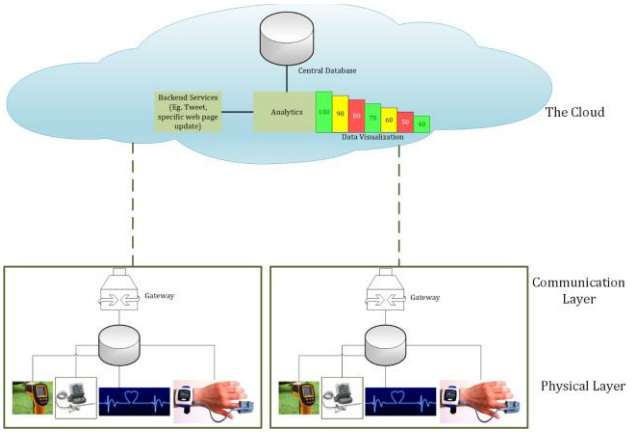


Fig. 1. Architecture of distributed IoT triage units for health emergency

The architecture is segmented into 3 major layers: Physical/Application layer, Communication/IoT layer and Cloud layer. Effective communication between these three layers ensures that data collected by the sensors are conveyed to the backend services.

The medical triage outfits are to house the assorted health parameter monitoring and measurement sensor. These sensors are connected to a local storage. The gateway links the local data to the cloud wirelessly, it provides the sensors with ability to communicate using the Internet protocol. The cloud and related backend services are used to integrate the distributed medical triage unit data. In the cloud, there is a central data storage and analytics. For this work, emphasis is placed on the Application layer.

A. Application Layer

The proposed medical triage use case incorporates features with the peculiarities identified below.

- Non-technological input that interfaces with the application layer like non-formal medical history from native approaches as part of the diagnosis process. This forms a strong aspect of our application layer which is peculiar to developing countries.
- Local interim storage facility as a framework for effective medical triage deployment especially with the inconsistency of network connectivity. The infrastructure provisions of the other architectures present cloud platform as a major part of storage facility in a primary mode.
- Artificial Intelligence data analysis. Insufficient medical personnel characterize the medical expertise in developing countries. Hence, a trained neural network is a significant part of this architecture.
- Sanitization: Sanitizes all users at entry and exit of the triage centre and in between medical intervention.
- Diagnosis: This component diagnoses possible carriers of infection and those that have met infected people.
- Quarantine: this process isolates positively testing patients from infectious disease to be treated until tests negative or perhaps, case of mortality.

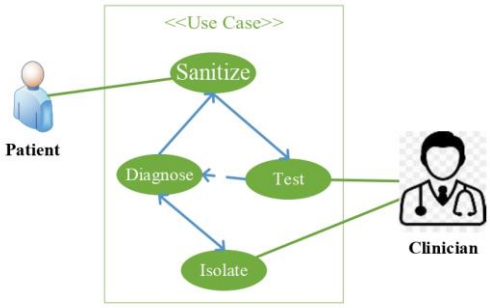


Fig. 2. Application Use Case for Infectious Disease Medical Triage.

This layer explains the use case in accessing service as a process by both patient and clinician. These processes provide services to Sanitize, Diagnose, Test and Isolate. To initiate the triage process, the patient is sanitized. This is automatically triggered as in Auto-sanitize from the architecture. Part of this is precautionary safety measure from getting infected and preventing the spread to others. Secondly, the diagnosis follows. This process takes input such as the vital signs from other technical medical officers in the laboratory or from other tools in the test process. The Diagnoses differs from the Test process in that Test produces empirical result either from medical testing tools like the laboratory, Radiology/X-Ray Scans. In addition, travel and medical history will also take input from other sections like medical records and perhaps, non-formal undocumented records as other forms of input to diagnosis. Depending on cumulative assessment of diagnosis, patients will be quarantined or not.

The relationships between these processes are outlined for patient to initiate the process at the Medical Triage Unit by Sanitizing first to access other services to avoid further spread. From there, diagnosis is proposed where testing is called in. Depending on the outcome, the patient is again sanitized and discharged or quarantined. The activities between Quarantine and Diagnosis is looped until Test shows negative of infection and subsequently discharged.

While in quarantine, iterations of processes between diagnosis and quarantine loops until a negative test of infectious disease is obtained.

IV. Discussion

The architecture above is particularized for use in the combat of health emergencies such as the COVID -19 pandemic. The adoption of an architecture like this in developing countries like Nigeria has become necessary because medical pandemics like COVID-19 tend to overwhelm the health care system, even in the developed countries.

The data collected by the health testing sensors is stored in a local Database and subsequently sent to the cloud using Advanced Message Queuing Protocol (AMQP). This conforms with the submission of [28]. The protocol is proposed to increase the availability of the cloud-backend services to nearly 100%, especially in low-cost and limited bandwidth of developing countries. In this protocol, data is sent from the physical layer in small efficient packets. The AMQP protocol is an enhance mode of sending message to the cloud to incorporate data persistence to the architecture.

Data persistence capability ensures that the gateway transmits unsent data to the Internet. Unsent data arise or come to exist when the Quality of Service (QoS) is poor, thereby preventing the effective communication of the gateway and the Cloud. Unsent data transmission occurs because of the low QoS of Internet connection, as is the case in developing countries.

For the networking technology, IEEE 802.15.4 based communication is proposed for adoption. The reason for this adoption is because of the high-power demand of IEEE 802.11x based technologies. Technologies like Sigfox and LoRA can be efficient in this application based on their low power demand while being able to travel long distances. These technologies are IPv6 over Low-Power Wireless Personal Area Networks (6LowPAN) capable. Hence, able to transmit and receive up to 250 kbps in distance >150m.

In addition, our framework ensures that only relevant data is transferred to the cloud. The proposed architecture supports efficient data collection from the sensor and transmission to the internet. These activities can be followed by central cloud data processing as proposed by [29].

Worthy of note is the use case sanitization process located as the fulcrum of the service delivery system. This process can either be in the form of auto-sanitizing infrastructure of manual access to handwashing and/or sanitizer facilities in between service processes.

In addition to the above, a close examination of the triage use case outlines the fact the triage of this paper tries to strike a balance in the use of the two main triage algorithms explained in the work of [30]. The algorithms mentioned are START (Simple Triage Algorithm and Rapid Treatment) and SALT (Sort, Assess, Lifesaving, Interventions, Treatment, and Transportation).

V. Discussion

To ensure the continuous existence of humans on earth, there is need to manage health pandemics effectively. With the above in mind, this paper has been able to achieve its objective of proposing an architecture based on IoT technology. In this work, a healthcare delivery architecture that can effectively support the combat of infectious diseases in health pandemics while focusing on the current COVID 19 disease has been developed.

In the operation of the triage, START (Simple Triage Algorithm and Rapid Treatment) and SALT (Sort, Assess, Lifesaving, Interventions, Treatment, and Transportation) algorithms were harmonized to make the efficiency of the triage process high, especially in the management of health pandemics.

Future works will be geared towards the real-life implementation of the proposed architecture.

References

[1] Worldometer, “Coronavirus Cases,” Worldometer, 2020. [Online]. Available: https://www.worldometers.info/coronavirus/coronavirus-cases/#daily-cases. [Accessed: 09-Apr-2020].

[2] CDC, “Can people in the U.S. get COVID-19? How does COVID-19 spread?,” 2020.

[3] Wu, K. Leung, and G. M. Leung, “Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: a modelling study,” Lancet, vol. 395, no. 10225, pp. 689–697, 2020, doi: https://doi.org/10.1016/S0140-6736(20)30260-9.

[4] WHO, “Coronavirus (COVID-19) events as they happen.” [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen. [Accessed: 09-Apr-2020].

[5] S. Mishra, S. Kannan, C. Manager, A. Statistics, R. Comments, and E. Alert, “omparing the Effectiveness of Three Ergonomic Risk Assessment Methods—RULA, LUBA, and NERPA—to Predict the Upper Extremity Musculoskeletal Disorders,” Indian J. Occup. Environ. Med., vol. 22, no. 1, pp. 17–21, 2018, doi: 10.4103/ijoem.IJOEM.

[6] L. O. Akanni and S. C. Gabriel, “The implication of Covid’19 on the Nigerian Economy | CSEA AFRICA - CENTRE FOR THE STUDY OF THE ECONOMIES OF AFRICA,” 2020. [Online]. Available: http://cseaafrica.org/the-implication-of-covid19-on-the-nigerian-economy/. [Accessed: 09-Apr-2020].

[7] H. L. Haller, P. Wurzer, C. Peterlik, C. Gabriel, and L. C. Cancio, “5 - Burn Management in Disasters and Humanitarian Crises,” in Total Burn Care (Fifth Edition), Fifth Edit., D. N. Herndon, Ed. Elsevier, 2018, pp. 36-49.e2.

[8] [8] R. K. Kanter, “Chapter 18 - Critical Care in Public Health Emergencies,” in Pediatric Critical Care (Fourth Edition), Fourth Edi., B. P. Fuhrman and J. J. Zimmerman, Eds. Saint Louis: Mosby, 2011, pp. 190–195.

[9] G. FitzGerald, G. A. Jelinek, D. Scott, and M. F. Gerdtz, “Emergency department triage revisited,” Emerg. Med. J., vol. 27, no. 2, pp. 86–92, 2010, doi: 10.1136/emj.2009.077081.

[10] J. S. Hinson et al., “Accuracy of emergency department triage using the Emergency Severity Index and independent predictors of under-triage and over-triage in Brazil: a retrospective cohort analysis,” Int. J. Emerg. Med., vol. 11, no. 1, p. 3, 2018, doi: 10.1186/s12245-017-0161-8.

[11] K. D. Johnson, G. L. Gillespie, and K. Vance, “Effects of Interruptions on Triage Process in Emergency Department: A Prospective, Observational Study,” J. Nurs. Care Qual., vol. 33, no. 4, 2018.

[12] S. Scrofine and V. Fitzsimons, “Triage: The Sorting of Patients,” J. Emerg. Nurs., vol. 40, no. 3, pp. 289–290, 2014, doi: https://doi.org/10.1016/j.jen.2014.03.004.

[13] “Global indicator framework for the Sustainable Development Goals and targets of the 2030 Agenda for Sustainable Development.” United Nations.

[14] L. Sengyee, “How China’s industrial internet is helping to fight COVID-19 | World Economic Forum,” Global Agenda, 2020. [Online]. Available: https://www.weforum.org/agenda/2020/04/china-covid-19-digital-response/. [Accessed: 09-Apr-2020].

[15] “WHO | Nigeria,” WHO, 2020.

[16] A. E. Asakitikpi, “Healthcare Coverage and Affordability in Nigeria: An Alternative Model to Equitable Healthcare Delivery,” in Universal Health Coverage, 2019.

[17] E. Akinkuotu, “Coronavirus: Doctors obtain Abba Kyari’s medical records from UK hospital,” Abuja, 25-Mar-2020.

[18] O. Albahri et al., “Fault-Tolerant mHealth Framework in the Context of IoT-Based Real-Time Wearable Health Data Sensors,” IEEE Access, vol. 7, pp. 50052–50080, 2019.

[19] S. Misbahuddin, J. A. Zubairi, A. R. Alahdal, and M. A. Malik, “IoT-Based Ambulatory Vital Signs Data Transfer System,” vol. 2018, 2018.

[20] M. X. Cicero et al., “Do you see what I see? Insights from using google glass for disaster telemedicine triage,” Prehosp. Disaster Med., vol. 30, no. 1, pp. 4–8, 2015.

[21] S. Moreno, A. Quintero, C. Ochoa, M. Bonfante, R. Villareal, and J. Pestana, “Remote monitoring system of vital signs for triage and detection of anomalous patient states in the emergency room,” in 2016 XXI Symposium on Signal Processing, Images and Artificial Vision (STSIVA), 2016, pp. 1–5.

[22] K. Guk et al., “Evolution of wearable devices with real-time disease monitoring for personalized healthcare,” Nanomaterials, vol. 9, no. 6, 2019.

[23] H. Chong and K. Gan, “Development of automated triage system for emergency medical service,” in International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES), 2016, pp. 642–645.

[24] J. Broach et al., “Usability and Reliability of Smart Glasses for Secondary Triage During Mass Casualty Incidents,” in 51st Hawaii International Conference on System Sciences, 2018, pp. 1416–1422.

[25] C. Sarkar, A. U. S. Nambi, R. V. Prasad, A. Rahim, R. Neisse, and G. Baldini, “DIAT: A scalable distributed architecture for IoT,” IEEE Internet Things J., vol. 2, no. 3, pp. 230–239, 2015.

[26] C. Dupont, T. Bures, M. Sheikhalishahi, C. Pham, and A. Rahim, “Low-cost IoT, Big Data, and Cloud Platform for Developing Countries,” in International Conference on the Economics of Grids, Clouds, Systems, and Services, 2017, pp. 285-299.

[27] “A Mobile Diagnosis Device to Mitigate Pandemics and Infectious Diseases,” 2020. [Online]. Available: https://innovate.ieee.org/innovation-spotlight/diagnosing-infectious-disease/?LT=XPLHL_XPL_2020_LM_XIS_Mobile_Diagnosis_Diseases_Highlight.

[28] S. J. Johnston, M. Apetroaie-Cristea, M. Scott, and S. J. Cox, “Chapter 15 - Applied Internet of Things,” in Internet of Things, R. Buyya and A. [Vahid Dastjerdi], Eds. Morgan Kaufmann, 2016, pp. 277–298.

[29] M. Moshtaghi, C. Leckie, and S. Karunasekera, “Chapter 9 - A framework for distributed data analysis for IoT,” in Internet of Things: Principles and Paradigms, 2016, pp. 163–180.

[30] M. C. Bhalla, J. Frey, C. Rider, M. Nord, and M. Hegerhorst, “Simple Triage Algorithm and Rapid Treatment and Sort, Assess, Lifesaving, Interventions, Treatment, and Transportation mass casualty triage methods for sensitivity, specificity, and predictive values,” Am. J. Emerg. Med., vol. 33, no. 11, pp. 1687–1691, 2015.

Leveraging Artificial Intelligence of Things for Anomaly Detection in Advanced Metering Infrastructures

Reginald Ekene Ogu
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
reginald.ogu@futo.edu.ng

Charles Ikerionwu
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
charles.ikerionwu@futo.edu.ng

Ikechukwu I. Ayogu
Dept. of Computer Science
Federal University of Technology, Owerri
Owerri, Nigeria
ignatius.ayogu@futo.edu.ng

***Abstract*—The integration of more sensory and actuation components to the Smart Grid produces high volume of data. Consequently, this big data stretches the transmission, processing, and storage capabilities of the Smart Grid infrastructures. The vulnerability of advanced metering infrastructures (AMIs) is on the rise, as more devices are connected to the Internet these days. The aforementioned realities have continued to necessitate a debate on the future of cloud-centered artificial intelligence (AI) services for latency-sensitive user-centric IoT applications. It is rapidly becoming necessary to leverage on the applicability of EdgeAI directly on IoT sensory nodes involved in energy metering. This paper proposes the applicability of Artificial Intelligence situated on smart meter, to perform micro analytics at the edge of AMI networks: Artificial Intelligence of Things. Therefore, a functional AMI model based on IoT and EdgeAI is presented herein. Additionally, an integration architecture for the anticipated Smart Grid based on IoT and EdgeAI is presented. On implementation, the proposed model would provide high-performance analytics and Edge computing capabilities to enable AMIs initiate instant data check at the source and relay relevant real-time data to the Utility through the Internet.**

***Keywords*— Edge computing, Energy Consumption, Intelligent systems, Internet of Things, Smart Grids**

I. INTRODUCTION

Smart meters (SM) are a key element in advanced metering infrastructures (AMI). SMs are prone to manipulation by some consumers for self-gains, at the detriment of the utility companies. The intent of such manipulative activities can vary, but the bottom line is usually to evade commensurate payment for energy consumed [1], [2]. The challenges associated with electricity theft increased significantly with the transition from the classical meters to SMs in smart grids [3]–[6]. Electricity theft remains a major challenge for the operators of smart grids [7]. It is the principal form of non-technical losses (NTL) encountered in smart grids [3], [8]. The spate of NTL due to compromised SM continues to draw the attention of all stakeholders – including researchers, and as such, there has been a rapid growth in the development and deployment of energy state-of-the-art monitoring infrastructure. Given the huge capital requirements for AMIs and smart grids, it is imperative to minimize NTLs since it degrades the capacity of the power companies to continually remain in business [2], [9]–[11].

Through embedded system technologies, SMs can record detailed electricity consumed by a customer and communicate the same to a designated sectoral or central system [10], [12]. A typical AMI often aggregates more than a 100k SMs that are often managed by the main systems. Since data is continuously accumulated and exchanged, the volume can quickly and expectedly grow huge and pose performance threats [13]. In [14], the researchers concluded that this scenario plays out in fog and cloud computing based AMIs.

The increasing sophistication of modern smart grids and AMIs, especially with Internet of Things (IoT) integrations create some interesting challenges to the status quo. With the increase in the integration of 'things', more data are captured, and thus, more pressure on the transmission, processing and storage subsystems in AMIs. This reality has continued to necessitate a debate on the future of cloud-centered artificial intelligence (AI) services for latency-sensitive user-centric IoT applications [15]. It is instructive to contemplate harnessing the suitability and potential benefits of edge-AI for monitoring of AMI components, including consumption data. Furthermore, with less transfer of sensitive data between devices and the cloud, there has been an increased potential to mitigate security threats in AMIs [16].

The popularity of Edge computing on IoT has been characterized by computation at the source of data. It encourages the processing of data at the sensory nodes to free up the cloud for more general-purpose activities while allowing the SMs to perform faster, and reduce latency by performing more localized data processing operations on the edge devices [17], [18]. Given that artificial intelligence techniques are not unfamiliar in the domain of anomaly detection in smart grids, it is theoretically possible to achieve good results with edge AI by seeking to use lightweight, non-computationally intensive AI and machine learning techniques on the resource-constrained processors. This paper, therefore, proposes an extension of SMs with edge computing capabilities and AI for anomaly detection in AMIs.

II. LITERATURE REVIEW

Although improvements have been recorded from Mechanical to Smart metering, electricity theft remains a classical impediment for the growth of the sector. Amongst the suggested mitigating factors, smart meters have undergone key processes such as de-pseudonymization, which provides data security and consumers' privacy [10] and formalization of metering requirement that allows the regulatory agency to enforce standards and supervise the smart meter production, from prototype to market [19]. The introduction of AMI has played a significant role in mitigating electricity theft in households and large-scale utility establishments such as Smart Grids. By implementing AMI, research findings suggest an improved system reliability and electricity

monitoring [20]. However, researchers and practitioners have been improving on the existing AMI by introducing different technologies and tools to improve the energy fraud detection rate. These technologies provide quick information gathering and analysis from large scale datasets involving thousands of smart meters from utility companies to forecast varying factors affecting electricity consumption, such as building's age, size and weather for quick decision making [21].

The work of [3] proposed a 3-tier GUI-based NTL detection algorithm that combines three sources of measurement to draw inference through triangulation. On implementation, utility organizations stand to benefit from recovery of NTL revenue at real-time. A related study indicates that the use of Principal Component based Theft Detection enhances the detection rate of energy theft [22]. To calculate Mahalanobis distance, the difference between historical consumption data and the transformed testing samples is inferred. These intricacies are captured in a performance model, primarily to predict resource usage, throughput and response time especially in time-critical tasks [13]. A fraud detection system (FDS) that focuses on differences between energy supplied from the smart grid and energy recorded in the smart meter was proposed in [23]. In Sensor based FDS an embedded smart meter in grid serves as a sensor for monitoring the distribution grid, meters, and communication network [16], [24]. For example, at the smart grid, fraud alert could be triggered at the slightest discrepancy in energy consumption before and after a specific period at the consumer's residence.

Earlier research effort indicate that consumers satisfaction have been considered through the application of AI in Demand Side Management prevalent in smart homes[15]. Specifically, artificial neural networks (ANNs) could be applied to perform load monitoring through the analyses of data emanating from the sensors nodes instead of waiting for the data transmitted from the cloud – client's server, which involves further analysis. Likewise, the use of machine learning by embedding mathematical algorithms to train big data collected over a period could reduce the hackers' menace. In this line, the work of [16] took the advantage of support vector machine to predict consumers' consumption profile, which triggers an alert whenever a discrepancy occurs. To detect electricity theft, researchers have introduced a wide array of f research efforts including machine learning [25], [26]. However, the applications are not at the edge metering nodes.

AMI is constantly exposed to cyber-attacks because of the communication network that prevails through the internet platform, and hackers have always utilized this opportunity to the maximum. To tackle the challenges posed by hackers, [4] proposed an integration of Vector-based algorithm, Honesty-based algorithm, and Kullback-Leibler distance algorithm within the principles of Swarm Intelligence. The procedure adopted an iteration method to sieve out a compromised meter within a swarm of smart meters. Some AMI employed clustering algorithm to aggregate neighboring smart meters in the neighborhood and perform cumulative analysis on smart meter readings [27], [28]. Similarly, [8] proposed a "Fast NTL Fraud Detection (FNFD) and varication scheme that utilizes Recursive Least Square (RLS) to model adversary behavior". In this model, a centralized monitoring approach was adopted, where several meters are instituted within the community and under one observatory center.

The work of [29] built from the scratch a Generative Adversarial Network (GAN) to mimic Neural Network (NN) trained real data set purposely to unleash a poison attack on AMI that is aimed at hiding energy theft. Findings suggest that AI environment is susceptible to been cheated by presenting fake dataset especially in a cluster of smart meters. Extant literatures suggest that most antifraud algorithms are developed with machine learning tools. However, in [30], it was suggested that machine learning based algorithms are fraught with challenges, which affects the outcome of the predictions. These challenges are noticeable in Data Imbalance, Big Data (volume, velocity, variance), and Feature Description and Selection. Thus, it is envisioned that timely fraud detection using edge-AI and IoT could mitigate electricity theft.

III. Structural Model of AIoT Enabled Smart Meter

To confer edge computing capabilities on the existing SMs, the existing design requires some careful modifications, especially the control chip. Although most current day SMs have the capability of connecting to the internet, computations on the consumption and other data generated at the nodes are still done at the fog and cloud levels. This is because these meters are not capable of edge analytics. To overcome these shortcomings, this study proposes to replace the core of the SM with a combination of the Arm Cortex-M55 processor and Ethos-U55 Neural Processing Unit (NPU) to bring in edge AI analytics on the metering nodes. The basic schematic for the modified SM is depicted in Fig. 1.

A Rogowski coil (RC) is proposed as the current (I) sensory element of the system. A voltage (V_S) is induced across the terminals of the coil by an alternating magnetic field produced by the current in the primary conductor (I_P). The output voltage of RC is not restricted for saturation but not for a large primary current. This is because of its non-magnetic core. This means that the RC produces a voltage that is proportional to the rate of change of the current in the conductor. The output voltage of the RC is computed using (1).

$$V_S(t) = -M\frac{dI_p(t)}{dt} \qquad (1)$$

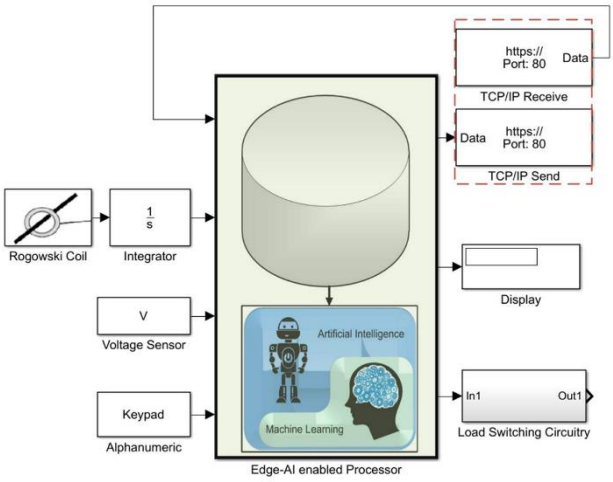


Fig. 1. Model of an AIoT Smart Meter.

The output voltage (V_S) of the RC is proportional to the

derivative of the instantaneous primary current (I_p). Hence, the need to retrieve the original current signal with an integrator. Its usefulness is noticeable where the primary objective is power measurement – the shift in Rogowski current output is calculated by noting the difference between current and voltage. For the voltage measurement, ZMPT101B sensor is proposed. An alphanumeric keypad is integrated into the system, to enable the user make inputs to the meter such as entering a subscription voucher. A Liquid Crystal Display (LCD) is proposed to be used as a user interface.

A combination of the Arm Cortex-M55 processor and Ethos-U55 Neural Processing Unit (NPU) is proposed to bring in edge AI to the meter. This combination forms the heart of the proposed SM design. To equip the SM with IoT capability, WINC1500 low power Integrated Circuit that is based on the IEEE 802.11 technology is proposed with ECC508A chip providing security to the entire system. Solid State Relay (SSR) is proposed to be the switching device that can connect and disconnect the loads to the grid.

IV. A Taxonomy of Feasible Edge Analytics Techniques in Resource Constrained Devices

To simulate how AI can be used to detect anomaly in user energy consumption for theft prevention, a dataset generated from consumers' SMs are used. For example, a household electricity consumption dataset such as the one from the UCI Machine Learning Repository by [31], is adopted. The general Minkowski distance metric of a Normed vector space of (2) is manipulated to estimate or compute the similarity or distance between data instances depending on the value of p. when p =1 in which case Manhattan distance is computed, when p = 2, Eclidean distance (2) is computed and when p = p = ∞, Chebychev distance is computed.

$$d(x,y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{1/p} \quad (2)$$

$$d(x,y) = \left(\sum_{i=1}^{n} |x_i - y_i|^2\right) \quad (3)$$

where:
n = number of variables,
x_i and $y_i$are the variables.

Subsequently, a suitable machine learning model which uses any of these or other suitable distance metric can be employed to map the dataset into two clusters normal and fraudulent consumption. For instance, K-means is handy; in the current case a two-centroid initial cluster would suffice. By this, a given instance is assigned to its nearest cluster center.

V. Proposed Integration Framework

Based on the concept presented in Fig. 1, this section presents the design of an IoT- Edge AI based electricity meter. The key features of the system are:

A. Sensing of electrical parameter to determine the energy consumption of a consumer.

B. Actuation/load control, to promptly disconnect a detected fraudster from the grid.

C. Communication with the power company using IoT on the status of the meter.

D. AI computation and subsequent identification of anomaly.

In view of these features, the conceptual framework of an Edge-AI based Advanced Metering Infrastructures is shown in Fig. 2.

The framework has three interdependent layers: the physical layer, the network layer and the cloud layer. The embedded systems metering nodes and user devices such as PCs and mobile phones make up the physical layer while the network layer covers the gateway that connects the physical layer to the cloud layer. The Cloud layer is the ubiquitous Internet.

For data exchange between the meter and the cloud, popular protocols such as HTTP[1] and MQTT[2] are proposed depending on the location. While HTTP can be employed in locations with good access to the Internet, MQTT can be applied in developing countries with poor quality of Internet services. To make the connection more reliable, auxiliary protocol such as the Constrained Application Protocol (CoAP) is combined with MQTT to ensure maximum data exchange.

While IEEE 802.11x based communication techniques can be adopted for the developed countries, the IEEE 802.15.4 based communication techniques are proposed for this application in developing countries. This is because of the high-power demand of IEEE 802.11x based technologies. Technologies like Sigfox and LoRA are considered efficient in this application based on their low power demand while being able to travel long distances. These technologies are IPv6 over Low-Power Wireless Personal Area Networks (6LowPAN) capable. Hence, able to transmit and receive up to 250 kbps in distance >150m.

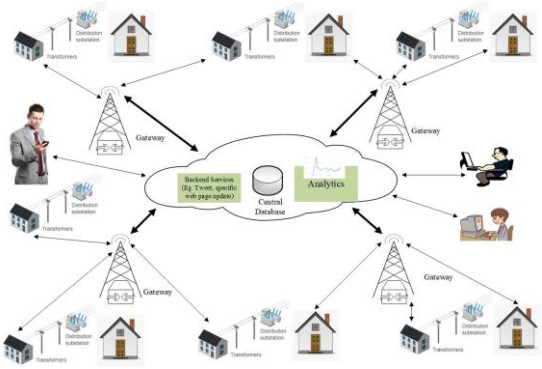


Fig. 2. Architectural model of an AIoT Advanced Metering Infrastructure.

[1] Hypertext Transfer Protocol

[2] Message Queuing Telemetry Transport

VI. Discussion

Due to increasing volume of Big Data and the quest for real-time response, Edge computation on the IoT ecosystem is becoming popular. AI capabilities are moving closer to the point of data collection. This paradigm shift is proving to mitigate the shortfalls of the conventional cloud computing [17]. Considering the high-level characteristics and computational requirements of an edge device in [17], the proposed IoT and edgeAI based AMI is envisioned to be right provisioned, judging from its basic components. By this, the system satisfies its functional requirements of measuring the energy consumption of a consumer. Also, it is expected that the system will not waste resources by incurring unnecessary overheads during its operation.

As with Industrial Internet of Things (IIoT) [32], the primary objective of the proposed IoT-Edge AI metering infrastructure is situated within the need to rapidly monitor and detect shifts in electricity consumption data to spot deviations from expected behaviour and forestall or mitigate electricity theft. Edge devices, gateways and data centers form the ecosystem within which AI can be used to transform, analyze, visualize and embed data from IoT nodes notwithstanding the setup, in fog or in the cloud [32], [33].

According to [32], the convergence of IoT and AI goes beyond the sensors, cameras, network infrastructure and computers that informs the intelligence of IoT. This convergence ensures that intelligence is deployed where it is needed most (in this case; at the sensory node – the electricity meter). Going by the above, real-time data analytics could be achieved. The IoT-Node AI will preserve the integrity of energy consumption data because data manipulation will be done at the metering systems. This can be achieved by using a variety of AI methodologies to process information contained in data streams for the purposes of detecting anomalous patterns and to resolve data issues.

VII. CONCLUSION

The applicability of Artificial Intelligence (AI) at the edge in AMIs has been proposed in this paper. The proposal describes the embedding of AI in the Advanced Metering Infrastructures to provide a way to rapidly and accurately identify anomalous patterns in energy consumption data. This has a potential to foster early detection and subsequent prevention of electricity theft.

In addition, a functional model of an Advanced Metering Infrastructure based on IoT and edgeAI is presented. Finally, an integration architecture was presented, to show an overview of the anticipated current day Smart Grid. In the architecture, peculiarities of developing countries such as poor access to the Internet were considered. The proposed system will provide high-performance analytics and Edge computing capabilities to enable AMIs act on the data instantaneously, at the source, without delay.

References

[1] M.H. Rashid, AMI Smart Meter Big Data Analytics for Time Series of Electricity Consumption, in: 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng., IEEE, New York, 2018: pp. 1771–1776. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00267.

[2] R.E. Ogu, G.A. Chukwudebe, Development of a Cost-Effective Electricity Theft Detection and Prevention System based on IoT Technology, in: IEEE 3rd Int. Conf. Electro-Technology Natl. Dev. Dev., IEEE, 2017: pp. 756–760.

[3] K.K. Kee, S.M.F. Shahab, C.J. Loh, Design and development of an innovative smart metering system with GUI-based NTL detection platform, in: 4th IET Clean Energy Technol. Conf. (CEAT 2016), IET, Kuala Lumpur, 2016: pp. 1–8. https://doi.org/10.1049/cp.2016.1293.

[4] P.S. Paikrao, R. Bose, Anomaly detection algorithms for smart metering using swarm intelligence, in: Annu. Int. Conf. Mob. Comput. Networking, MOBICOM, 2018: pp. 3–8. https://doi.org/10.1145/3243318.3243319.

[5] J. Zheng, D. Gao, L. Lin, Smart meters in smart grid: An overview, in: 5th IEEE Conf. Green Technol., 2013: pp. 57–64.

[6] X. Xiong, Z. Cheng, G. Chen, Y. Zhang, M. Fu, M. Liu, A SVM-based fraud detection system using short-lived electricity consumption data, ACM Int. Conf. Proceeding Ser. (2019). https://doi.org/10.1145/3386415.3387061.

[7] C. Carquex, C. Rosenberg, Multi-timescale electricity theft detection and localization in distribution systems based on state estimation and PMU measurements, in: 9th ACM Int. Conf. Futur. Energy Syst., 2018: pp. 282–290. https://doi.org/10.1145/3208903.3208908.

[8] W. Han, Y. Xiao, FNFD: A fast scheme to detect and verify non-technical loss fraud in smart grid, WTMC 2016 - Proc. 2016 ACM Int. Work. Traffic Meas. Cybersecurity, Co-Located with Asia CCS 2016. (2016) 24–34. https://doi.org/10.1145/2903185.2903188.

[9] P. Arjunan, H.D. Khadilkar, T. Ganu, Z.M. Charbiwala, A. Singh, P. Singh, Multi-user energy consumption monitoring and anomaly detection with partial context information, in: BuildSys 2015 - Proc. 2nd ACM Int. Conf. Embed. Syst. Energy-Efficient Built, ACM, 2015: pp. 35–44. https://doi.org/10.1145/2821650.2821662.

[10] M. Jawurek, M. Johns, K. Rieck, Smart metering de-pseudonymization, in: ACSAC '11 Dec. 5 - 9, Orlando, Florida USA, 2011: pp. 227–236. https://doi.org/10.1145/2076732.2076764.

[11] Y. Kang, X. Wang, X. Cao, Y. Zhou, Z. Lai, Y. Li, X. Zhang, W. Geng, Detecting anomalous users via streaming data processing in smart grid, ACM Int. Conf. Proceeding Ser. (2018) 14–20. https://doi.org/10.1145/3230876.3230893.

[12] Y. Liu, S. Hu, T. Ho, Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks, in: IEEE/ACM Int. Conf. Comput. Des., IEEE, San Jose, CA, 2014: pp. 183–190. https://doi.org/10.1109/ICCAD.2014.7001350.

[13] J. Kroß, A. Brunnert, C. Prehofer, T.A. Runkler, H. Krcmar, Model-based performance evaluation of large-scale smart metering architectures, in: 4th ACM/SPEC Int. Work. Large-Scale Testing, Conjunction with ICPE 2015, 2015: pp. 9–12. https://doi.org/10.1145/2693182.2693184.

[14] A. Metwaly, J.P. Queralta, V.K. Sarker, T.N. Gia, O. Nasir, T. Westerlund, Edge computing with embedded AI: Thermal image analysis for occupancy estimation in intelligent buildings, ACM Int. Conf. Proceeding Ser. (2019) 1–6. https://doi.org/10.1145/3372394.3372397.

[15] Y.-Y. Chen, Y.-H. Lin, C.-C. Kung, M.-H. Chung, I.-H. Yen, Design and Implementation of Cloud Analytics-Assisted Smart Power Meters Considering Advanced Artificial Intelligence as Edge Analytics in Demand-Side Management for Smart Homes, Sensors (Basel). 19 (2019) 1–26. https://doi.org/10.3390/s19092047.

[16] A. Amara Korba, N. El Islem Karabadji, Smart Grid Energy Fraud Detection Using SVM, Proc. - ICNAS 2019 4th Int. Conf. Netw. Adv. Syst. (2019). https://doi.org/10.1109/ICNAS.2019.8807832.

[17] T. Adegbija, R. Lysecky, V.V. Kumar, Right-provisioned IoT edge computing: An overview, in: ACM Gt. Lakes Symp. VLSI, GLSVLSI, 2019: pp. 531–536. https://doi.org/10.1145/3299874.3319338.

[18] B. Chun, B. Oh, C. Cho, D. Lee, Design and implementation of lightweight messaging middleware for edge computing, ACM Int. Conf. Proceeding Ser. (2018) 170–174. https://doi.org/10.1145/3284516.3284535.

[19] A. Fuchs, S. Gürgens, D. Weber, C. Bodenstedt, C. Ruland, Formalization of Smart Metering requirements, ACM Int. Conf. Proceeding Ser. (2010). https://doi.org/10.1145/1868433.1868439.

[20] I. Shin, J.H. Huh, Y. Jeon, D.M. Nicol, A distributed monitoring architecture for AMIs: Minimizing the number of monitoring nodes and enabling collided packet recovery, Proc. ACM Conf. Comput. Commun. Secur. (2013) 35–40. https://doi.org/10.1145/2516930.2516948.

[21] S. Iyengar, S. Lee, D. Irwin, P. Shenoy, Analyzing energy usage on a city-scale using utility smart meters, in: 3rd ACM Conf. Syst. Energy-

Efficient Built Environ. BuildSys 2016, 2016: pp. 51–60. https://doi.org/10.1145/2993422.2993425.

[22] S.K. Singh, R. Bose, A. Joshi, Energy theft detection in advanced metering infrastructure, IEEE World Forum Internet Things, WF-IoT 2018 - Proc. 2018-Janua (2018) 529–534. https://doi.org/10.1109/WF-IoT.2018.8355148.

[23] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, I. Chueiri, A Tunable Fraud Detection System for Advanced Metering Infrastructure Using Short-Lived Patterns, IEEE Trans. Smart Grid. 10 (2019) 830–840. https://doi.org/10.1109/TSG.2017.2753738.

[24] F. Fathnia, M.H.J.D. Bayaz, Anomaly Detection in Smart Grid with Help of an Improved OPTICS Using Coefficient of Variation, in: Iran. Conf. Electr. Eng. (ICEE), IEEE, 2018: pp. 1044–1050. https://doi.org/10.1109/ICEE.2018.8472534.

[25] V. Ford, A. Siraj, W. Eberle, Smart grid energy fraud detection using artificial neural networks, in: 2014 IEEE Symp. Comput. Intell. Appl. Smart Grid, 1-6, 2014: pp. 1–6.

[26] C. Cody, V. Ford, A. Siraj, Decision tree learning for fraud detection in consumer energy consumption, in: 2015 IEEE 14th Int. Conf. Mach. Learn. Appl., IEEE, 2015: pp. 1175–1179.

[27] Z.A. Baig, A. Al Amoudy, K. Salah, Detection of compromised smart meters in the Advanced Metering Infrastructure, 2015 IEEE 8th GCC Conf. Exhib. GCCCE 2015. (2015) 1–4. https://doi.org/10.1109/IEEEGCC.2015.7060073.

[28] R. Blom, M. Korman, R. Lagerström, M. Ekstedt, Analyzing attack resilience of an advanced meter infrastructure reference model, in: 2016 Jt. Work. Cyber- Phys. Secur. Resil. Smart Grids, IEEE, Vienna, 2016: pp. 1–6. https://doi.org/10.1109/CPSRSG.2016.7684095.

[29] F. Marulli, C.A. Visaggio, Adversarial deep learning for energy management in buildings, Simul. Ser. 2019-July (2019).

[30] A. Maamar, K. Benahmed, Machine learning techniques for energy theft detection in AMI, ACM Int. Conf. Proceeding Ser. (2018) 57–62. https://doi.org/10.1145/3178461.3178484.

[31] D. Dua, C. Graff, UCI Machine Learning Repository, (2017). http://archive.ics.uci.edu/ml.

[32] SAS, The Artificial Intelligence of Things, 2018. https://www.sas.com/en/whitepapers/artificial-intelligence-of-things-110060.html.

[33] X. Wang, Y. Han, V.C.M. Leung, D. Niyato, X. Yan, X. Chen, Edge AI, Springer, 2020.

A Novel Smart CBT Model for Detecting Impersonators using Machine Learning Technique

John-Otumu A. M.
Dept of Information Technology
Federal University of Technology
Owerri, Nigeria.
adetokunbo.johnotumu@futo.edu.ng

Nwokonkwo O. C.
Dept of Information Technology
Federal University of Technology
Owerri, Nigeria.
obi.nwokonkwo@futo.edu.ng

Izu-Okpara I
Dept of Information Technology
Federal University of Technology
Owerri, Nigeria.
floxy83@yahoo.co.uk

Dokun O. O.
Dept of Information Technology
Federal University of Technology
Owerri, Nigeria.
oyewoledokun1@gmail.com

Konyeha Susan
Dept. of Computer Science
University of Benin
Benin city, Nigeria
susan.konyeha@gmail.com

Oshoiribhor E. O.
Dept. of Computer Science
Ambrose Alli University
Ekpoma, Nigeria
emmaoshor2001@gmail.com

***Abstract*— The computer-based testing (CBT) platforms for conducting mass-driven examinations over computer networks in order to eliminate certain challenges such delay in marking, misplacement of scripts, impersonation, monitoring and so on associated with the conventional Pen and Paper Type (PPT) of examination has also been seriously bedeviled with the same issue of impersonation commonly associated with the PPT system. The existing CBT systems relies solely on the CCTV system for monitoring people passively and the human invigilators (Proctors) for going round the examination halls in order to physically confirm the students face against their pictures on their respective system dashboard which takes so many time and effort just to screen people against impersonating and yet impersonation is on the increase with CBT system. The propose Smart CBT model integrates an intelligent agent assessor to the existing CBT model using K-Nearest Neighbor (KNN) machine learning technique for detecting a likely case of impersonation threat considering the considering the level of accuracy and response time in answering the questions the agent delivers to the students shortly before the actual examination can commence. A total of 3,083 dataset was gathered, and 80% (2,466) of the dataset was used for training the model, while 20% (617) dataset was used in testing the model to enable the model detect unseen data correctly. Results revealed that 99.99% accuracy rate, precision, recall and f-score were obtained. The propose Smart CBT model is recommended for all tertiary institutions and commercial CBT software product adoption.**

***Keywords*—** *Smart CBT Model, Online Examination, Intelligence, Machine Learning, Computer Networks*

I. INTRODUCTION

Examination is simply seen as a regular use and standard factor for evaluating students understanding and reasoning capability of a topic he or she was taught [1]. Examination is also discussed as the utmost practice of judging the understanding and skills of an individual under a particular condition [2-3]. Ismail and Shami [4], is of the opinion that examinations can also control the amount of which instructive purposes have stayed accomplished as well as the extent to which enlightenment has been establishments in order to assist the public in general.

Recently, the swift improvement of Information and Communication Technologies (ICT) has shaped a new paradigm-shift for teaching and learning over the Internet and other network environments; which has undeniably compelled a thoughtful change from the conventional pen and paper type (PPT) of examination to Computer-Based Testing (CBT). The CBT can also be referred to as e-Assessment, Computer-Based Examination (CBE), E-Examination, web-based examination, online examination system [4, 5].

The application of information technology (IT) for assessment and related activities has paved way for a well-crafted and engineered CBT platform, which permits instructors and educators to program reviews, questions, experiments and examinations through the Internet and intranet [1-3], [6-7].

The Triple-A model which stands for "Assembling, Administering and Appraising" was proposed as a basic classroom testing system by [8]. The recommendation for the adoption of the Triple-A model as a reference point condition in the development of a standard CBT application was necessitated by [9]. CBT applications can be installed either as a desktop-based application or a web-based application over the Internet or intranet using web-based technologies [10]. The two (2) basic types of CBT applications exist for online examinations: i. Linear-test ii Adaptive-test [1, 6, 17].

CBT systems offer several beneficial benefits in the areas as follows:

(i) Examination can be scheduled at any time and can be done from anyplace [12]
(ii) Improved testing capacity of partakers [13, 18].
(iii) Delivery of very few human resources and reduced paper work [14-15].

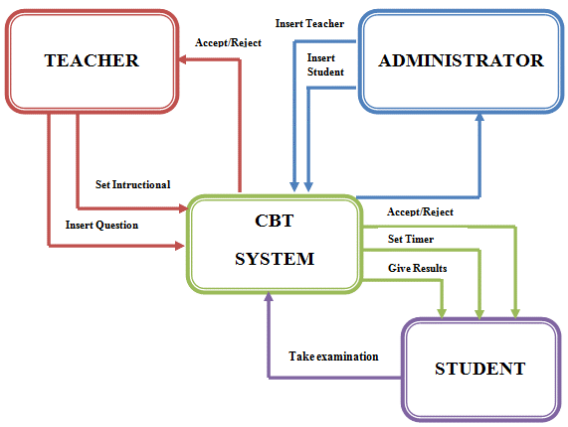


Fig. 1: Existing CBT Platform Data Flow Diagram [1, 5]

CBT platforms are specifically developed for the conduct of mass-driven examinations over computer networks in order to eradicate known challenges such delay in marking, misplacement of scripts, impersonation, monitoring and so on associated with the conventional Pen and Paper Type (PPT) of examination. The existing CBT application uses passive methods such as CCTV and human invigilators (Proctors) to monitor and detect impersonations by physically moving from one system to the other in an examination hall in order to confirm the students' faces against their pictures on their respective system dashboard which takes so much time and effort and at the end very little or nothing is achieved, because many students still impersonate without being detected.

However, this research paper seeks to seriously address the issue of impersonation associated with the existing computer-based testing (CBT) platforms during examinations which is on the increase as noted by [6, 16], in order to proffer a robust and smart CBT platform for the effective conduct of online examinations.

II. RELATED WORKS

This section systematically review and summarizes twenty (20) related works done on CBT product design and development in a tabular form in order to justify the research gap created.

TABLE I: SUMMARY OF RELATED WORKS DONE ON CBT PLATFORMS

S/N	Author	Purpose	Methodologies used	Findings
1	Fagbola, Adigun and Oke [5]	Online examination system	Waterfall model. Microsoft SQL Server 2008, Macromedia Dreamweaver 8.0, and Microsoft Visual Studio 2012 3-Tier architecture	✓ Basic security: username/ password & users privileges. System supports Triple-A model. System lacks resumption capability ✓ System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test
2	Ajinaja [1]	Online examination system	Waterfall model and component based software engineering model. PHP, JavaScript, HTML, MySQL, CSS and XAMP Server. 3-Tier architecture	✓ Basic security: username/ password & users privileges. System supports Triple-A model. System lacks resumption capability ✓ System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test
3	Suleiman and Nachandiya [17]	Online examination system	Agile software Model. PHP, MySQL, JavaScript, CSS, HTML and XAMP Server 3-Tier architecture	✓ Basic security: username/ password & users privileges. System supports Triple-A model. System lacks resumption capability ✓ System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test
4	Omotehinwa and Durojaye [11]	Online examination	Sequence & use case diagrams PHP, HTML, and MySQL 3-Tier architecture	✓ Basic security: username/ password & users privileges. System supports Triple-A model. System lacks resumption capability ✓ System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test
5	Ismail and Soye [3]	Securing Online examination	Biometric fingerprint and Advanced Encryption Standard (AES). Java programming language and MySQL. Sequence and Use case diagrams 3-Tier architecture	✓ Basic security: username/ password & biometric fingerprint, user's privileges and data security using AES. System supports Triple-A model. System lacks resumption capability. System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test
6	Al-Saleem and Ullah [16]	Mitigating threat associated with computer based testing application for online examination	Software Methodology: Not discussed A hybridization of the conventional username/password verification structure with palm-based biometric authentication. 3-Tier architecture	✓ Security basic: username/password + biometric authentication, and user's privileges. System supports Triple-A model. System lacks resumption capability ✓ System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test

TABLE I: SUMMARY OF RELATED WORKS DONE ON CBT PLATFORMS (Continuation)

S/N	Author	Purpose	Methodologies used	Findings
7	Adebayo and Abdulhamid [2]	Mitigating threat associated with computer based testing application for online examination and the integrity of questions and results	Software Methodology: Not discussed Security: Biometric fingerprint technology, username/password and cryptographic technique. Java Applet, HTML, PHP, and MySQL. 3-Tier architecture	✓ Basic security: username/ password + biometric authentication + cryptography and users rights/privileges ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
8	Kuyoro et al [6]	Web-based online examination system	Waterfall model, Cascading Style Sheets (CSS), JavaScript, PHP, HTML, MySQL and WAMP Server 3-Tier architecture	✓ Basic security: username/ password & users privileges only ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks multi-level security measures. ✓ System lacks is not smart to detect impersonation. ✓ The CBT-type is linear-test
9	Oluwole [20]	Desktop-based online examination system	Software Methodology: Not discussed Java programming language MySQL 3-Tier architecture	✓ Basic security: username/ password & users privileges only ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
10	Zheming et al [21]	Novel electronic examination system	Software Methodology: Not discussed Distributed Component Object Module Browser/server framework technologies Ajax, PHP, HTML, MySQL, IIS 4.0 Cryptographic function to secure transmission 3-Tier architecture	✓ Basic security: username/ password & users privileges. ✓ System supports questions encryption ✓ System lack randomization of questions/distribution choice & resumption capability ✓ System supports the Triple-A model. ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ CBT-type is linear-test
11	Yuan-Lung et al [22]	A web-based online examination system	Software Methodology: Not discussed ▪ Visual Basic Script in Active Server Page (ASP), Microsoft Access ▪ Microsoft Windows 2000 O.S 3-Tier architecture	✓ Basic security: username/ password & users privileges only ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
12	Indoria et al [23]	A web-based online examination system	Software Methodology: Not discussed ▪ ASP.NET, VB.NET, Microsoft Access ▪ MS-Windows 95/98/2000/NT 3-Tier architecture	✓ Basic security: username/ password & users privileges only ✓ System cannot generate random questions ✓ Teachers cannot login directly to the system ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test

TABLE I: SUMMARY OF RELATED WORKS DONE ON CBT PLATFORMS (Continuation)

S/N	Author	Purpose	Methodologies used	Findings
13	Rashad et al [24]	Arabic Web-based Examination management system	Software Methodology: Not discussed ▪ AJAX. PHP, HTML. MySQL 3-Tier architecture	✓ Basic security: username/ password & users privileges ✓ System support multiple questions type generation. ✓ System supports instructors direct login to the system ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks Random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
14	Henke [25]	Web-based Test, Examination and Assessment System (WETAS)	Software Methodology: Not discussed Java Applet, PHP 3-Tier architecture	✓ Basic security: username/ password & users privileges ✓ System supports multiple questions type generation. ✓ Supports the Triple-A model ✓ Supports eLearning. ✓ System lacks resumption capability ✓ System lacks random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
15	Ayo et al [19]	A model for electronic examination system	Software Methodology: Not discussed 3-Tier architecture	✓ Basic security features: username/ password & users privileges ✓ System supports multiple questions type generation. ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
16	Akinsanmi et al [27]	Web-based examination system	Software Methodology: Not discussed ASP.NET web server, C#, ADO.NET, Microsoft SQL Server 3-Tier architecture	✓ Basic security features: username/ password & users /privileges ✓ System supports multiple questions type generation. ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test

TABLE I: SUMMARY OF RELATED WORKS DONE ON CBT PLATFORMS (Continuation)

S/N	Author	Purpose	Methodologies used	Findings
17	Tasci et al [26]	Online examination system	Software Methodology: Not discussed Architecture: 3-Tier	✓ Basic security features: username/ password & users rights/privileges ✓ System supports multiple questions types generation ✓ System supports the Triple-A model. ✓ System supports intelligent agent to detect problems such as shortage of time ✓ System lacks resumption capability ✓ System lacks multi-levels security measures. ✓ System is not smart to detect impersonation. ✓ CBT-type is linear-test
18	Qiao-fang [28]	Online examination system	Software Methodology: Not discussed JSP, JavaBean, Tomcat, JavaScript, 3-Tier architecture	✓ Basic security features: username/ password & users privileges ✓ System supports multiple questions type generation such as Yes/No, MCQ, Fill-in gaps, numeric and essay questions ✓ System supports instructors direct login to the system ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
19	Adewale et al [29]	Web-based online examination system	Software Methodology: Not discussed VB.NET, ASP.NET, 3-Tier architecture	✓ Basic security features: username/ password & users privileges. ✓ System supports multiple questions type generation. ✓ System lacks direct login of lecturers to the system ✓ System supports the Triple-A model. ✓ System lacks resumption capability ✓ System lacks random questions generation & random choice distribution ✓ System lacks multi-level security measures. ✓ System is not smart to detect impersonation. ✓ The CBT-type is linear-test
20	Mohammed and Maysam [30]	Online Examination System with Resumption and Randomization Capabilities	Software Methodology: Spiral Model Java programming language and Derby database Application-based Client/Server architecture	✓ Basic security features: username/ password & users privileges ✓ System lacks multiple questions type generation. ✓ System supports the Triple-A model. ✓ System supports multi-instructor login ✓ Systems supports resumption capability ✓ System supports random question selection, distribution and choices selection. System lacks multi-level security measures. System is not smart to detect impersonation. The CBT-type is linear-test

II. METHODOLOGY

This section describes the different methods used in achieving the design and development of the Smart CBT prototype model.

(a) Data Collection Technique:

The following data collection techniques were used in gathering information about the propose system:

(a) Key Information Interview Technique (KIIT) for interviewing seasoned expert in the IT industry.

(b) Observation of existing industry-based CBT software products such as Moodle LMS and JAMB CBT system.

(c) Download of published articles on CBT systems from Open Journal Access for critical examination.

(d) Download of Dataset from online repository for training and testing the developed Smart CBT model.

(b) Development environment

The development environment used in actualizing the Smart CBT are as follows:

(a) Visual Studio Code: was used in coding the entire Web Platform (HTML/CSS, PHP and JavaScript)

(b) Jupyter Notebook: was used in executing the Python language used in the dataset preparation, preprocessing and algorithm evaluation.

(c) XAMPP: this serves as the web server to host the entire platform on a local host.

(c) Software methodology adopted

Software methodology can be seen as a software life cycle for developing quality software product from the beginning to the end. The agile software model was adopted in this case because it can perform tactic learning requirements and evolves proffering solutions via organized group efforts and users. The model also delivers quality advantages such as timely product delivery, adaptive design, evolutionary enhancement, and insistent enrichment. Finally, it also encourages supple responses to adjustments. Figure 2 depicts the diagram of an agile software model revealing its different phases.

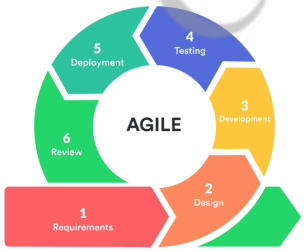


Fig. 2: Agile software model adopted

(d) Propose Smart CBT notation

The propose Smart CBT integrated intelligence into the existing CBT system, and was modeled using the notations as follows:

(i) SCBTP = {CBTS, IAS}

Where:

SCBTP = Smart Computer Based Testing Platform

CBTS = Computer Based Testing System

IAS = Intelligent Agent Services interacting within the CBT environment in carrying out its specific function of detecting impersonators using KNN machine learning technique.

(e) Propose system architecture

The system architectural diagram shows the blueprint of the propose Smart CBT model for detecting impersonators during online examinations.

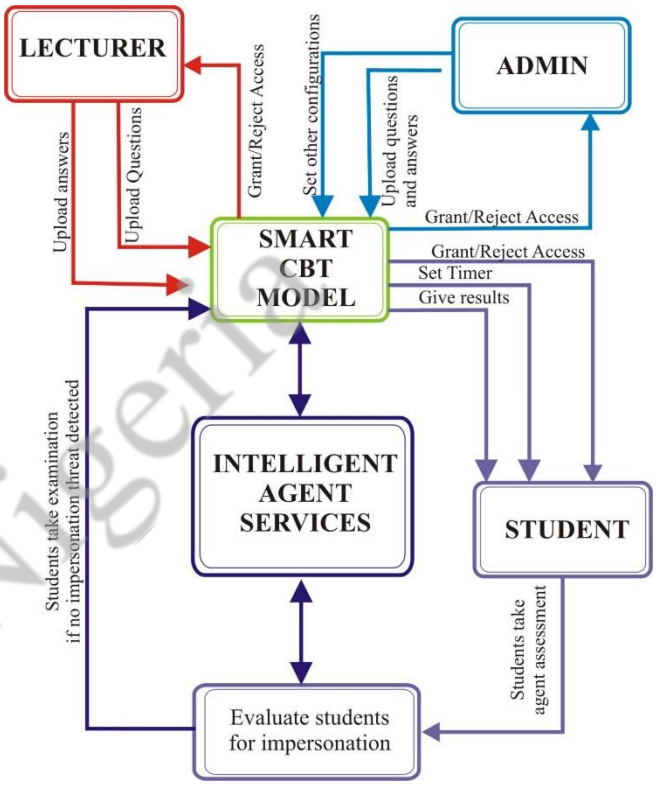


Fig. 3: Propose Smart CBT Architecture

Figure 3 shows the blueprint of the propose Smart CBT model with an intelligent agent service integration using K-Nearest Neighbor machine learning classification algorithm for analyzing and classifying the students for any possible case for impersonation tendencies before giving the students control to write the actual online examination as compared to figure 1 that gives the students direct control to write the online examination without any form of active check by the CBT application.

(f) Algorithm adopted

The choice of adopting the K–Nearest Neighbor (KNN) algorithm for implementing the intelligent agent services responsible for detecting likely impersonation threats was based on its strength such as: it is cheap and easy to build, well suited technique for many class labels and multi-modal classes, and finally, it has a low error rate when compared to naïve bayes technique.

Step 1: For implementing the algorithm, we need a dataset. So during the first step of KNN, we must load the training as well as test data.

Step 2: Next, is to select the value of K i.e. the nearest data points. K can be any integer.

Step 3: For each point in the test data do the following for (**Step 4 to step 7**)

Step 4: Calculate the distance between test data and each row of training data with the help of Euclidean distance equation

$$d = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2 + (z_1 - z_0)^2}$$

Step 5: Based on the distance value, you can now sort them in ascending order.

Step 6: Next, it will choose the top K rows from the sorted array.

Step 7: Now, it will assign a class to the test point based on most frequent class of these rows.

Step 8: End

Fig. 4: K-NN Algorithm adopted

IV. RESULTS AND DISCUSSION

This section discusses the various results obtained from the proposed Smart CBT model.

(a) Responsive interfaces:

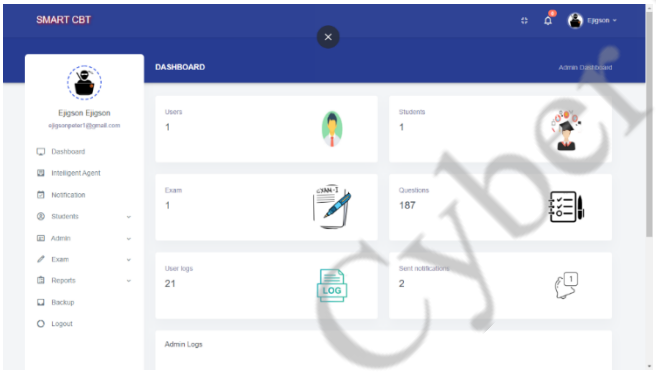


Fig. 5: Admin dashboard interface

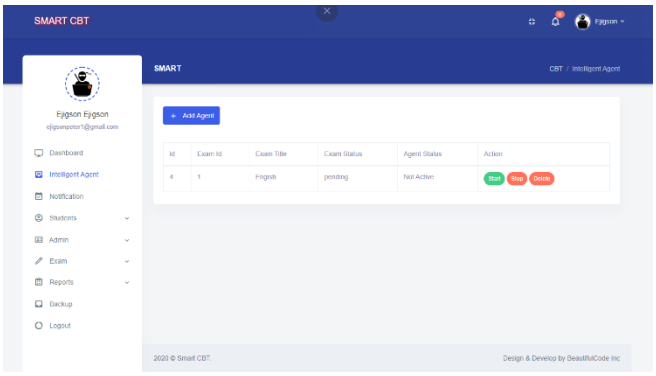


Fig. 6: admin dashboard to activate the agent services

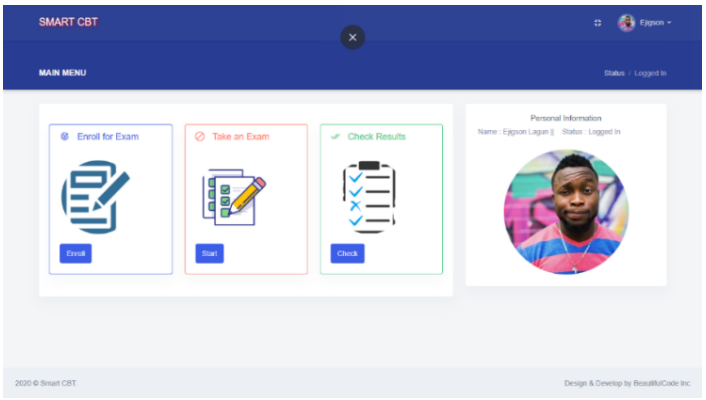


Fig. 7: Student's dashboard

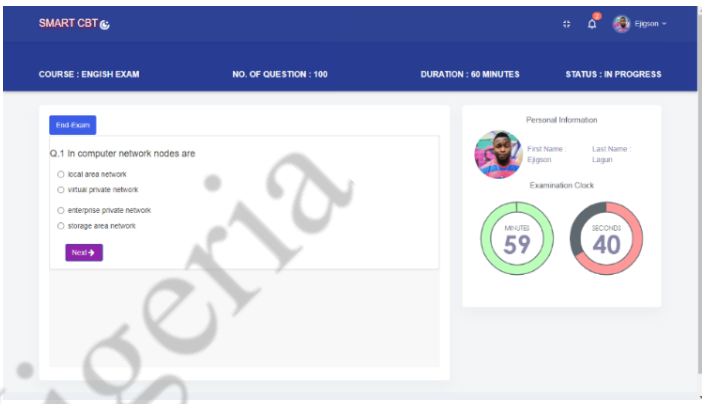


Fig. 8: Student's examination interface

Fig. 9: intelligent agent service loading

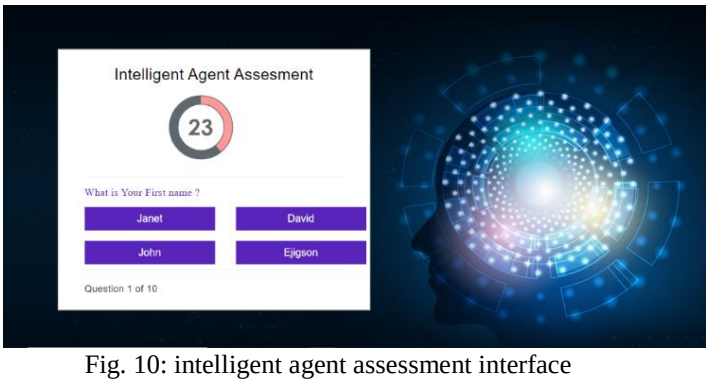


Fig. 10: intelligent agent assessment interface

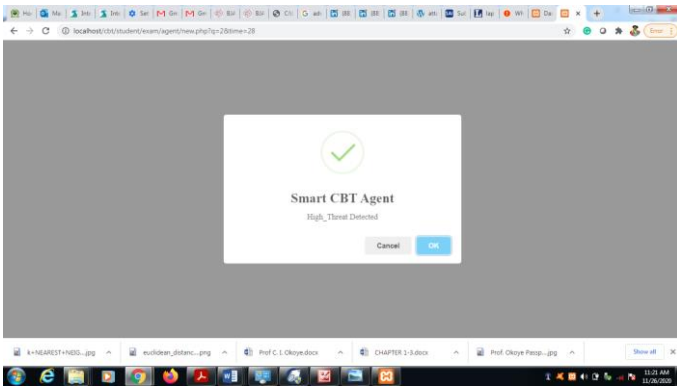


Fig. 11: Screen shot of impersonator detected

(b) Performance evaluation

The performance of the developed model was evaluated using the confusion matrix. The level of classification rate or accuracy rate, recall, precision and f-score were all considered in this evaluation.

TABLE II(a): Confusion matrix

N = 617	Predicted: low_threat	Predicted: no_threat	Predicted: threat
Actual: low_threat	124	0	0
Actual: no_threat	0	77	0
Actual: High_hreat	0	0	416

TABLE II(b): Confusion matrix false alarm breakdown

N = 617	Predicted: low_threat	Predicted: no_threat	Predicted: threat	
Actual: low_threat	TP = 124	FP = 0	FP = 0	124
Actual: no_threat	FN = 0	TP = 77	FN = 0	77
Actual: High threat	FN = 0	FN = 0	TN = 416	416
	124	77	416	

- **Calculation of Classification Rate / Accuracy**

Classification Rate or Accuracy is given by the relation:

$$\text{Accuracy} = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\text{Accuracy} = \frac{(TP + TP + TN)}{(TP + TP + TN + FP + FN + FN + FN + FN+ FN)} \quad \ldots\ldots (2)$$

$$\text{Accuracy} = \frac{(124+77+416)}{(124+77+416+0+0+0+0+0+0)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Accuracy = 1.00

- **Calculation of Recall**

Recall gives us an idea about when it is actually a yes, how often does it predict yes.

$$\text{Recall (No Threat)} = \frac{(TP)}{(TP + FN)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\text{Recall (No Threat)} = \frac{(77)}{(77 + 0)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Recall (No Threat) = 1.00

- **Calculation of Precision**

$$\text{Precision (No Threat)} = \frac{(TP)}{(TP + FP)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\text{Precision (No Threat)} = \frac{(77)}{(77 + 0)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Precision (No Threat) = 1.00

- **Calculation of F-measure:**

$$\text{F1-score (F-Measure)} = \frac{(2 * \text{recall} * \text{precision})}{(\text{recall} + \text{precision})} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\text{F1-score (F-Measure)} = \frac{(2 * 1.0 * 1.0)}{(1.0 + 1.0)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

F1-score (F-Measure) = 1.00

The general evaluation results exposed that the KNN algorithm used in building the intelligent agent services implementation in order to detect impersonators during online examinations was 99.99% accurate.

,

V. CONCLUSION

This research paper critically examined about twenty published articles on CBT systems downloaded from open journal access and also two industry related software products on CBT platform (Moodle LMS and JAMB CBT software), based on the issue of curbing impersonation cases in online examinations that is quite increasing and has become very worrisome with the level of menace introduced in the online examination environment as noted by [6, 16]. The research work adopted the existing CBT model assessment technique based on the standard way for conducting online examination using the Triple-A model (Assembling, Administering and Appraising) as proposed and recommended by [8, 9]. Intelligence was integrated into the existing CBT model using KNN machine learning classification algorithm based on its positive advantages in implementation to enable the model becomes Smart CBT for active monitoring and detection. The developed Smart CBT model can effectively detect likely cases of impersonation during online examination based on the internal control mechanism put in place with a 99.99% accuracy as compared to other CBT systems investigated [1-3, 5-6, 11, 16-17, 19-30], which relies solely on passive techniques such as CCTV system and human invigilators (proctors) as its control mechanism for cheating and impersonation. Future research directions should consider hybridized techniques and Artificial Neural Network (ANN)/Deep Neural Network (DNN) in designing and developing intelligence into the CBT application based on their ability to reason like humans and also in the area of multi-layer security measures integration to CBT platforms for better efficiency.

REFERENCES

[1] M. Ajinaja, "The Design and Implementation of a Computer Based Testing System using Component Based Software Engineering", International Journal of Computer Science and Technology, vol. 8, no. 1, pp. 58 – 65, 2017

[2] O. Adebayo, and S. M. Abdulhamid, "E-Exams System for Nigerian Universities with Emphasis on Security and Results Integrity", International Journal of the Computer, the Internet and Management, vol. 18, no. 2, pp. 1 – 12, 2009.

[3] H, M. Ismail, and B. M. Soye, "Biometric Enabled Computer Based Testing System with Advanced Encryption Standard (AES)", JETIR, vol. 5, no. 8, pp. 1 – 8, 2018.
[4] M. Ismail, and P. A. Shami, "Computer-Based Vs Paper-Based Examinations: Perception of University Teachers", The Turkish Online Journal of Educational Technology, vol. 11, no. 4, pp. 371 – 381, 2012.
[5] T. M. Fagbola, A. A. Adigun, and A. O. Oke, "Computer Based Test (CBT) System for University Academic Enterprise Examination", International Journal of Scientific and Technology Research, vol. 2, no. 8, pp. 336 – 342, 2013.
[6] S. O. Kuyoro, G. U. Maminor, R. U. Kanu, and O. Akande, "The Design and Implementation of a Computer-Based Testing System", Journal of Applied Computation, vol. 1, no. 1, pp. 1 – 7, 2016.
[7] E. Delen, "Enhancing a Computer-Based Testing Environment with Optimum Item Response Time", Eurasia Journal of Mathematics, Science & Technology Education, vol. 11, no. 6, pp. 1457-1472, 2015.
[8] N. E. Gronlund, and R. L. Linn, "Measurement and Evaluation in Teaching", 6th edn, MacMillan, New York, 1990.
[9] T. H. Wang, S. C. Huang, W. L. Wang, and L. Y. Kuo, "Development of a Web-based assessment system: a case study", Proceedings of the 6th Global Chinese Conference on Computers in Education/National Education In-formalization Forum (GCCCE2002), Beijing Normal University, Beijing, China, pp. 385 – 388, 14 – 16 June 2002.
[10] A. R. Taylor, "A Future in the Process of Arrival: Using Computer Technologies for the Assessment of Student Learning", Kelowna, British Columbia: Society for the Advancement of Excellence in Education, 2005
[11] T. O. Omotehinwa and D. S. Durojaye, "Computer Based Test: Security and Results Integrity", International Journal of Computer and Information Technology, vol. 2, no. 2, pp. 324 – 329, 2013.
[12] H. Jeong, "A comparative study of scores on computer-based tests and paper-based tests", Behavior and Information Technology, vol. 33, no. 4, pp. 410 – 422, 2014. doi:10.1080/0144929X.2012.710647
[13] Y. P. Chua and Z. M. Don, "Effects of computer-based educational achievement test on test performance and test takers' motivation", Computers in Human Behavior, vol. 29, no. 5, pp. 1889 - 1895, 2013. doi:10.1016/j.chb.2013.03.008
[14] F. Kaya and E. Delen, "A computer-based peer nomination form to identify gifted and talented students", The Australasian Journal of Gifted Education, vol. 23, no. 2, pp. 29 – 36, 2014.
[15] P. Schatz and J. Browndyke, "Applications of computer-based neuropsychological assessment", Journal of Head Trauma Rehabilitation, vol. 17, no. 5, pp. 395 – 410, 2002.
[16] S. M. Al-Saleem and H. Ullah, "Security Considerations and Recommendations in Computer Based Testing", The Scientific World Journal, Hindawi Publishing Corporation, pp. 1 – 7, 2014
[17] A. Suleiman and N. Nachandiya, "Computer Based Testing (CBT) System for GST Exams in Adamawa State University, Mubi", Asian Journal of Research in Computer Science, vol. 2, no. 1, pp. 1 – 11, 2018
[18] C. P. Newhouse, "Computer-Based Exams in Schools: Freedom from the limitations of paper", Research and Practice in Technology Enhanced Learning, vol. 8, no. 3, pp. 431－447, 2013
[19] C. K. Ayo, , I. O. Akinyemi, A. A. Adebiyi, and U. O. Ekong, "The Prospects of E-Examination Implementation in Nigeria", Turkish Online Journal of Distance Education, vol. 8, no. 4 , pp. 125 – 135, 2007.
[20] O. Oluwole, "Design and Implementation of an Open-Source Computer-Based Testing System with End User Impact Analysis in Africa", International Journal of Modern Education and Computer Science, vol. 8, no. 1, pp. 17 – 24, 2015.
[21] Y. Zhenming, Z. Liang, and Z. Guohua, "A novel Web- Based online examination system for computer science education", 33rd ASEE/IEEE Frontiers in Education Conference.S3F-7-S3F-10. 2003.
[22] Y. Yuan-Lung, H. Tsung-Chih, C. Li-Chaun, "Development of a web Based Online Examination System", East sea management comment, vol. 7, no. 1, pp. 109 – 120, 2005.
[23] V. Indoria, P. Sharma and A. Soni, "Online Examination", International School of Informatics and Management, 2012.
[24] M. Z. Rashad, M. S. Kandil, A. E. Hassan, and M. A. Zaher, "An Arabic Web-Based Examination Management System", International journal of Electrical and Computer Sciences, vol. 10, no. 1, pp. 35 – 41, 2010.
[25] K. Henke, "Web-Based Test, Examination and Assessment System", Advanced Technology for Learning, vol. 4, no. 3, 2007. DOI: 10.2316/Journal.208.2007.3.208-0911
[26] T. Taşci, Z. Parlak, A. Kibar, N. Taşbaşi, and H. I. Cebeci, "A Novel Agent-Supported Academic Online Examination System", Educational Technology & Society, vol. 17, no. 1, pp. 154 – 168, 2014.
[27] O. Akinsanmi, O. T. R. Agbaji, and M. B. Soroyewun, "Development of an E-Assessment Platform for Nigerian Universities", Research Journal Applied Sciences, Engineering and Technology, vol. 2, no. 2, pp. 170 - 175, 2010
[28] Z. Qian-fang, and L. Yong-fei, "Research and development of online examination system", In proceedings of the 2012, 2nd International Conference of Computer and Information Applications, 2012.
[29] O. A. Adewale, T. O. Ajadi, and J. O. Inegbedion, "Perception of learners on Electronic Examination in Open and Distance Learning Institutions: A Case Study of National Open University of Nigeria", US-China Education Review, vol. 5, no. 1, pp. 639 – 644, 2011
[30] I. Y. Mohammed and S. H. Maysam, "Construction of an Online Examination System with Resumption and Randomization Capabilities", International Journal of Computing Academic Research (IJCAR), vol. 4, no. 2, pp. 62 – 82, 2015.

A Framework for Securing i-voting System in Nigeria using Blockchain Technology

Akintola K.G.
Department of Sodftware Engineering,
Federal University of Technology, Akure.
Akure, Nigeria
[+]akintola2087@yahoo.com

Emmanuel J.A.
School of Science and Technology,
United States International University, Africa,
Nairobi, Kenya.
eadejoke@usiu.ac.ke

Abstract

Election in Nigeria and all over the world is full of problems such as vote tampering, ballot stuffing, and multiple voting and so on. Many electronic voting systems have been proposed and even deployed to solve these challenges but the security aspect still remains largely unsolved. In this paper, the use of block-chain technology to secure i-voting system is proposed. In the design, each computer in the polling units, in the local government areas, and in the geo-political zones serves as a node in the system. Each node stores the block-chain of votes cast by voters hence no single authority is required validate the vote but it is done through consensus.. In the implementation of the system, MySql serves as the database server, HTML, CSS and JavaScript are used to develop the frontend while PHP serves as the server side scripting language. The block-chain is implemented using Java. For the block-chain, the algorithm used for hashing the block is SHA-256. Each block, except the initial genesis block has a link to the previous block. A prototype implementation of the system shows that tampering with the votes will never be allowed by the system thus increasing the security of the voting system.

Index Terms: election, evoting, i-voting, blockchain, web-based

I. INTRODUCTION

It has been discovered that election all over the world is usually marred with several irregularities among which include ballot stuffing, ballot box snatching, multiple voting, late collations of results, database hacking and some other electoral malpractices. The resultant effect of these dubious practices is political, social and economic instabilities as witnessed in the USA presidential election of 2020 and regularly in Nigeria during elections. In order to address these issues, several voting systems and methods have been adopted such as electronic voting machines, e-Voting, i-Voting and so on. Despite this, the electoral system is still bedeviled with electoral malpractices. With the introduction of Internet, voting can now be done online. In this paper, a secure web based online voting system using blockchain is proposed. This eVoting system if implemented will provide an enabling environment for conducting a secured and transparent election and will alleviate the security problem of i-voting systems.

In recent years, we have witnessed several attempts to develop the e-voting systems in some countries including Australia, France, the Netherlands, Swiss, United Kingdom and recently in Nigeria. The state of e-voting, however, is still new in Nigeria. The predominant voting system in Nigeria is still the paper–based voting system which records votes, counts votes, and produces a tabulation of the vote count from votes cast on paper cards or sheets. However, recently, the use of Direct Data Capture Machines (DDCM) for the registration of voters in Nigeria is a step towards electronic voting [10]. The DDCM was introduced to prevent the case of double registration, double voting and other electoral malpractices and for authentication of voters [10]. In Akintola and Boyinbode [11], a web based online voting system that is interactive and user-friendly is proposed. The eVoting system is to provide a platform for conducting free and fair election and to alleviate some of the challenges usually associated with the paper-ballot system. It is noted however that the evoting system can be compromised by the administrators who have high level access to the database of the system for vote counting and others. This necessitates the introduction of block-chain to strengthen the security of the ivoting system.

II. LITERATURE REVIEW

A. Voting Systems

A voting system is a means of choosing between a number of options, based on the input of a number of votes. Voting can also be used to award prizes, to select between different plans of action, or by a computer program to determine a solution to a complex problem. Voting can be contrasted with consensus decision making. A voting system consist of the rules for how voters express their desires, and how these desire are aggregated to yield a final result.

Electronic voting system is voting process that enables voters to cast their votes through the use of computers or other electronic or computerized equipment. There are two main types of electronic voting: offline voting and online voting. Offline voting is voting thorough a computer system that is not connected directly with the system processing the election result. Online voting is voting through a computer that is connected through a network to the computer system processing the election result.

Electronic voting can further be classified into two groups based on where the casting of the vote takes place: the poll-site and the remote electronic voting system. In poll-site system, voters have to go to the polling stations to cast their votes using Direct Recording Electronic (DRE) equipment located at the polling stations while in remote electronic voting, people can cast their votes over the Internet.

Votes cast on an EVM are supposed to be secured, however, the problems with these systems is the reliance on an authority for the monitoring and the allegations of influence by political parties [1;4]. It is observed that evoting has the risk of tampering. Apart from this, other issues concerning evoking include lack of transparency, fake voter IDs, political manipulation in remote locations, as well as delay in the result declaration [1]. It is noted in [1] that all these issues can be mitigated by replacing an evoking system with a block-chain based electronic-voting system. The block-chain technology being an incontrovertible ledger, immutable and distributed makes it safer for voting [5].

B. Basic Principles of E-voting

The main principle of e-voting is that it must be as similar to regular voting as much as possible, compliant with election legislation and principles and be at least as secure as regular voting. Therefore e-voting must be uniform and secret, only eligible persons must be allowed to vote, every voter should be able to cast only one vote, a voter must not be able to prove in favour of whom he/she voted. In addition to this the collecting of votes must be secured, reliable and accountable.

In this proposed system

- Voters are required to vote electronically on the web page of the Independent National Electoral Commission (INEC) by himself or herself.
- A voter shall identify himself or herself using the identity number entered on his
- or her identity card
- Voters are required to register online
- After identification of the voter, the voter shall proceed to cast his vote
- A notice that the vote has been taken into account shall be displayed to the voter on the web page.

C. Scope of E-voting System

From a technical viewpoint, the elections are made up of the following components:

- Registration
- Voter's authentication
- Voting
- Results revelation
- The e-voting system discussed in this paper assumes that:
- voter national identity card has been given to voters.
- the candidate lists have been prepared and entered by the system administrator.
- voters registration takes place online
- Vote counting takes place online by the administrator

D. BLOCKCHAIN EVOTING SYSTEM

Block-chain was first introduced by Satoshi Nakamoto [7]. The block-chain is a peer to-peer distributed ledger system that allows transactions through the Internet without relying on trust or third party financial institution [7; 4]. The Bitcoin was the first cryptocurrency that works entirely over the Internet without the need for third parties such as banks. [4] noted that Bitcoin is important because the underlying technology which is the blockchain technology [4].

Blockchain technology provides a distributed architecture that distributes digital information synchronously among the peer to peer network without a central database. The adoption of this Blockchain in Online Voting System (BOVS) will enhance the integrity and transparency of the voting system [9;1]

.

[7] identifies the following features of blockchain technology as follows:

- Eliminate the central database. Since each peer has the same blockchain (data) will result in no single point of failure.
- When a new data or a block is created, the previous block will be referenced by the new block which renders the blocks an immutable chain that leads to the data being tamper-proof.
- Control over half of the nodes (51%) in the network which made the system extremely secured.

[8], observed the following about block-chain evoting systems:

- The block-chain-based e-voting scheme is public, distributed, and decentralized.
- The block-chain-based e-voting scheme allows the voters to audit and verify the votes
- The database of votes is managed autonomously and is using a distributed server of timestamp on a peer-to peer network.

Voting on blockchain is a workflow where voters' regarding data security is marginal.

E. Related Works

So many researches have been conducted on this issue but we have selected the follosing related works:

[9] presents a blockchain system for electronic voting. The author reviewed some methods of voting such as paper based voting, e-voting, i-voting and block-chain based i-voting. Their advantages and disadvantages were enumerated. The authors finally proposed an i-voting system based on block-chain on an ethereum platform.

[2] proposed a blockchain technology for evoting using the ethereum platform for implementation. The system consist of a Hash Function. Using this hash function, each block is processed one by one where a hash from the previous block is connected to the next block and a digital signature for authentication in the blockchain. The implementation is carried out using the ethereum blockchain platform and was found to be effective and secured.

[8] presented a paper on Securing e-voting based on blockchain in P2P network. All votes in the blockchain is cryptographically linked block by block. The voter selects the candidate he wants to vote for. The vote is public, thus the information of vote is not encrypted. The system uses ECC public key cryptography.

III. METHODOLOGY

A prototype of the Proposed blockchain evoting has been developed. The Prototype is christened BlockchainNetvote. The Node architecture of the block-chain evoting system with emphasis on the peer to peer architecture of the electronic voting system. The clients require a browser installed on the local machines while the main application functionally is provided by the system and the security is based on the block-chain. The component of the system node architectures is presented in Figure 1.

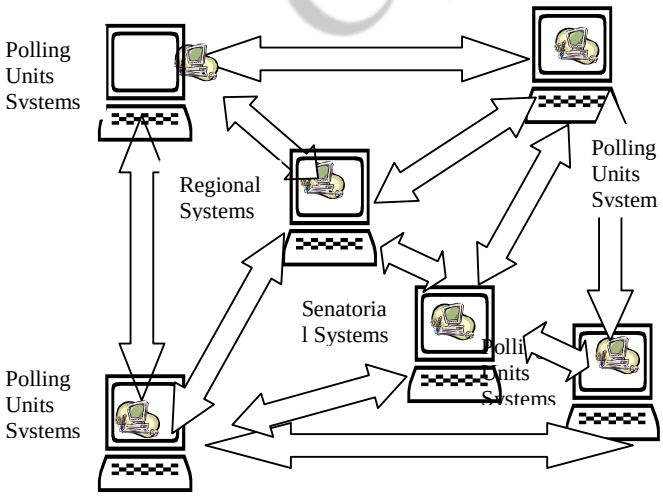


Figure 1 The Node Architecture of the block-chain evoting system.

The system has a client node at each of the polling stations in Ondo State, Nigeria. A regional system connects the systems in each local government. A senatorial node connects all the nodes at the senatorial district. The connected computers work in peer to peer version. The registration of voters by local Governments is given in Figure 2. This Figure 2 will guide the developer the capacity of the servers to be presented in each local government and the average number of voters expected.

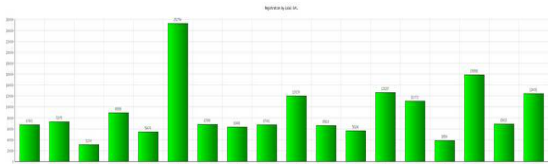


Figure 2 Voters Registration in Ondo State, Nigeria (source ODINEC)

Figure 3 shows the number of the polling units in each of the local government areas of Ondo State. This figure guides on the number of servers to be provided for each of the local governmentsd in Ondo sate.

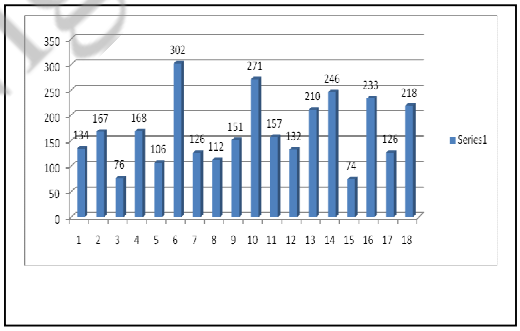


Figure 3 Distribution of 3009 wards in Ondo State, Nigeria (source ODINEC)

The structural Diagram of the evoting system is depicted in Figure 4. This provides the access logic and control of the system. Static pages are pages that do not change during the program run and provides important information for the voters and the general public while dynamic pages provides on the fly functionalities to the voters and administrators. Figure 4 shows the site-map of the system.

A. **Registration**
Each and every voter is required to first register by entering their personal records such as name, sex, age, addrerss, national identity card number and then click submit. The system will then give the voter his private and public keys. A ballot ID will also be sent to the voter The server then binds the credentials submitted to the system with a unique ballot ID to cast his vote. This ID is encrypted with the voters public key. During election, this encrypted ballot will be decrypted using the voter's secret key.This will prevent identity fraud or impostors voting with another persons ballot.

B. **Voting.**
In this period, the voter can cast their vote. Th ballot record contains the voters vote, digital signature, timestamp,. Wneh the voter casts his vote, it will be verified by the system before it is added to the blockchain. Each ballot submitted is encrypted using the server public key. The server machines will have his own public and private keys This is to prevent the voters vote against tampering during transmission. This is shown in Figure 5.

C. **Post-Voting.**
After voting, the server decrypts the ballot so that we can have access to the candidate the voter voted for. As shown in our result section, each ballot will contain hash to the previous block, the ballot information, the timestamp, The first block will serve as the genesis block. The vote is then counted and the result announced. The blockchain cannot be tampered with since the records are linked together using the hash.

D. **Security.** The use of public cryptosystem to hide the vote data will enhance the security of the vote data. Also, SHA-256 will be used to generate the hash address. This generates a unique hash address for each block using the data stored in the block. so any attempt to change the data leads to another different hash address which would be detected as error..

E. Database Design of the system.
In this framework, the database is conceptualized as a set of relations. A relation ia two dimensional table containing tuples and attributes. The general form of a relation is $R[A_1, A_2, A_3, A_4, \ldots\ldots\ldots\ldots, A_n]$ The name of the relation is denoted by R while the set {Ai} i=1,2,3…..n, represents the attributes of the relation [3].
The Relations of internet-based Electronic Voting System are:
Voter_login[Userid, Password]
Administrator[Userid, Password]
Gubernatotial[U_Id,Vcard_Id,Party,State]
Voter Register Table[U_Id, Card_Id, Password, Name,Nationality,Urstate,Age,Email]
Party Table[P_Id, Name, Position, Candidate, State]

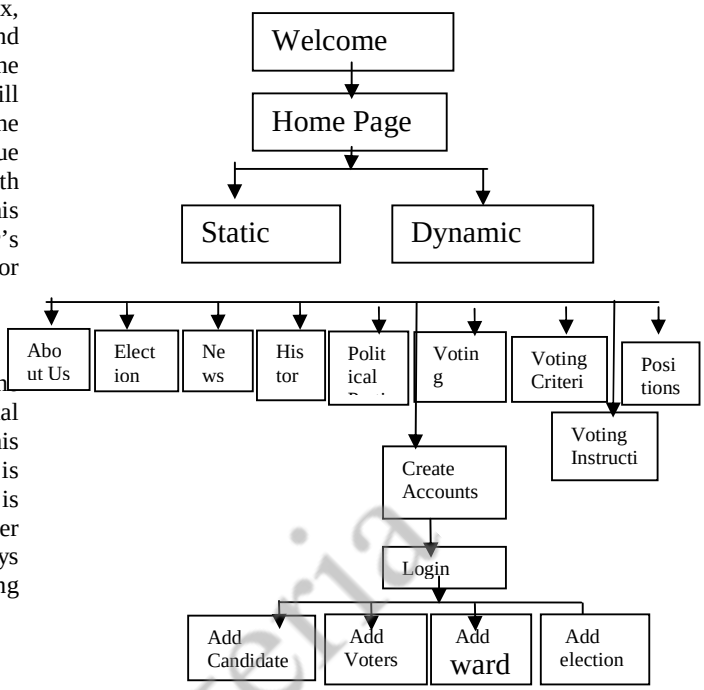


Figure 4 The structural diagram of the evoting system

Voting flowchart

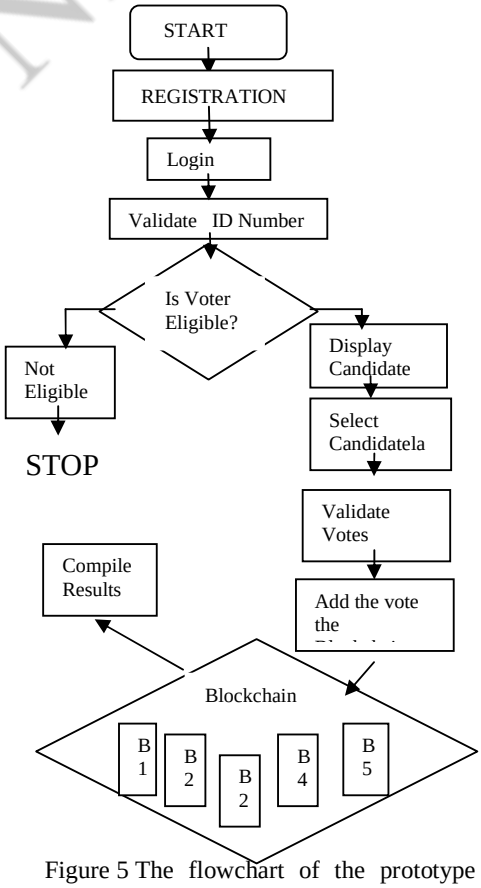


Figure 5 The flowchart of the prototype evoting system Database Relational design

IV. SYSTEM IMPLEMENTATION

The implementation consists of four stages: voter registration, voter's authentication and verification, lectronic block-chain voting and result declaration. To start the system the user types in the URL. For this prototype. The URL is localhost/voting/index.php. This takes the user to the homepage shown in Figure 6 below. The homepage gives the user the general overview of the voting system. It provides a platform by which user can navigate through the system using the various links available on the page.

A. The voting process

The voting process in the blockchain voting system takes place as follows as shown in Figure 5

- The voter accesses via HTTPS-protocol and identifies him/herself with the ID-card.
- The system verifies the eligibility of the voter and identifies his or her constituency. If the voter is not eligible, a corresponding message is delivered.
- The system checks whether such voter has already voted. If this is the case, the voter is informed about it.
- The system makes a query using the constituency data from the candidate list database and as a result receives the list of candidates to be voted for. The list is displayed to the voter.
- The voter selects a candidate.
- The voter application, having the candidate list, asks the user to submit his/her choice.
- The Vote is verified by all the nodes in the blockchain.
- The Vote is added to the blockchain
- In case of successful vote, the system sends a confirmation that the vote has
- been received to the voter.

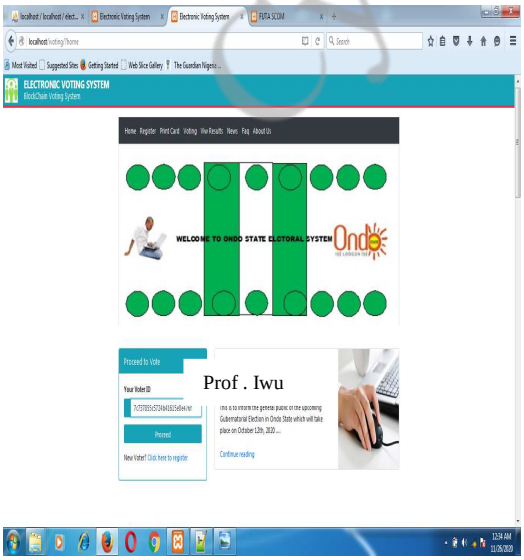


Figure 6 Homepage

A. Registration:

In order to register voters, the link 'register' is clicked. The page in Figure 7 allows eligible voters to register. Without registration, a user cannot vote in any of the elections. On submitting the voter's registration form, an acknowledgement page showing the voter's ID number is displayed. The voter is allowed to print this page.

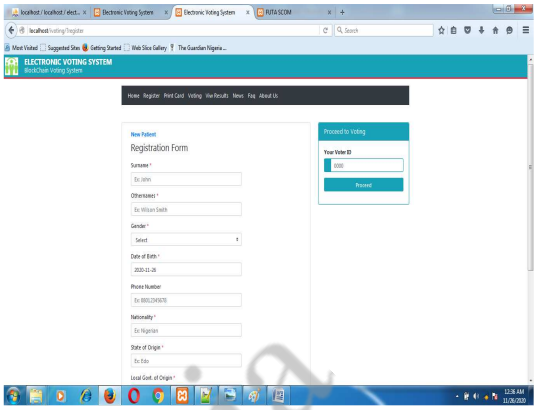


Figure 7 Voters Registration Page

B. Voting.

In order for a user to vote, the user must have registered. He will be given ID number. The user clicks login under voting. This takes the user to the page in Figure 8 below.

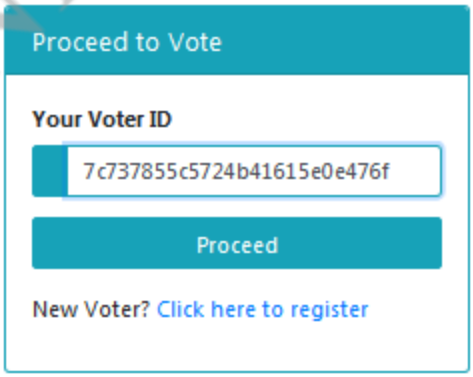


Figure 8.Voter Login

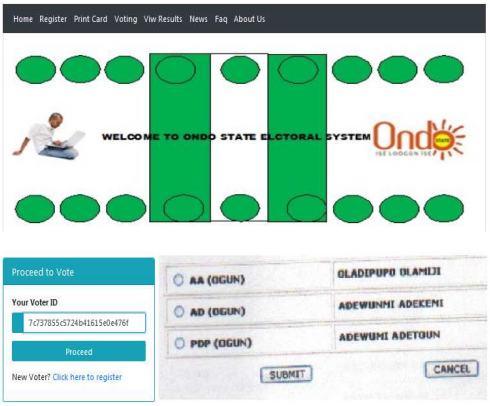


Figure 9 Gubernatorial voting page.

IV. RESULT

A. Blockchain of votes

Chain is Valid
Genesis Block
0
v0
0
1606383386934
49f5701566fbd3e5cadac4e78e80d67c8d1bf14d26f3315d7043b395d4c75b24

Block1
voter1 ID:
7c7737855c5724b41615e0e3500e476f
candidate: 1
previous hash:
49f5701566fbd3e5cadac4e78e80d67c8d1bf14d26f3315d7043b395d4c75b24
timestamp 1606383386934
hash:
f3148a0e42976ee7394b64772546d1369d37a7bf7afc4b4693c568db660d3d9d

Block2

voter2 ID:
06fdde738336672c12b2a78ba7cc2c81
candidate 1
previous hash:
f3148a0e42976ee7394b64772546d1369d37a7bf7afc4b4693c568db660d3d9d
timestamp: 1606383386981
hash:
f3f7d31a2bba92230cd13ad0743ba5bc735fc45d990a201e1b22432723852ee8

Block3

Voter3 ID:
cb57306f55918cc14c02aa03d3ef018
Candidate: 2
Previous hash:
f3f7d31a2bba92230cd13ad0743ba5bc735fc45d990a201e1b22432723852ee8
Timestamp: 1606383387027
Hash:
27882b9bd91d7be5686165f9e19865c84b071d9675e71a924d0a2b13439f24b6

Block4

Voter4ID:
e9b3f6ff8e9c83228fc0ac34167d9eae
Candidate 3
previous hash:
27882b9bd91d7be5686165f9e19865c84b071d9675e71a924d0a2b13439f24b6
timestamp: 1606383387074
hash:
95a2dafef375b2a53744d2ed642ff71a284ed1cb993780e9d16b428129ec7040

Block5

voter5ID:
dc4c050e6ff6ab1d3a86do5f7ae5207f
candidate 1
previous hash:
95a2dafef375b2a53744d2ed642ff71a284ed1cb993780e9d16b428129ec7040
timestamp: 1606383387105
hash:
51f3762f9a3b3628b782aa06d86fc6980891a4959b68f9788a4e6a21e5b4e57f

Figure 10: sample block chain of five voters

B. Vote counting.

To calculate the vote, the administrator page is clicked which brings the page below. From five votes cast so far the results are as follows:
Candidate 1 3
Candidate 2 1
Candidate 3 1

Conclusion
We have been able to design and implement an online block-chain voting system aims at removing most of the security challenges associated with i-voting systems. From the blocks generated, it could be seen that each vote block is linked to the previous block. Any attempt to change any of the information in the block will lead to the generation of a new hash value which will go contrary to the design philosophy of the block-chain. This will generate an error since the blocks chain will be broken. The benefits of this system is enormous.

It allows for cost savings through the reduced amounts of specialists printing required. It allows faster counts and so quicker delivery of final election results. Finally it also increased participation (voter turnout), because it uses Internet. Further to this, it is secured, transparent and supports anonymity of voters. With this system, it is possible for the voter to check that her ballot is included but cannot prove how she voted.

Future work
No electronic voting systems has been certified to even the lowest level of the U.S. government or international computer security standards (such as the ISO Common Criteria or its predecessor, TCSEC/ITSEC), nor has any been required to

comply with such,. Hence, no current electronic voting system has been verified secured. The main challenge facing electronic voting system today is security. As future work, we will be looking at deploying this system on blockchain network such as the Etherium. Also, the use of biometric to secure evoting systems in order to prevent multiple registration and voting impersonations will be considered..

References

[1] Anjan S., Sequeira J.P. (2019). Blockchain Based E-Voting System for India Using UIDAI's. Aadhaar. Journal of Computer Science Engineering and Software Testing e-ISSN: 2581-6969 Volume 5 Issue 3

[2] Arun V., Dutta A., Rajeev S., Mathew R.V. (2019) E-Voting using a Decentralized Ethereum Application. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-4, April 2019
29-4188/02.

[3] Codd E., (1970), "Relational Model of data for large shared databanks" Communication of ACM, vol. 13 No 6.

[4] Kovic, M. (2017): Blockchain for the people. Blockchain technology as the basis
for a secure and reliable e-voting system. ZIPAR Discussion Paper Series, Volume
1, Issue 1. Zurich, Switzerland.

[5] Lafaille, C. (2018). What is Blockchain Technology? An Easy Guide for Beginners Retrieved 22 8, 2018, from https://www. investinblockchain.com/what-is-blockchain-technology/., 2018

[6] Lambrinoudakis C., Gritzalis D. and Katsikas S. K. (2002). Building a Reliable e-Voting System: Functional Requirements and Legal Constraints Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02)15. p. 435

[7] Nakamoto, S. Retrieved 22 8, 2018, from https://bitcoin.org /bitcoin.pdf., 2008.

[8] Yi H. (2019) Securing e-voting based on blockchain in P2P network. *EURASIP Journal onWireless Communications and Networking* (2019) 2019:137 https://doi.org/10.1186/s13638-019-1473-6.

[9] Yi O.K. and Das D. (2020). Block Chain Technology for electronic Voting. Journal of Critical Reviews JCR. 2020; 7(3): 114-124. doi:10.31838/jcr.07.03.22

[10] Olufemi K. (2020). How close is Nigeria to adopting a proper e-voting system? https://techpoint.africa/2020/11/06/nigeria-adopting-e-voting/

[11] Akintola K.G. Boyinbode O.K. (2009). Framework For Implementation Of A Web Based Electronic Voting System. African Journal of Physical Sciences, 2009.

A Secured Payment System for online Livestock Feeds business using Cryptography

Akintola K.G.
Department of Sodftware Engineering,
Federal University of Technology, Akure.
Akure, Nigeria
[+]akintola2087@yahoo.com

Emmanuel J.A.
School of Science and Technology,
United States International University, Africa,
Nairobi, Kenya.
eadejoke@usiu.ac.ke

Abstract
It is noted that online trading is faced with a lot of security challenges which make online transactions unsafe. This paper presents the development of a secured platform for the transmission of payment details to merchants during online trading. The motivation for this work is to secure customer details while buying livestock feeds online. The security architecture of the system is designed using the RSA encryption /decryption algorithm. In the online system, after users have selected their products, they are asked for payment details such as the credit card details of the customers. The details will be encrypted using the private key of the customer and sent over the channel. At the receiving end, it will be decrypted using the public key. A prototype of the system has been developed and in computer laboratory of the Federal University of Technology, Akure using PHP, MySql, HTML, CSS, and Javascript. An implementation of the system shows that the system can be effective at securing customers details during online transactions.

Keywords: Cryptosystem, RSA, eCommerce, Asymmetric, Symmetric

I. INTRODUCTION

Electronic Commerce (eCcommerce) refers to the buying and selling of goods and services via electronic channels, primarily the Internet [2; 4]. e-commerce transactions include many entrepreneurs such as online fish sales, online bookstores, online feeds sales, e-banking, online ticket reservation and online funds transfer and so on [4]. e-commerce transactions involves the transfer of confidential information such as the credit card details, users personal information, account details and so on, as such, securing these information is of utmost concern to ecommerce users. An RSA algorithm has been found to be useful in securing users details in online transactions. Therefore this research develops a secured payment system using the RSA algorithm.

II LITERATURE REVIEW

A. SECURITY ISSUES IN ECOMMERCE

The security issues and vulnerabilities usually witnessed by the users of ecommerce include the following among others:

- Sniffers: Sniffers are software used to capture keystrokes from a particular person. This software could capture log on IDs and passwords.
- Guessing passwords. This is the act of using software to test all possible combinations to gain entry into a network.
- Brute force: This is a technique to capture encrypted messages then using software to break the code and gain access to messages and user's IDs and password.
- Random dialing: This technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could be use as a point of attack.
- Social engineering: An attacker call the bank's help desk impersonating authorized Information about the system including changing passwords.
- Trojan horse: A programmer can embed code into a system that will allow the programmer or another person-unauthorized entrance into system or network.
- Hijacking: Intercepting transmission than attempting to deduce information from them.

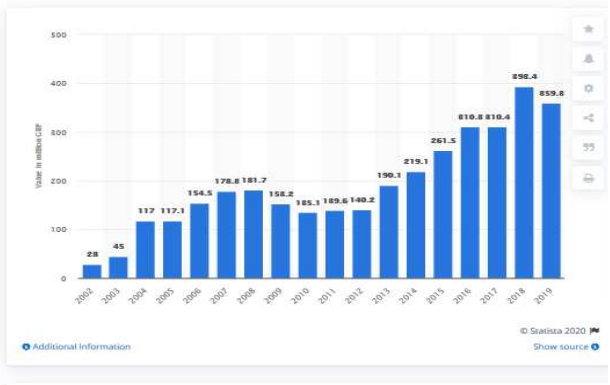


Figure 1 Value of annual e-commerce fraud losses on UK-issued debit and credit cards in the United Kingdom (UK) from 2002 to 2019 (source: statista)

The Key components that will help maintain a high level of public confidence in an open network are enumerated as follows:

- **AUTHENTIFICATION:** Authentication is another issue in ecommerce. Transactions on the internet or any other telecommunication network must be secured to achieve a high level of public confidence.
- **TRUST:** Trust is another issue in internet ecommerce. In cyberspace, a trusted third party which is the certificate authority (CA) used to secure trust.
- **NONREPUDIATION:** Is the undeniable proof of participation by the sender and the receiver in a transaction. This can be achieved by using the public key encryption [7].
- **PRIVACY:** This is concerned with the protection of users' information from unauthorized users.
- **AVAILABILITY:** Availability is also used in maintaining a high level of public confidence in the network environment. Users of a network expect access to systems 24 hours per day, seven day a week.

B. THE RSA ALGORITHM

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman developed a cryptographic algorithm, which was essential to replace the less secure National Bureau of Standards (NBS) algorithm. RSA can be applied to a public-key cryptosystem as well as digital signatures systems. In RSA, the encryption key is public while the decryption key is kept secret. The architecture of the RSA algorithm is presented in Figure 2.

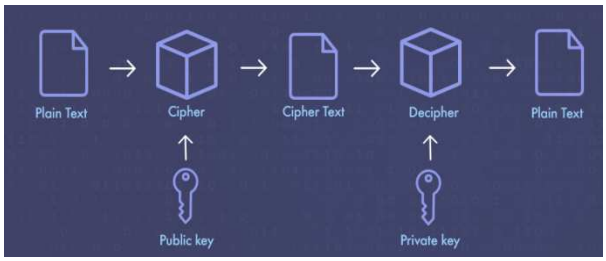


Figure 2 RSA crtptosystem

C. RELATED WORKS

Several works have been done in this area. In [1], a secured online eCommerce store that uses password for security is developed. The password is used to prevent unauthorized access to the system. Sensitive information such as password are encrypted before storage. Also, to prevent SQL injection into input fields obtained from forms, a mysql_real_escape_string( ) function is used. This increases the security of the system. A cryptographic function using Message-Digest 5 (MD5) was used to increase the security of the files and messages transmission in the system. In the work, MD5 function was used to encrypt the VISA-ID information of the customer to provide more security.

[3] presents a secure online electronic transaction (SOET) system for a cashless society. The main objective of the work is to secure an online electronic transaction system. An online store scenario was developed to model a market plaza where goods and services are displayed for buyers to access. A biometric security mechanism was used for online authentication. A potential customer will have to create an online account with the modeled E-Naira bank to participate in the transaction. The system was implemented using (WAMP: Window, PHP, Apache, MySQL). The system needs fingerprint hardware for effective operation.

[5] presents the design of a secured Electronic Payment System for E-Commerce. Their work presents a secure electronic payment protocol for e-commerce where consumers can connect with the merchant. Each entity in the system that is, the client, merchant, user banks, and merchant bank, registers with the payment gateway to create its secret key with the gateway. In addition, the user and merchant also create a secret key between themselves. The customer requests for the product with her temporary identity created in the merchant website, and the

merchant sends the request to the payment gateway. The RSA algorithm is adopted as the security model.

[8] developed an e-Commerce security system using the RSA Cryptosystem. The proposed system is called an RSA e-Commerce security system (RSA-ESS). It aims to solve the security and privacy problems of credit card information in e-Commerce transactions. In this system, RSA is used encrypt and decrypt credit card details during an e-commerce transaction.

[6] developed a secured electronic payment system which include four modules: the certification of participants of the electronic transactions, the encryption of sensitive data using multiple encryption technique, monitoring of the information sent against hacking and provision for defense system againt attacks on the ecommerce application.

III. THE PROPOSED SECURED PAYMENT SYSTEM

The proposed system is just to provide security for the exchange of data and information between the client and the merchant. Figure 3 presents the flow of information in the system. The user logs on to the system. He makes an order for fish feeds through the user interface of the system. The customer supplies his/her payment details. The payment details are forwarded to the acquire (merchant) bank. Acquire Bank forwards the details to the issuer bank, (the customer bank). The issuer authorizes the payment. The merchant confirmed the payment. The merchant then completes the order. Finally the issuer sends the bill to the customer.

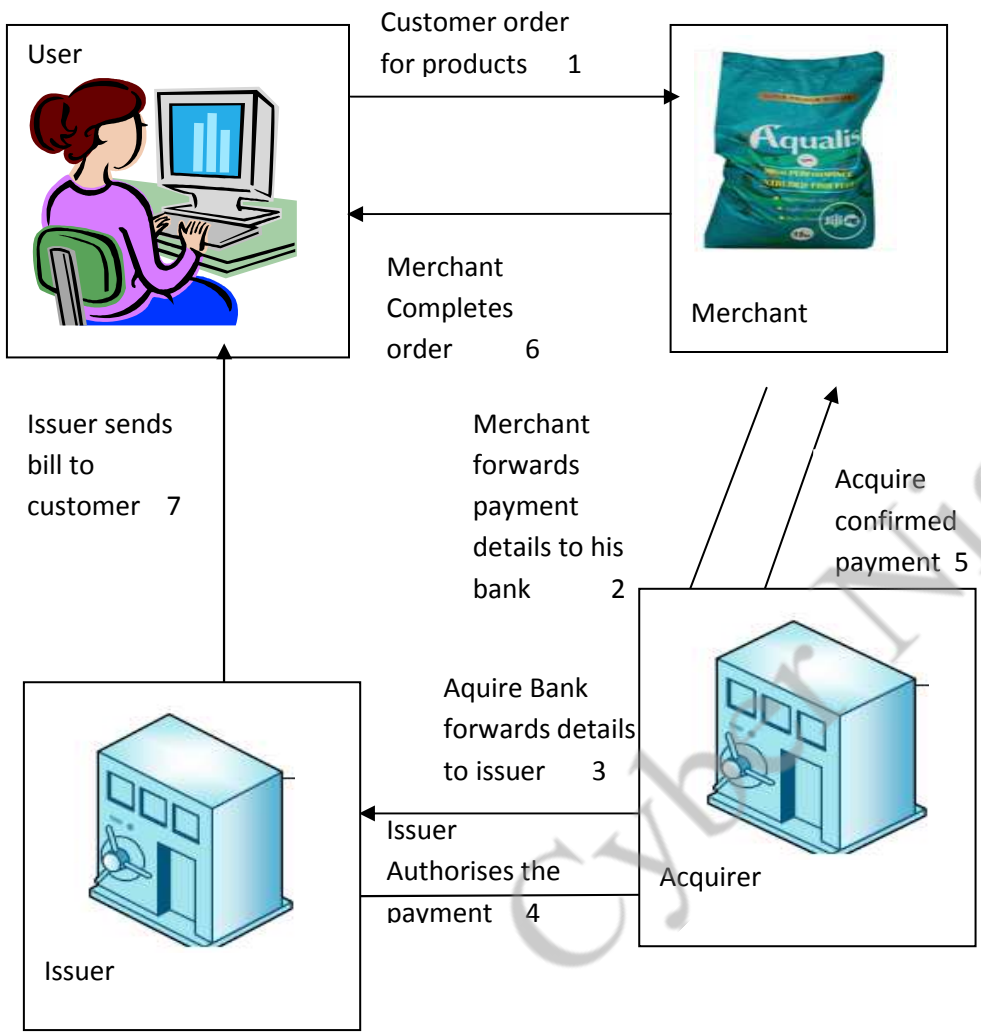


Figure 3 flow of transactions in the ecommerce

Figure 4 presents the flow of encryption system. The user logs on to the system. He makes an order for fish feeds through the user interface of the system. The customer supplies his/her payment details. The payment details are encrypted using the private key before being forwarded to the merchant. The merchant decrypts the message using his/her private key.

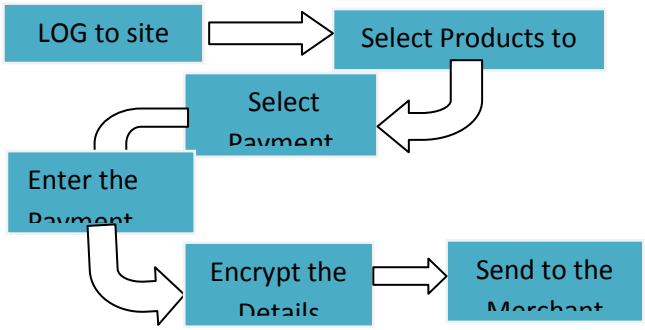


Figure 4: Flow of the Proposed secured ePayment system

The RSA algorithm is divided into three parts:
Key generation: RSA uses a *public key* and a *private key for its operation.* The keys for the RSA algorithm are generated using algorithm 1 as follows:

Algorithm 1 Key Generation

1. Choose two distinct large random prime numbers p & q such that p ≠ q.
2. Compute n= p × q.
3. Calculate: phi (n) = (p-1) (q-1).
4. Choose an integer e such that 1<e<phi(n)
5. Compute d to satisfy the congruence relation d × e = 1 mod phi (n); d is kept as private key exponent.
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

Encryption: Encryption can be done using algorithm 2 as follows:

Algorithm 2 Encryption

1. *Plaintext:* $P < n$
2. $Cipherttext: C = P^e mod\ n$

Decryption: Decryption can be done using algorithm 3 as follows:

Algorithm 2 Decryption

1. *c. Decryption*
2. *Ciphertext: C*
3. $Plaintext: P = C^d mod\ n$

IV. SYSTEM IMPLEMENTATION

A case study of fish feeds ecommerce site was developed using RSA Security System for protecting the payment transaction details. The software allows potential buyers to log into the system, selects products to buy and encrypt the credit card payment information at the sending end and decrypts the information at the receiving end. The information allows the withdrawal of money from the customer account and crediting of the merchant account. The system is user-friendly and modularized to allow for easy system flexibility, implementation and maintenance.

Figure 5 Login Page

Figure 6 Product Selection Page

Figure 6 Product Ordering Page

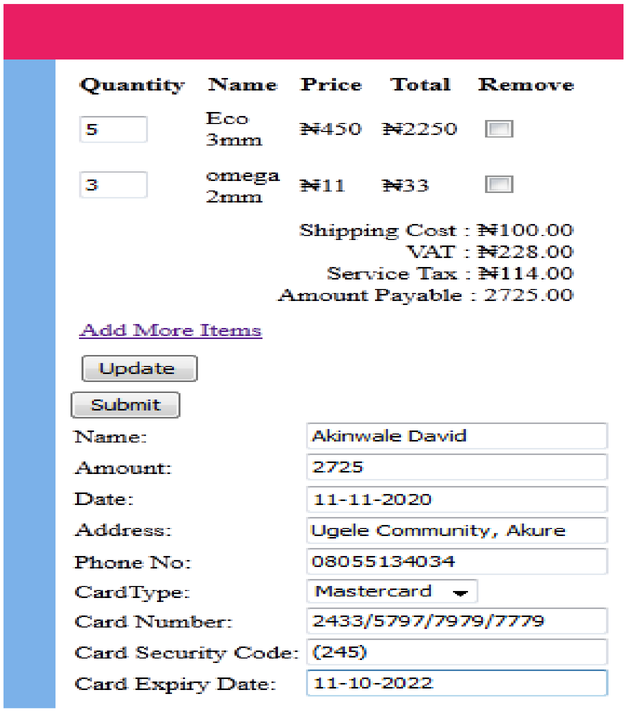


Figure 7 Payment Page

The encrypted Card Information

Name:

篐硇鐡呺 ·琻闈浲 岞琻鐋鐡牃

Amount: 峙磾峙寀

Card Number:

ຄ◌́㊤㊤ · 瞳⌷ · ⌷ · ⌷ · ⌷ · ·

⌷⌷⌷ ·

Card Security Code: 岚曼 · 獰庰

Card Expiry date:

11魅1ʊ魅lxʊlx lx

Figure 8 Encrypted Payment Page

V. CONCLUSIONS

This paper proposed the use of password and RSA for effective security of ecommerce transactions with a case study of livestock ecommerce system. This will solve the of privacy in online transactions. Experiments proved that the system performs excellently at hiding information from unauthorized users. The future work will look at other privacy preserving solutions such as the elliptic curve with the aim of increasing the security of ecommerce applications.

REFERENCE

[1] Abed B.F., Al-Hamadani R.S., Mohmmed S.G. (2016) Design and Implementation of Secured E-Commerce System, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 63-72 www.iosrjournals.org

[2] Akintola K.G. and Akinyede R.O. and Agbonifo C.O.(2011) "Appraising Nigeria Readiness for Ecommerce Towards Acheiving vision 20:2020" *International Journal of research and review in applied Science*(IJRAS) Vol. 9 Number 2, pp330-340.

[3] Etuh E, Obiniyi A.A, Yusuf Akinyele O.A. (2017) Design and Implementation of a Secure Online Electronic Transaction (SOET) System for a Cashless Society. August 2017. Journal of Computer Sciences and Applications 5(2):83-89

[4] Hussain M.A. (2013). A Study of Information Security in E-Commerce Applications. International Journal of Computer Engineering Science (IJCES) Volume 3 Issue 3 (March 2013) ISSN : 2250:3439 https://sites.google.com/site/ijcesjournal.

[5] Hassan M.A., Shukur Z. and Hasan M.K. (2020). An E_cient Secure Electronic Payment System for E-Commerce. Computers 2020, 9, 66.

[6] Khandare N.B. (2015). Transaction Security for Internet E-commerce Application. International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 2, February 2015 ISSN: 2277 128X

[7] Michael G., Arunachalam A.R., Srigowthem S. (2017). International Journal of Pure and Applied Mathematics Volume 116 No. 13 2017, 285-289 ISSN: 1311-8080 (printed version); ISSN: 1314-3395

(on-line version) url: http://www.ijpam.eu Special Issue.

[8] Nwoye, C.J. (2016) Design and Development of an E-Commerce Security Using RSA Cryptosystem. Int. J. Innov. Res. Inf. Secur. **2015**, 2, 2349–7017. Pyae Pyae Hun (2008).

IoT based method to enhance testing frequency against COVID-19

1st Ajaero Emmanuel
Department of Computer Engineering
Michael Okpara University of Agriculture
Umudike, Nigeria
ajaero.emmanuel@mouau.edu.ng

2nd Chinenye Ezeh
Department of Computer Engineering
Michael Okpara University of Agriculture
Umudike, Nigeria
0000-0002-9235-2024

3rd Chinomso Daniel Okoronkwo
Sofware Engineering
Federal University of Technology
Owerri, Nigeria
chinomso.okoronkwo@futo.edu.ng

***Abstract*—For well over one year, the world has been ravaged by a global pandemic which has affected every sphere of human endeavor. In a bid to effectively fight against the novel coronavirus 2019 (COVID-19), the World Health Organization recommended to countries testing, isolation, and contact tracing. These recommendations are somewhat highly dependent on testing, of which isolation and contact tracing would not be feasible if proper tests are not conducted. Recent researches indicate that the focus had been on volume of tests, accuracy of tests and velocity of tests with little or no attention on frequency of tests. In this paper, a solution is designed and developed to enhance the frequency of tests by aiding individuals to perform tests at regular intervals, whether they manifest symptoms of COVID-19 or not. A Bluetooth enabled Oximeter device is used to monitor an individual's blood Oxygen level to avert deteriorated respiratory symptoms due to late detection. The device is interfaced with a mobile application to measure and record Oxygen concentration levels. Results obtained from every test is promptly shared with relevant authorities for immediate action if need be. The data captured equally helps authorities keep track of areas that might be at the risk of an outbreak. Experimental tests were carried out to ascertain the effectiveness of the proposed solution. It proved to be very efficient and helpful as frequency of tests were scaled up and real-time information about people at the risk of COVID-19 are promptly made available to the relevant authorities.**

***Index Terms*—COVID-19, frequency, Oximeter, Oxygen, testing**

I. Introduction

The world has been greatly ravaged by the outbreak of COVID-19 pandemic. This current pandemic which was caused by the novel coronavirus (SARS-CoV-2) started in Wuhan, China in December 2019 [1], [2]. The symptoms include respiratory droplets from coughing and sneezing that results to different forms of respiratory infection. A large number of infected patients experience flu like symptoms, while some are asymptomatic. Also, the replication process of the virus could result to diarrhea, acute respiratory distress syndrome (ARDS) and death [3]. The World Health Organization (WHO) is at the forefront of the fight against COVID-19 due to their presence in most countries. Lately, similar health bodies and stakeholders have collaborated with WHO to scale up testing capacities for COVID-19 [3].

In a bid to mitigate the rapid spread of COVID-19, WHO recommended that countries should make efforts at testing, isolation and contact tracing as highlighted by WHO director's remarks on March 11, 2020 [4]. Due to the widespread of COVID-19, the ideal response from health officials has been early testing of people across the world.

The question now is, how efficient is this approach with respect to the velocity (how fast can the population be tested) and the capacity of tests performed within the shortest possible time? In some countries, the lockdown policies resulted in various economic catastrophes. The WHO's approach when implemented alongside strict lockdown measures, yields effective results but it's quite expensive. On the flipside, flouting it has left the world with a grim death rate which necessitates that there is need to come up with a more efficient approach.

A. Concerns with Current Approach Employed in the Fight Against COVID-19.

In line with WHO's aim to reduce the spread and mortality rate correlated to COVID-19, there are four main issues that must be addressed namely volume(capacity), velocity, veracity and frequency of testing.
Interestingly, most countries have aggressively concentrated on investing in solutions to handle the first three concerns as enumerated above rather than on frequency of testing. This lopsided attention or rather less noticed essential factor (frequency of testing) make it seem as though regular testing is not so important particularly to the most vulnerable population.

The frequency of testing in the context of this publication refers to how many times an individual is tested, regardless of a visible symptom or the previous infection history. Due to low frequency of testing, an individual who takes a test will go for days or months without taking another test and will only take a test if the symptom of the virus surfaces. The low frequency of testing degrades to a great extent the successes achieved by high volume, high velocity, and high veracity of testing. This trend can only be reversed if people can self-test consistently.

Therefore, in this paper, a solution is designed and developed to enhance the frequency of tests by aiding individuals to perform tests at regular intervals. A Bluetooth enabled Oximeter device is used to monitor an individual's blood Oxygen level to avert deteriorated respiratory symptoms due to late detection. The device is interfaced with a mobile application to measure and record Oxygen concentration levels and

the results obtained are remotely transmitted to the relevant authorities for necessary actions.

The rest of the paper is organized as follows: section II presents related relevant literature. Section III presents the methodology. In section IV, the software design is presented. In section V, system testing is carried out and experimental results discussed . Finally, the paper is concluded in section VI.

II. Related Works

There has been a rapid rise in the number of COVID-19 patients and related cases around the world. It is of great importance that measures to curtail the spread of this infectious disease is speedily implemented [5]. This section briefly reviews works with respect to the use of technologies to mitigate the spread and management of COVID-19 pandemic to scale up testing capacities for COVID-19 [3].

A. Newly Developed Technologies to Fight COVID-19

Li et al [6] presents an IoT based architecture that can curtail the spread of COVID-19. The developed architecture describes the deployment of sensors, such as infrared thermometer in public areas, whereby data retrieved from sensors are uploaded to cloud via use of internet enabled microcontroller such as NodeMCU as an IoT gateway device. The data retrieved were analyzed using machine learning model as a decision technique, as well as representation of data on mobile application in real-time.

An IoT based drone technology was designed by Mohammed et al [7], with the use of virtual reality that integrates real-time video streaming of thermal image and capture process to screen people in crowded places. Based on statistics in [1], [2], about 99% of COVID-19 patients nearly 140 in number at the Zhongnan Hospital of Wuhan University had fever with extreme high temperature symptoms.

Mohammed et al [8] proposed an IoT based helmet temperature screening design. Although, the authors were more concerned about how such technology could be mobile in their recent research, the system utilizes thermal images generated from input and output images analyzed from the thermal camera. A notification is sent to health officials whenever the thermal camera captures a person with high temperature. The proposed system was designed and simulated on Proteus software and the results obtained, indicated that the IoT based application could save time, curtail spread and contracting of the virus in real-time.

Garmendia et al developed a cost effective, non pressure ventilator prototype [9], for the treatment of COVID-19 patients. The idea behind the innovation was based on research findings on 138 infected COVID-19 patients in Wuhan, China by the authors in [5]. Their findings revealed that 17% of these patients experienced Acute Respiratory Distress Syndrome (ARDS). The authors developed a ventilator prototype using high-pressure blower, two pressure transducers and a digital display system, which were all connected to an Arduino Nano controller. Evaluation of the developed ventilator was performed and compared to a commercial ventilator. Results obtained from the assessment shows that the developed pressure ventilator prototype operation was similar to a commercial ventilator.

A Smart Tracing System was proposed by Ng et al in [10] as an alternative to manual contact tracing of individuals "who may have had contacts with" infected COVID-19 patients. The time involved in alerting persons who had been in contact with COVID-19 patients is very essential in order to control the spread of the disease [5]. The development of smart contact tracing system was achieved by use of a smartphone's Bluetooth Low Energy (BLE) signals and machine learning classifier. The smart contact tracing system could also alert persons in crowded areas, whenever a social distancing rule is violated. This application consists of interaction and tracing phases integrated into the smart phone's Bluetooth Low Energy (BLE). The contact tracing phase involves the utilization of advertised packets from Received Strength Signals of mobile devices to determine distance observed by persons in crowded places. The tracing phase uses machine learning based classifiers to classify an individual's risk levels based on time and distances spent with an infected COVID-19 patient.

B. The Science of the New Approach

In all the reviewed works, none of them actually deals with frequency of tests. All of the works are more or less focused on preferring solutions for contact tracing and compliance with social distancing. Hence, this work approaches the fight against COVID-19 through a device that enhances the frequency of tests of individuals. The Oximeter device is interfaced to a mobile application to measure and record the Oxygen concentration levels of individuals. The notion of regular self-testing leads us to the main idea of this work, which is to curb the deaths due to COVID-19.

It was observed that COVID-19 patients who were hospitalized had a deficiency of Oxygen blood (hypoxia) of which some were as low as 50 per cent. Dr. Richard Levitan was surprised that most of the patients still exhibited normal brain activity, similar to mountain hikers who experienced low Oxygen concentration in their blood at high altitude. He concluded that the depletion of the concentration in both cases happens gradually but the physiological response of the body keeps the individual going till it gets to an acute hypoxia [11].

III. Methodology

A. System Architecture

The proposed automated-wearable medical report system involves both hardware and software development phases. The system was built based on three (3) layered architectural design as shown in Fig. 1. This architectural design includes: perception layer (device), network layer and presentation layer (application) via a reliable communication medium.

Perception Layer

This is the physical hardware system which is the personal health device. Perception layer can be referred to as the

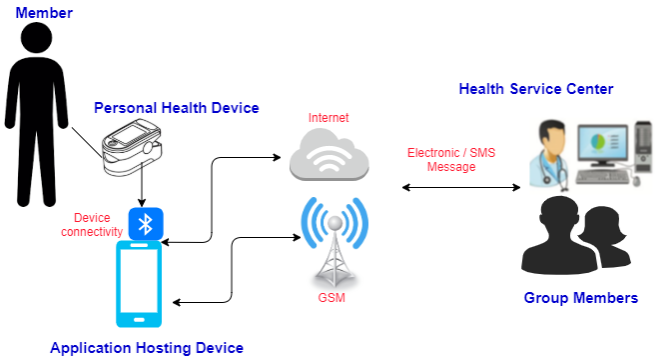


Fig. 1. System architecture

Fig. 2. Oximeter device

recognition layer [12]. The perception layer is described as the lowest layer of the conventional IoT architecture. The basic functions associated with this layer include, collection and transformation of data from objects and environment into useful information. The personal health device in Fig.2, represents the perception layer of the proposed architecture. This device is associated with a Bluetooth enabled Oximeter connected to a microcontroller. This device (wearable sensor) normally attached to the finger, has the capability to measure an individual's Oxygen saturation (SpO2) level.

Network layer

The network layer is also referred to as the transmission layer. It is responsible for the transmission of data generated from the perception layer to the application layer [13]. Hence, it acts as the bridge that connects the perception layer and the application layer. This layer utilizes numerous communication networks for transmission of data. The Bluetooth enabled Oximeter utilizes a personal wireless network via Bluetooth Low Energy (BLE) technology for the transmission of data from the personal health device (Oximeter) to the application hosting device. Afterward, multi Wide Area Network protocol is adopted in the transmission of data to the health service center and group members are registered on the health application.

Fig. 3. User Interface

Application layer

The application layer is the top layer of the conventional IoT architecture. This layer enables users and medical practitioners to interact with the system. A user interface is provided in a graphical format via connected mobile devices as shown in Fig.3. The transmitted data from the personal health device of users are viewed by other members on the application and mobile messenger. Numerous application services are provided by this layer which include: health monitoring, transportation, disaster monitoring among others.

B. System Description

The system comprises of hardware and software that provides convenient monitoring of Oxygen saturation level of individuals. The prototype also permits the transfer of reports to medical practitioners in remote locations.

The hardware is a wearable Bluetooth enabled Oximeter which determines the Oxygen saturation level or concentration level once it is placed on the finger, earlobe, or toe. Individuals are registered on the Android application in a group or single user account. The test method involves the user launching the mobile application, after which the user selects the corresponding account on which they were registered. The health application then displays guidelines on the connection of the Bluetooth enabled Oximeter to the mobile phone. After a successful connection, users are required to place their finger on the Oximeter. The flow diagram of the system's operation is shown in Fig 4.

The Oximeter is made of a light-emitting diode and light detector with which the device retrieves the Oxygen saturation readings. The Oxygen saturation (SpO2) reading is measured based on the change of light absorption in oxygenated or

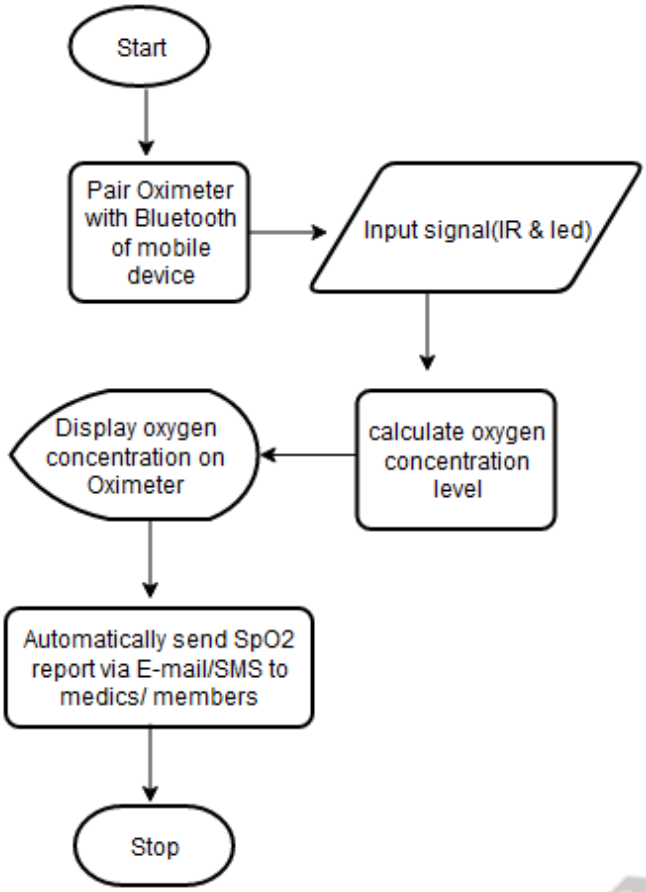


Fig. 4. System flow chart

deoxygenated blood. The test report is automatically shared with other group members and the doctor's office via mobile application. The doctor could schedule a meeting based on the medical report received via mail or message.

IV. Software Design

The software of this system is divided into two areas namely: the client side (the graphical interface between the user, the Oximeter and the server side) and the server side (the interface between the authorities and the system).

A. Client Side

The software design was implemented with reactnative; a JavaScript framework for developing cross platform mobile applications. The Oximeter used does not have a datasheet in the public domain. In other to retrieve the service UUID and the characteristic UUID of the Oximeter, software named NRF Connect was used. NRF Connect is available for free on the Google Android play store. After connecting the NRF Connect software with the Oximeter and collecting all the necessary information from the device, the information was used to integrate the Oximeter mobile application. The data received from the Oximeter is in the following format: Data: RSI, BPM, SpO2, Pi.

Fig. 5. User finger in an oximeter

The information represented by the data received was deciphered empirically by comparing the values being displayed on the Oximeter 's display interface with the values received on the reactnative code. The target parameter is the SpO2 which represents the measured Oxygen concentration in the blood, while the other parameters can be used for other applications.

B. Server Side

The server side followed the Model, View Controller paradigm and was implemented with Django, a Python back-end framework. Since at this time not much data is expected to hit the server, the SQLLite which is native to Django framework was used. In the future, if the system is adapted for public use, the SQLLite will be swapped with POSTGRES SQL to enable it handle high volume of data. For the purpose of testing, the server was also hosted locally on a Raspberry Pi which has to be on the same local network as the mobile phone running the application.

V. System Testing and Evaluation

The proposed system was tested as shown in Figs 5 and 6. After a user is registered, the Bluetooth enabled Oximeter device is attached to the user's finger. The device can equally be disinfected by swiping a damp disinfectant over it after each use. According to (World Health Organization Pulse oximetry training manual), a normal Oxygen saturation is graded between 100% and 95%. Hence, any result below 95%, could mean that such individual is deemed to be in a critical condition and needs urgent health care.

To eliminate the possibility of sending an erroneous reading that does not represent the actual reading, the app takes 30 sample readings from the Oximeter and sends the mode value. The choice of 30 samples was made by empirically observing the settling time of the system. After taking 30 samples, the mode value is always the stable value. It is worth noting that these 30 samples are taken within 20 seconds.

Fig. 6. Mobile application

The system works perfectly well with the Oximeter in Fig 5. We may not guarantee that the system will work with other Oximeters till we are able to test with different Oximeters and publish a list of compatible Oximeters. The mobile application is designed to be data intolerant in the sense that if an incompatible Oximeter sends a data frame that is not comprehensible to the system, the mobile application fails gracefully by populating the Oxygen concentration value with double hyphen and percent sign (- -%).

VI. Conclusion

In this work, a personal health device to aid the fight against COVID-19 is proposed. The Bluetooth enabled Oximeter interfaced to a mobile device, records the Oxygen concentration levels of individuals. The concept is to enhance the frequency of self-tests by individuals at regular intervals who might have been exposed to the risk of contracting COVID-19.
The evaluation results carried out proved that the proposed system is able to detect accurate Oxygen concentration levels of individuals. A normal Oxygen concentration level ought to be 95% and above. Persons who have COVID-19 might be at the risk of developing respiratory diseases which greatly reduces the Oxygen concentration in their blood stream. Regular tests using the system proposed in this work will save individuals and alert relevant authorities about persons who need medical help most. The records can equally aid agencies fighting COVID-19 in detecting areas that are most at risk.

References

[1] S. Ahmad, A. Hafeez, S. A. Siddqui, M. Ahmad, and S. Mishra, "A review of covid-19 (coronavirus disease-2019) diagnosis, treatments and prevention," 2020.

[2] M. A. Shereen, S. Khan, A. Kazmi, N. Bashir, and R. Siddique, "Covid-19 infection: Origin, transmission, and characteristics of human coronaviruses," *Journal of Advanced Research*, vol. 24, pp. 91 – 98, 2020.

[3] A. Union and A. CDC, "Africa joint continental strategy for covid-19 outbreak," Mar 2020, accessed online on May 17, 2020. [Online]. Available: https://africacdc.org/download/africa-joint-continental-strategy-for-covid-19-outbreak/

[4] W. H. Organization, "Who director-general's opening remarks at the media briefing on covid-19 - 11 march 2020," Mar 2020, accessed online on March 30, 2020. [Online]. Available: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020

[5] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact," *IEEE Access*, vol. 8, pp. 90 225–90 265, 2020.

[6] D. Li, Y. Hu, and M. Lan, "Iot device location information storage system based on blockchain," *Future Gener. Comput. Syst.*, vol. 109, pp. 95–102, 2020.

[7] M. N. Mohammed, N. A. Hazairin, S. Al-Zubaidi, A. Sairah, S. Mustapha, and E. Yusuf, "Toward a novel design for coronavirus detection and diagnosis system using iot based drone technology," 2020.

[8] M. N. Mohammed, H. Syamsudin, S. Al-Zubaidi, A. Sairah, R. Ramli, and E. Yusuf, "Novel covid-19 detection and diagnosis system using iot based smart helmet," 2020.

[9] O. Garmendia, M. A. Rodríguez-Lazaro, J. Otero, P. Phan, A. Stoyanova, A. T. Dinh-Xuan, D. Gozal, D. Navajas, J. Montserrat, and R. Farré, "Low-cost, easy-to-build noninvasive pressure support ventilator for under-resourced regions: open source hardware description, performance and feasibility testing," *The European Respiratory Journal*, vol. 55, 2020.

[10] P. C. Ng, P. Spachos, and K. Plataniotis, "Covid-19 and your smartphone: Ble-based smart contact tracing," *ArXiv*, vol. abs/2005.13754, 2020.

[11] R. Levitan, "The infection that's silently killing coronavirus patients," Apr 2020. [Online]. Available: https://www.nytimes.com/2020/04/20/opinion/sunday/coronavirus-testing-pneumonia.html

[12] P. Sethi and S. Sarangi, "Internet of things: Architectures, protocols, and applications," *J. Electr. Comput. Eng.*, vol. 2017, pp. 9 324 035:1–9 324 035:25, 2017.

[13] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *2012 International Conference on Computer Science and Electronics Engineering*, vol. 3, pp. 648–651, 2012.

Impact of Pixel Scaling on Classification Accuracy of Dermatological Skin Diseases Detection

Afiz Adeniyi Adeyemo
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
abdulhafeez_adeyemo@yahoo.com

Sulaimon A. Bashir
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
bashirsulaimon@futminna.edu.ng

Abdulmalik D. Mohammed
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
drmalik@futminna.edu.ng

Opeyemi O. Abisoye
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
o.abisoye@futminna.edu.ng

***Abstract*—Images are made up of many features on which the performance of the system used in processing them depends. Image pixel values are one of such important features which are often not considered. This study investigates the importance of image preprocessing using some calculated statistics on the pixels of skin images in classifying images using HAM10000 dataset. Image pixel values make a great impact on the classification performance of Convolutional Neural Network (CNN) based image classifiers. In this study, the 'original pixel values' of the skin images are used to train three carefully designed CNN architectures. The designed architectures are further trained with some calculated statistical values using 'global centering', 'local centering', 'dividing pixel values by the mean' and 'root of the division' techniques of data normalization. The results obtained have shown that, out of the five different forms of values used in training the architectures, the CNNs trained with the original (unscaled) image pixel values perform below those trained with calculated statistics that are computed on the image pixel values.**

Keywords—image pixel scaling, image preprocessing, classification accuracy, dermatological skin diseases

I. INTRODUCTION

Skin infections have been rated to be the most common of all diseases [1] and dangerous of all cancers [2]. There are many skin conditions that affect man, which are diagnoseable and identifiable by their various symptoms [3] and are accordingly treated by skin experts. The traditional process of screening skin infection for classification involves a pathologist performing prognosis examination on the infected part of the skin [4]. This is followed by biopsies which involve removal of the affected skin portion for laboratory investigation [5] to establish cancer presence in the skin area. To further classify the infections to appropriate types, another group of medical experts specialized in autopsy performs histopathology on the skin sample [6] to grade the diseases for appropriate medical administration. This process requires the patient to wait for some period of times thereby his condition becomes more severe, unbearable financial burdens committed and wrong classification may be specified at the end which will subsequently lead to administering wrong medication. The adoption of deep learning and the continuous growth and availability of computing power have made the classification of image models more efficient [7], [8]. The representations (features) learnt by an image classifier have been proven to have noticeable effect on the performance accuracy of the classifier [9]. The effects of some of these image features as discussed in some literatures include image quality distortions [10], image compressions [11], illumination quality [12], image resolution [13], [14] and spatial resolution [15]. One other feature that has direct impact on image classification is the pixel which has not got much attentions of the researchers, especially on dermatological images.

A pixel in digital imaging is the smallest addressable element in an all points addressable display device, so it is the smallest controllable element of a dermatological skin image. Each pixel is a sample, and represents the original image more accurately [16]. The variation in the pixel values denotes the intensity of the color representation presence at a particular point of an image. Image pixel scaling involves generation of new image with higher or lower number of pixels without loss in the quality of the image [17]. The need for scaling the pixel information of an image is necessary to remove the unwanted pixels from the image [18] thereby preparing the images for processing. Image preprocessing is highly required in preparing image data to bring improvement to the features of the image data. This improvement suppresses unwanted distortions and/or enhancing some important image features which can result in improved data to work on [19]. Data normalization is an imperative measure taken in image pre-processing. The goal of normalizing image values is to change the values of numeric columns in the dataset to a common scale especially when there are different ranges in the features of the data [20].

This study aims at analyzing the experimental study of applying different statistical scaled values and their effects on the classification accuracy of dermatological skin diseases detection. To achieve this, a proposal of an experimental methodology is designed. In the designed experiment, the Convolutional Neural Network (CNN) architectures used are built to make up of different convolutional filter sizes. In each of the experiments, the network is trained and evaluated using the calculated statistics computed on the pixel values of the HAM10000 dermatological dataset collected from the Medical University of Vienna. The result of this study may be different from the ones obtained in the previous

investigations for the fact that the features used in training the networks in this work are directly extracted from the images, and not transformed nor deformed in any form.

The remaining part of the paper is organized as follows: Section 2 highlights some previous related research works, while section 3 describes the methodology and the experimental set up used in performing the experiment for the study. The results and discussion are carried out in Section 4 of the paper while Section 5 presents the conclusion and future work.

II. RELATED STUDIES

As the application of deep learning pathological skin diseases classification and diagnosis has become widespread, many researchers have put on the responsibility of investigating the contribution of some features on the processing of skin images and consequently, on the resulting accurate classifications. For example, authors in [21], examine the effect of image compression on telepathology. In carrying out the task, they selected ten diagnosed cases from the teaching files of Department of Pathology, University of Illinoise Hospital, Chicago. Each of these ten samples was then snapshot in six different forms and captured with a Polaroid DMC 1 digital camera. The original (uncompressed) images were saved in Windows bit-map and later compressed using Adobe PhotoShop 5.0. These images were compiled and sent on the internet. The selected sets were monitored on the net by a group of ten experts according to a laid down protocol. The final diagnosis based on the glass slides from UIC was used as the reference diagnosis. Independently, three among the authors did compare the correspondents' diagnoses blindly with the reference diagnosis using four categories of classification evaluations: no diagnosis (n=0) when no diagnosis was provided, no difference (n=1) if there was total agreement with the reference diagnosis, minor difference (n=2) if the disagreement to the reference diagnosis was minor and did not require any change in the management of the skin diseases, and (n=3) when the difference in the correspondence diagnosis required that a major alteration be carried out in the malignant administration. The work equally adopts the following four categories of confidence levels and these are n=0, when no response was provided by an expert, n=1 for very confidence, n=2 for quite confident while n=3 when there was no confidence. Assessment of images quality were placed on five categories; n=0 (no response), n=1 (excellent response), n=2 (very good response), n=3 (fair response) and n=4 (poor performance). The results were analyzed using comparison of proportions. The results from the analysis show that there were no statistical differences at the rates of acceptability for both compressed and uncompressed image samples at 95% level of confidence interval. Similarly, there was no difference statistically at the rates of accuracy for the samples at the same 95% level of confidence interval. The results further reveal that no notable deviation was observed when the assessment was carried out on the quality of both the compressed and uncompressed images at 95% level of confidence interval. This investigative work considers the ability of pathologists in diagnosing skin disease using telepathology if the original samples are manipulated with compression technique of image preprocess. The experiments performances were evaluated using statistical analyses, does not employ an algorithmic process and does not work on the pixel values of the pathological images.

In another studies, [22] carries out investigation on the effect of lossless compression of JPEG2000 on diagnostic virtual microscopy. The authors have previously in one of their efforts, established that image quality is not destructed by lossless compression. In this new work, evaluation was carried out on virtual 3-dimentional microscopy using JPEG2000 whole slide images of gastric biopsy specimens. The authors collected specimens of gastric biopsy from the Department of Pathology, Otto-vonantrum mucosa (VM) and scanned to 0.23µm resolution. With the aid of Kakadu software, 3D slides of uncompressed (that is lossless compression; 1:1) images were created, as well as samples derived from lossy compression using ratios 5:1, 10:1, 20:1. These compressed slides were mixed up and diagnosed by three senior pathologists in a blinded manner according to the updated Sydney classification. The consultants made use of a Windows XP system which was connected to monitor resolved to 1600 x 1200 pixels for VM. SPSS software was used in performing the statistical analysis considering 0.5 level of significant. The results obtained from the pathologists reveal that there exists significant variation from the observation made by Consultant B while grading the density of Helicobater pylori gastritis (H pylori), but in the detection of H pylori, there was no significant difference. In the grading of neutrophil inflammation and in the evaluation of its presence, the significant difference was obtained from the observations made by Pathologist C. It was also shown from the results that out of 46 observations, maximum of 2 false negatives were observed by Pathologists A and B, while C claimed to have observed as much as 9 false negatives. The results further revealed that Pathologists A and B diagnosis specificity performance was over 0.9, while that of C was not beyond 0.9. Similarly, Pathologists A and B recorded above 0.85 while determining the sensitivity performance of their diagnoses, but the highest recorded by pathologist C was 0.8. The results of the K-values show that A and B achieved up to 0.8, while that of C was rated to be 0.77. The observations made by the three pathologists indicate that there is no better performance in the diagnosis of H pylori of the same malignant with the use of lossy compression. It is summarily established that there is no any significant effect made by JPEG2000 compression ratio up to 20 on the detection of H phlori. This study only shows the relative performances of human diagnosis ability using statistical analysis.

Moreover, [23] explores the need to define a clinical task in the valuation of quality of digital pathology image. In the research work, an experiment was performed (at the pre-study level) to select an appropriate test parameters for image alterations. In the main study, three experimental cases were conducted using the same samples of pathology and were overseen by six pathologists. These three experiments were designed to function using different protocols. The images used were collected from animal pathological samples, magnified by 40 with the use of a BX50 Olympus microscope. An approximate area of 1200 x 750 was removed from the original pixel images dimensioned 2776 x 2074 to fit the image presentation requirements. The image qualities were effected with the methods of Gaussian blur, unsharp masking, decreasing/increasing gamma, increasing/decreasing color

saturation, adding low/high frequency white Gaussian noise, and JPG compression. These were applied on every reference image once at a time. In an attempt to achieve the set goal, the six pathologists selected to evaluate the experiment were screened for color vision deficiencies but all passed the examination. These observers performed three experiments each, and to answer some questions as regard the quality of color digital images from pathological clinics. The questions are :– (1) what are the effects of image alterations on clinical performance? (2) How sensitive are pathologists to image alterations? And (3) how do pathologists judge IQ and its attributes? Analysis carried out on the image data was performed with the use of median and inter-quartile range while Kruskal-Wallis testing was performed to take the level of statistical significance. The results obtained revealed that the findings are in agreement with the experimental question 1. However the findings in experiments (2) and (3) do not agree with the questions set. While the results from experiment (2) indicate that the pathologist could not notice the JPG artifacts similarity with high similarity M-JPG and M-NONE, the PIQ results from experiment (3) show that the observers failed to observe what had previously been observed in (1). The authors made use of animal skin samples, did not use any preprocessing technique to ensure full control over the alteration of the images, the experiment was not algorithimic as well.

The first study that adopts a conventional algorithm to evaluate human related skin problem is [24]. Visiopharm HER2-Connect image algorithm is used to evaluate the level of Human Epidermal Growth Factor Receptor 2 (HER2) in immunohistochemical images. In their own efforts, the authors collected and digitalized samples of 55 different patients diagnosed with breast cancer. Of these 55 samples, 30 were analyzed with score 0, 10 samples with 1+, 5 samples were analyzed with 2+ and the remaining 10 were analyzed with 3+. Four image variation parameters which include brightness, contrast, JPEG2000 compression and out-of-focus blurring were applied on each of the images to obtain HER2 scores. The Visiopharm HER2-Connect image algorithm was utilized and its robustness against images serially degraded with the four image parameters was graded. This algorithm was to detect and quantify the amount of HER2/neu (c-erb2-2) in formalin-fixed, paraffin-embedded breast tissue. While the successively degraded images were generated by computer simulation using Matlab. The results obtained show that HER2 scores reduced when illumination increases, compression ratios are higher and when blurring is increased, but inflated with high contrast. It is also established that image adjustment did not affect the cases with no HER 2 score. While the study utilizes a conventional algorithm to solve epidermal problem, it is observed that the problem solved is limited to the breast cancer only which excluded the other parts of the human skin.

Moreover, the authors of [25] explore the impact of JPEG 2000 compression on deep convolutional neural networks for metastatic cancer detection in histopathological images. They proposed an algorithmic CNN based image classifier to detect cancer metastases in the lymph nodes of human breast. The effect of reducing the quality of the image data was monitored by applying different ratios of compression on the image samples used for both training and testing of the algorithm. The dataset used for the experiment is CAMELYON16 image dataset, collected from some clinics in the Netherlands. The images consist of WSIs of pixels resolved to approximately 0.243µm. A total of 650 thousand of size 300 x 300 pixels patched image data was generated with the aid of CNN patched classifier. The proposed CNN which uses Inception_v3 architecture was used to perform binary classification on the inputted data. In training the network, 14 different compression ratios of JPEG algorithm were used to compress samples of 150 thousand from the regions with positive WSIs and 500 thousand from the negative regions. The effect of changing compression ratios of JPEG on the performances of the classifier was measured in three different instances. In the first instance, the system was trained with the original images and its performance was measured using degraded quality images of different ratios of compression. Here, the performances of the CNN in both F1 score and AUC evaluation metrics were observed to be decreasing as the image quality decreases due to increase in compression ratio though of no considerable changes. The performance values of 0.927 was recorded for F1 score and 0.981 for AUC at the compression ratio of 24:1, the point where high disparity exists between performance and compression. In the second instance, the quality of the training and testing images were made to be the same, the performance of the CNN image based classifier shows that a CNN is efficient in handling images compressed with higher ratio as there exists manageable differences under various ratios. The results show that there is significant improvement in the performances as the compression ratios increase. The experiment in the third scenario examined the performance of the CNN on images of various qualities when trained with a fixed compressed images. The results obtained here indicate that the performance recorded for F1 score; 93.4% is the highest at the compression ratio of 48. The implication of this is that the ratio of 48:1 is capable of performing almost equal well on all higher and low quality samples. This study establishes the fact that the CNN is adaptable to maintaining its efficiency on images of different qualities once its parameters have successfully learnt. Though, the study utilizes an analytical algorithm to assess performance of classification on degraded pathological images, which were transformed into another form which might have defected the pixels contained in the images. To our conviction, the effort and all the previous ones have not studied the effect of the original pixels of the skin images in the performance accuracy of the skin diseases classification.

III. METHODOLOGY

A. Materials

In carrying out this study, dermatological HAM10000 dataset, published by the Medical University of Vienna, Harvard is used. The dataset is adopted in examining the performance of CNNs to classify dermatological skin diseases into seven different classes.

The dataset contains a total of 10,015 samples of skin images collected from different populations of various background. This sum is obtained from the total frequency of the disease types as shown in *Table 1*. These images were manually cropped with lesion centered to 800 x 600px at 720PDI. Manual histogram corrections as well were applied to enhance visual contrast and color reproduction [26].

TABLE 1. THE FREQUENCY DISTRIBUTION TABLE OF THE SKIN DISEASE TYPES

S/N	DISEASE TYPES	ACCRONYM	NUMBER
1.	Actinic keratoses and intraepithelial carcinoma disease	Akiec	327
2.	Basal cell carcinoma	Bcc	514
3.	Benign keratosis-like lesions	Bkl	1,099
4.	Dermatofibroma	Df	115
5.	Melanoma	Mel	1,113
6.	Melanocytic nevi	Nv	6,705
7.	Vascular lesions	Vsasc	142
Total			10,015

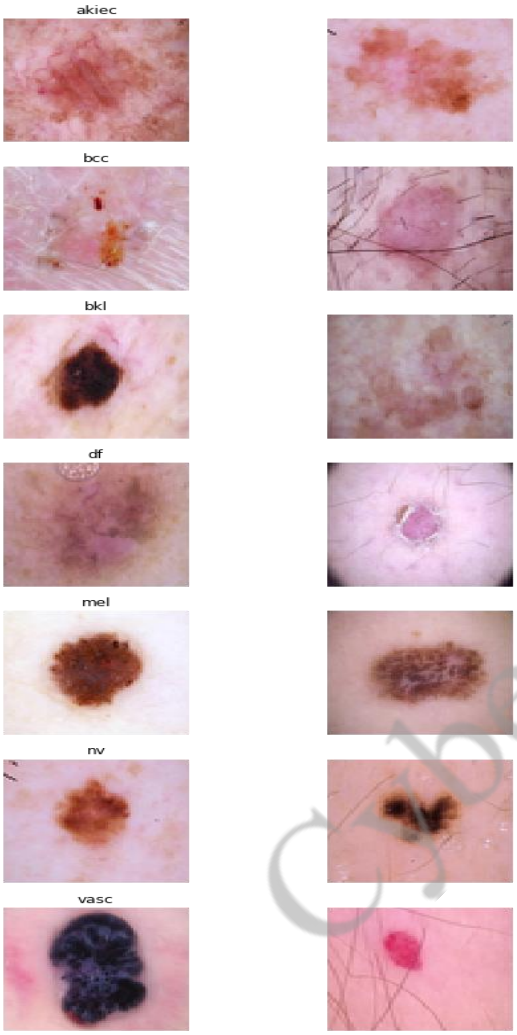


Fig. 1. Samples of infected skin image caption

The number of samples in the Melanocytic nevi (Nv) class is reduced by 5,000 to 1,705 to check its dominance over others, the number of samples considered for the study is 5,015.

B. CNN Architectural Design

In order to make a difference, three architectural networks are carefully designed for the purpose of realizing the set goal on image data. The scaled and unscaled pixel values of the images are then used to train the designed network architectures. The performance metric accuracy, which is the metric used in measuring the performance of the network architecture is observed in each case. The activation function used in output node is softmax. The choice for choosing softmax as the activation function is informed by its probabilistic interpretation in classifying values [27], especially when the values are more than two.

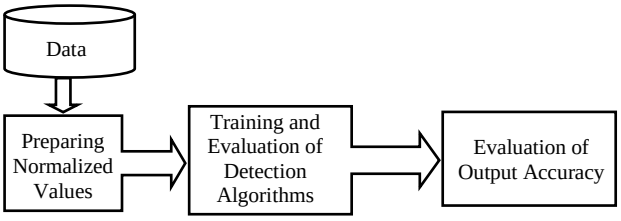


Fig. 2. Architecture of the detection process

C. Preparing Normalized values for the images

In preparing the data for processing, the pixel values of the skin images are extracted, some statistics are performed on the pixel values. The classifiers are then trained with the original (unscaled) and scaled pixel values.

To scale the pixels of the images for the training and evaluation of the CNN based image classifiers; 'global centering' and 'local centering' techniques are used. Also, 'division of image pixel value by the mean' and 'root of the division' are determined on the image pixel values. These statistics are discussed as follows:

1) Unscaled pixel

Here the original pixel values of the image data are directly fed into the classifier to train the model. The motive of using the original pixel values of the images is to set a base line for comparative analogy to meet the goal of this study. The function for this method is:

$$f(x) = x \tag{1}$$

2) Global Centering

Scaling of pixel values to have a zero mean. This is one of the popular data preparation techniques for image data. The method involves subtraction of the mean of the entire pixel values from each of the pixel values across the color dimension or channels. These are computed before being normalized to avoid feeding the network with negative values. Equation (2) below defines the global centering function.

$$f(x) = x - mean(x) \tag{2}$$

3) Local Centering

Calculating one mean per channel arrays. With this technique, the mean of the pixel values of each color channel is determined and subtracted per channel hereby centering the values of the pixels in the particular channel. The technique does not center the pixel values to zero but to values nearest to zero. Equation (3) defines the computational function for this technique.

$$f(x_i) = x_i - mean_{ichannel}(x) \tag{3}$$

4) Dividing by mean

The pixels are scaled by dividing the values of the pixels by their means. The function used here is defined (4)

$$f(x) = \frac{x}{mean(x)} \quad (4)$$

5) Root of the mean division

After dividing the value of a pixel by the mean, the square root of the division is further taken to reduce the value to more appreciable real computable values. The function applied to obtain the values used here is

$$f(x) = \sqrt{\frac{x}{mean(x)}} \quad (5)$$

D. Training and Testing

Different sessions of training and testing were performed to analyze the effects of different computed statistics on the performances of the classifiers. The standard classification performance metric accuracy is used to evaluate the classifiers' performances. Accuracy is the most intuitive performance measure which is a ratio of correctly predicted observation to the total observations.

After the preparation, each of the CNN based image classifiers is implemented using Python Anaconda library and Keras with the Tensorflow backend. The architectures of the designed CNN image based classifiers are detailed in *Tables 2*, *3* and *4*.

TABLE 2. ARCHITECTURE 1

Convolutional Filter	Filter Size	Activation Function
Conv2D Conv2D maxPooling2D	(32, (3, 3)) (32, (3, 3)) (2, 2)	Relu Relu
Conv2D Conv2D maxPooling2D	(32, (3, 3)) (32, (3, 3)) (2, 2)	Relu Relu
Dense Dropout	128 0.2	Relu
Dense Dropout	64 0.2	Relu
Dense	7	Softmax
Number of Parameters	1,680,807	

TABLE 3. ARCHITECTURE 2

Convolutional Filter	Filter Size	Activation Function
Conv2D Conv2D maxPooling2D	(32, (3, 3)) (32, (3, 3)) (2, 2)	Relu Relu
Conv2D Conv2D maxPooling2D	(64, (3, 3)) (64, (3, 3)) (2, 2)	Relu Relu
Dense Dropout	128 0.2	Relu
Dense Dropout	64 0.2	Relu
Dense	7	Softmax
Number of Parameters	840,807	

TABLE 4. ARCHITECTURE 3

Convolutional Filter	Filter Size	Activation Function
Conv2D Conv2D maxPooling2D	(32, (3, 3)) (32, (3, 3)) (2, 2)	Relu Relu
Conv2D Conv2D maxPooling2D	(64, (3, 3)) (64, (3, 3)) (2, 2)	Relu Relu
Conv2D Conv2D maxPooling2D	(128, (3, 3)) (128, (3, 3)) (2, 2)	Relu Relu
Dense Dropout	128 0.2	Relu
Dense Dropout	64 0.2	Relu
Dense	7	Softmax
Number of Parameters	707,239	

IV. RESULTS AND DISCUSSION

Performance metric accuracy is considered in measuring the performance of the CNN based image classifiers in the experiments. The results obtained from an experiment are the ratios of the correctly predicted observations to the total observations. The results of the training testing performance are shown in *Table 5*.

TABLE 5. THE RESULTS OF THE EXPERIMENTS

Statistics	CNN Classifier		
	Architecture 1 (Accuracy)	Architecture 2 (Accuracy)	Architecture 3 (Accuracy)
Unscaled pixel values	50.4	54.2	54.5
Local centering	58.39	59.4	56.8
Global centering	55.39	61.0	58.2
Division by mean	58.4	59.8	56.8
Root of division	60.0	61.8	60.8

It is observed from *Table 5* that all networks are very sensitive to the image pixels despite non-specific pattern of performances across the calculated statistics. The sensitivity to the values may be connected to the weights of the pixel values in each experiment. The network is more sensitive to smaller real values.

According to the results obtained in *Architecture 1*, classification accuracy rate of 60% is obtained from training the network with 'root of the division of x values by the mean(x)'. The training with 'division of x by the mean(x)' and 'local centering' perform higher after the 'root of the division' with approximate scores of 58.4% classification accuracy. The network performs lower when trained with 'global centering' with performance rate of 55.39% and least performance is obtained when it is trained with the 'original pixel values' of the skin images with an accuracy of 50.4%.

Similarly, in *Architecture 2*, the network performs best when trained with the 'root of the division of the x values by the mean(x)' with 61.8% and performs very low with 54.2% when trained with 'unscaled pixel values'. In contrast to the order of the performance in the *Architecture 1*, the performance of the network with 'global centering' comes next to the leading grade with 61%, while the training with the 'division of x value by the mean' comes third having performed at 59.8%. The network records 59.4% accurate

performance when trained with 'local centering', which is the fourth grade in performance record.

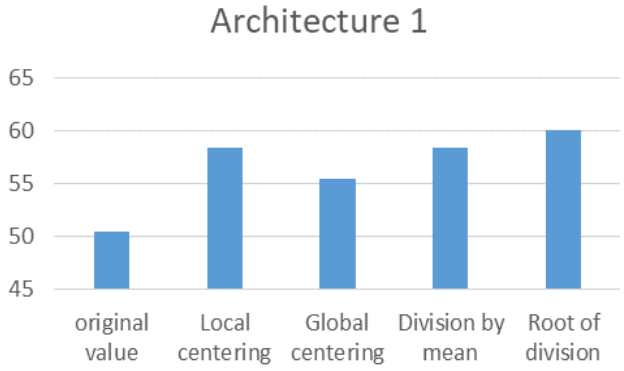
The results obtained from *Architecture 3* show that the network equally performs better when trained with the 'root of the division of x value with the mean(x)' than with trainings on other calculated statistics by producing an accuracy of 60.8%. As recorded in *Architecture 2*, the 'global centering' comes second in ranking with 58.2%. This time, the performances with both the 'local centering' and 'division by mean(x)' come third with accurate performance of 56.8% each while training with the 'original pixel values' records the least accuracy performance with 54.5%.

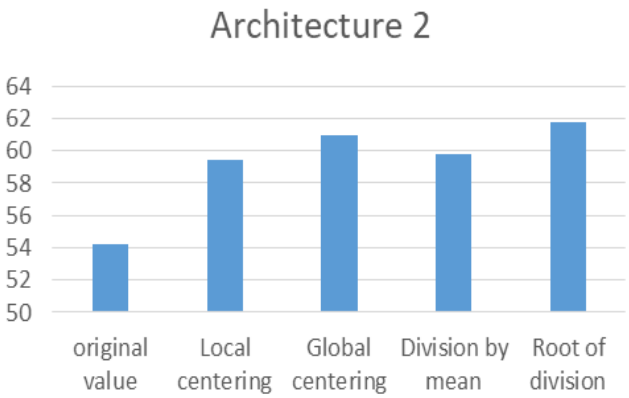
It is expected that the order of performance be maintained in the three network architectures, but this was not. While 'local centering' and 'division of x value by the mean(x)' techniques perform better than 'global centering' technique in the first *Architecture 1*, the performances of the 'global centering' technique in *Architectures 2* and *3* are better than the performances of 'local centering' and 'division by mean(x)' techniques. The discrepancy in the performance patterns across the three CNNs may be attributed to the small number of image data set used for the training [28].

However, it can be seen that the CNN architectures performances are consistently high when trained with the technique of 'root of the division of x value by the mean(x)' over other calculated statistics. The best performance with this technique can be attributed to the values involved whose range is very minimal due to the small sizes of the values of the calculated statistics which is very easy for an instance based algorithm like CNN.

Also, the performances of the networks when trained with the 'unscaled pixel values' of the skin images are generally low across all the CNN architectures. The networks perform the least on the original pixel values of the images. This is obviously connected to the fact that the values are only not preprocessed, but equally very diverse big, expectedly having a big range of values.

Pictorial representations of the results obtained from the experiments are further made in the comparison graphs in Fig. 3. The graphs provide visual analysis of the performances of the *Architectures 1, 2* and *3* on the statistics calculated on the image pixel values.





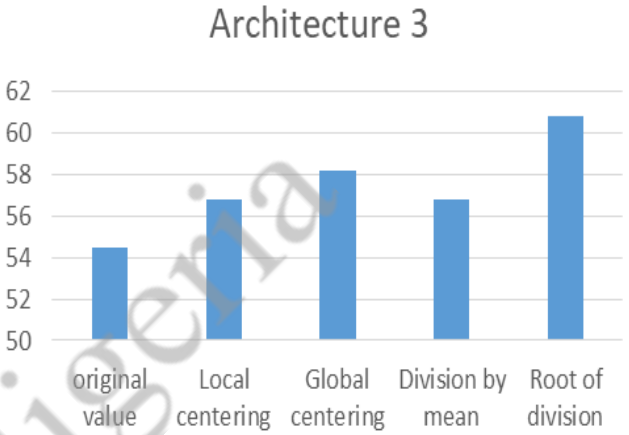


Fig. 3. Charts showing visual interpretations of the results

V. CONCLUSION AND FUTURE WORK

This study proposed a methodology and implemented on HAM10000 dataset for the study of effects of pixel scaling on the performance accuracy of CNN based image classifiers. The results obtained have thereby provided solution to the problem. From the analysis presented above, it is revealed that 'the root of the division of the x value by the mean(x)' outperforms all other calculated statistics, while the 'original pixel values' performs the least in all network architectures. Our results also show that a CNN image classifier performance is lower when trained with the original image pixel values but greater when the pixel values are scaled, irrespective of statistics calculated on the pixel values of the images. Finally, it is empirically being established that performance of the classifier is obviously affected by the image pixel values. This finding can assist in designing a more efficient skin disease classifier in the future.

The results obtained here emphasize the impact of calculated statistics on skin image pixel values using CNN architectures. With these results, having observed that there is no specific pattern in the order of performances of the network architectures on those calculated statistical values, it is a future task to enquire whether the parameters trained in an architecture have effect on performance accuracy of the skin diseases classification.

REFERENCES

[1] L. Daniel, M. D. Stulberg, A. Marc, M. D. Penrod, A. Richard, "Common bacteria skin infections," American Family Physician, vol. 66, issue 1, pp. 119-125, 2002.

[2] American Cancer Society (ACS), "Skin cancer," [Online] Available: www.amp.cancer.org>cancer, 2009.

[3] J. Johnson, "Common skin diseases and conditions", Medical News Today, March, 2017

[4] Mayo Clinic, "Diagnosis: Cancer screening," [Online] Available: www.mayoclinic.org, 1998.

[5] National Breast Cancer Foundation (NBCF), "Inc. About breast cancer," [Online] Available: www.nationalbreastcancer.org, 2019. 2019

[6] AnaPath, "Things to know about histopathology," [Online] Available: www.anapath.ch, 2019

[7]. G. Yanming, L. Yu, O. Ard, L. Songyang, W. Song, and S. L. Micheal, "Deep learning for visual understanding: a review. Neurocomputing," vol. 187, pp. 27-48, 2016.

[8] H. C. Shin, H. R. Roth, L. Lu, Z. Xu, I. Nogues, J. Yao, D. Mollura, and R. M. Summers, "Deep convolutional network for computer-aided detection: CNN architectures, dataset characteristics and transfer learning," IEEE Transactions on Image Processing, vol. 15, issue 2, pp. 430-444, 2006.

[9] H. Wang, D. Chong, D. Huang, and Y. Zou, "What affects the performance of convolutional neural networks for audio event and classification." 2019 8th International Conference on Affective Computing and Intelligent Interaction Workshops and Demos (ACIIW). pp. 140-146, doi: 10.1109/ACIIW.2019.8925277, 2019.

[10] D. Samuel, and K. Lina, "Understanding how image quality affects deep neural networks," Quality of Multimedia Experience (QoMEX), 2016 Eighth International Conference on IEEE, 2016.

[11] D. Mathieu, D. Karol, A. Kamel, H. Wassim, M. Lucc, and P. Maxime, "Study of the impact of standard image compression techniques on performance of image classification with a convolutional neural network," Diss. INSA Rennes; Univ Rennes; IETR; Institut Pasca, 2017.

[12] A. Sanchez, A. B. Moreno, and J. Velez, "Analysing the influence of contrast in large-scale recognition of neural images," Integrated Computer-Aided Engineering, vol. 23, issue 3, pp. 221-235, 2016.

[13] M. Chevalier, T. Nicolas, C. Mattheu, F. Jerome, H. Gilles, and D. Elodie, "LR_CNN for fine-grained classification with varying resolution, image processing (ICIP)," IEEE International Conference, 2015.

[14] P. K. Suresh, and J. Gaurav, "Effects of varying resolution on performance of CNN based image classification: An Experimental study," JCSE International Journal of Computer Sciences and Engineering, vol. 6, issue 9, pp. 451-456, 2018.

[15] D. Chen, D. A. Stow, and P. Gong, "Examining the effect of spatial resolution and texture window size on classification accuracy: an urban environment case," International Journal of Remote Sensing, vol. 25, issue 11, pp. 2177-2192, 2004.

[16] Pixel-Wikipedia. [Online] Available: www.en.m.wikipedia.org

[17] Image scaling–Wikipedia. [Online] Available: www.en.mwikipedia.org

[18] All about images. University of Michigan Library Research Guides. [Online] Available: www.guides.lib.umich.edu

[19] C. Prince, "Image pre-processing," 2018. [Online] Available: www.towardsdatascience.com

[20] J. Urvashi,"Why data normalization is necessary for machine learning models," 2018. [Online] Available: www.medium

[21] A. Marcelo, P. Fontelo, M. Farolan, and H. Cualing, "Effect of image compression on telepathology," A randomized clinical trial, Archieves of Pathology & Laboratory Medicine, vol. 124, issue 11, 2000.

[22] K. MD. Thomas, Z. Ralf, G. MD. Florian, S. MD. Sien-Yi, S. MD. Saadettin, H. Harald, and R. MD. Albert,"Lossless compression of jpeg2000 whole slide images is not required for diagnostic virtual microscopy," American Journal of Clinical Pathology, vol. 136, issue 6, pp. 889-895, 2011.

[23] L. Platisa, V. B. Leen, K. Asli, D. Richard, and P. Wilfried, "The influence of study design in digital pathology image quality evaluation: The need to define a clinical task," Journal of Medical Imaging, Doi: 10.1117/1.JMI.4.2.021108, 2017.

[24] P. Liron, L. Chi, H. Yue, G Huazhang, and K. R. Gustavo, "Impact of altering various image parameters on human epidermal growth factor receptor 2 image analysis data quality,". Journal of Pathology Informatics, Doi: 10.4103/jpi.jpi_46_17, 2017.

[25] G. Z. Farhad, Z. Svitlana, P. Bastian, M. Saeed, S. Peter, and H. N. W. Peter, "Impact of JPEG compression on deep convolutional neural networks for metastatic cancer detection in histopathological images," Journal of Medical Imaging, vol.6, issue 2. 2019.

[26] T. Philip, R. Cliff, and K. Harald, "The HAM10000 dataset, a large collection of multi-source dermatoscopic images of common pigmented skin lesions," [Online] Available: www.ncbi.nlm.nih.gov>pmc, 2018.

[27] K. Ayyuce, "Comparison of Activation functions for deep neural networks," [Online] Available: www.medium, 2019.

[28] X. G. Jiu, W. Zhenhua, K. Jason, M. Lianyang, S. Amir, S. Bing, L. Ting, W. Xingxing, C. Jianfei, and C. Tsuhan, "Recent advances in convolutional neural networks," arViv:1512.0710806, 2017.

Recognition Based Graphical Password Algorithms: A Survey

Jiya Gloria Kaka
School of information and communication technology
Federal University of Technology
Minna, Nigeria
jiyakaka7@gmail.com

Ishaq Oyefolahan O.
School of Information and Communication Technology
Federal University of Technology
Minna Nigeria
o.ishaq@futminna.edu.ng

Ojeniyi Joseph O.
School of Information and Communication Technology
Federal University of Technology
line 4: City, Country
ojeniyija@futminna.edu.ng

***Abstract*- User Authentication is an important aspect of information security. Alphanumeric passwords are the most common and widely adopted means of user authentication. Nevertheless, there are several disadvantages attached to the alphanumeric forms of authentication for example, user choose passwords that are easy to guess (dates of births, their names, car plate number) in other to remember them, because difficult passwords are not easily remembered; this brought about the alternative of graphical passwords, research have been carried out to proof that humans find it easier to recall images. This paper reviews 10 recognition based graphical passwords algorithm; common usability and security threats of these systems where analyzed. This paper also suggests future research directions.**

Keywords- Graphical Passwords, recognition based, user interface.

I. INTRODUCTION

Researchers have come up with numerous graphical password algorithms to help users memorize their passwords, passwords should be easy to use and secured, therefore, ten (10) recognition based graphical password algorithms were analyzed in terms of common usability and security threats. Security threats arise with the evolving technology, important document files are stored on devices, most of the devices we use today have applications such as bank applications and private documents that need to be secured [1]. The most widely used authentication method is the text based authentication method, a user registers a username and text password then provides this information upon log in [2]. However users tend to choose passwords that are simple in order to remember them and that makes them easily guessable, they also tend to forget their passwords when strong, most times, they try to write them down thereby jeorpardising the security, or use same password across different platform [3] this brought about the alternative of graphical password to overcome the drawbacks of the tradional text passwords. According to [4] the fact that the human brain processes images easily makes graphical passwords superior to textual passwords. The Graphical password scheme is a form of authentication where users draw/click or select images as their pass images and are asked to redraw or reselect this image upon sign in [1]. Psychology research has been carried out to propose that humans recall pictures/images better than texts [5], similarly, [6], also established the fact that if users authentication tasks are personalized to their cognitive features it will assist the users to be efficient in processing details cognitively as well as task execution performance and in due course improve their experience and acceptance of such tasks [6]. This paper reviews Ten (10) recognition based graphical password algorithms, common usability and security threats were analyzed.

II RELATED WORK

Twenty five (25) recognition based graphical password systems was reviewed by [1], their study is aimed at providing countermeasures and suggestions to mitigate security threats, the security threats addressed in their research includees guessing attack, direct observation attack & frequency of occurrence, a comparison table was presented at the end of their study. Similarly five (5) graphical password authentication techniques was reviewed by [7] in terms of registration and log in time in seconds. Techniques from recognition based, recall based and cued recall based was studied, a general performance analysis was provided. In the same light, [8] discussed the advantages and limitations of graphical password authentication techniques, at the end of their study suggestions were made on enhancement of future graphical authentication scheme. The paper also proposed solutions to prevent shoulder surfing attacks, hidden camera and spyware attack [8]. An attempt to answer the question “are graphical passwords more secured than text passwords” was made by Jaffar and Ahmed in their study which was aimed at evaluating graphical password schemes in terms of attack resistance and usability [9].

However a comprehensive review in terms of usability and security threats involving recognitiion based graphical password is needed. This paper reviewed 10 recognition based graphical password algorithms from 2000 to 2020, a comprehensive survey on usability according to the ISO standard was carried out on the selected algorithm coupled with security threats (shoulder surfing attack, frequency of occurrence and social engineering), a comparison table is presented at the end of the study to guide future research study and researchers interested in coming up with new graphical password techniques.

III METHODOLOGY

This research is conducted by gathering information on present recognition based graphical password schemes. Information was gotten from different sources such as journals, conference proceedings, papers and legitimate websites such as google scholar. The selected recognition based graphical password scheme were evaluated to unveil the strength, weaknesses, usability and security aspect of the scheme. The results from the survey shows the present challenges and strengths of the recognition based graphical password scheme.

IV OVERVIEW OF THE GRAPHICAL PASSWORD AUTHENTICATION CATEGORIES

There are two categories of the graphical password authentication scheme which are both knowledge based authentication, these are:

- Recognition based graphical password scheme
- Recall based graphical password scheme

Recognition based graphical password scheme creates a platform for the user to select pictures from a variety of images provided, during authentication the user is asked to recognize the previously selected images to gain access hence, the name recognition based graphical scheme.

Recall based graphical password scheme gives the users an opportunity to recreate previously created passwords, users are either given hints or reminders (cued recall based) or asked to reproduce the passwords without reminders (pure recall based)

V. REVIEW OF SOME SELECTED RECOGNITION BASED GRAPHICAL PASSWORD SCHEMES

Some selected recognition based graphical passwords are reviewed in this section from 2000 to 2020

A. PassFace Sheme

This scheme was developed in the yeaar 2000 by a commercial company (Real user corporation) in an attempt to replace the traditional passwords with passface based on the argument that the mind can remember human faces easily making passfaces memorable [10], this scheme gives users an opportunity to select three (3) to seven (7) faces as their pass image, during the authentication process the users are given a trial version of authentication to get familiar with the process then requested to select each at a time their registered pass images from groups of nine faces each set of 9 contains random images [11]. This process is evidently time consuming, in a recent performance analysis conducted by [7], they stated that it takes 3 to 5minutes to register images.

Fig. 1. An example of PassFaces

In a research by [12] on user choice in graphical password scheme in 2004 advised against PassFaces stating that users select faces from the same race or most attractive, making the password easily guessable or predictable, they suggested that users should be educated on better password choice or forbid/limit the user choice of passwords.

It is easy for the attacker to attack the scheme using mouse clicks and keypad(keyboard) as it is notable for the attacker to see the pass images being selected by the user.

B. Déjà Vu

The Déjà vu scheme is one of the earliest proposed recognition based graphical password scheme, where users create image portfolio from a given set of images, during the authentication process the system presents the images from the user's portfolio and other decoy images, the user must select correctly the images from her portfolio to gain access, after portfolio creation process users undergo the training process to help memorability. It was documented that the creation time for the Déjà vu system is 45seconds while login time after 1week is 36seconds [13]. The strength of the system includes the fact that about 90% of the users had a successful login, but selecting a set of images to make a portfolio can be time consuming and tiring.

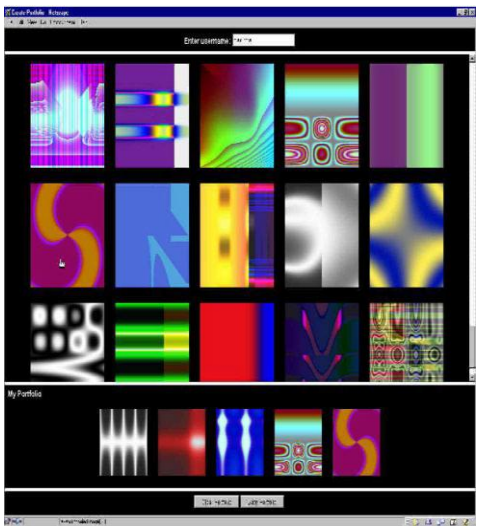


Fig. 2. Random Art used by Dhamija and Perrig.

C. *Triangle scheme and moveable frame*

In 2002 Sobrado and Bridget proposed various graphical password technique to overcome the challenge of the shoulder surfing threat. The user choses a pass image from a set of predefined images, upon login an invisible triangle is formed using the three pass images the user has chosen, the user must click inside the convex hull space, sobrado and bridget suggested the use of 1000 images in the login phase to increase password space, but this will make the display of images crowded and users will find it hard to locate their pass images on time [14]

Fig.3. Triangle Scheme

Also, in 2002 Sobrado and Bridgte proposed the moveable Frame Scheme using the same idea as in triangular scheme, here the user selects three pass objects upon authentication the user moves the frame with the images by dragging the mouse around the frame till the other two pass images lines up. The process is repeated several times to avoid accidental or random log in.

D. *Picture Password*

Jansen et al proposed a recognition based graphical password scheme for handheld devices/mobile devices, the strength of their algorithm includes embedded salting. During the registration phase a user selects a theme (cat,sea etc), then 30 thumbnail images are presented to users for selection in a 5by6 matrix, images can be chosen individually or by pair selection, upon login users selects the images chosen in the correct sequence, each thumbnail image generates a numerical password, the major drawback of this is the numerical password generated is shorter than textual passwords length [15]

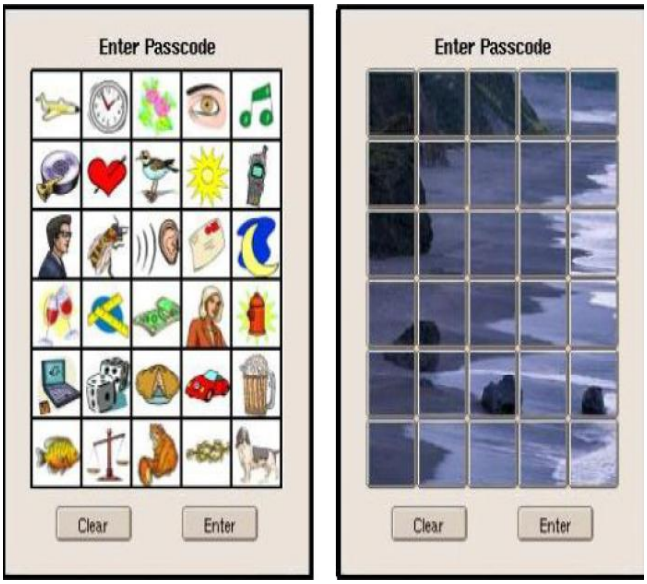


Fig. 4. An Example of the picture password on a PDA Screen

E. *A Secure Recognition based Graphical Password by Watermarking*

In 2011 [16] proposed a watermarking technique in an attempt to solve the challenge of image gallery attack and shoulder surfing. The users are presented with a 5by5 matrix and select 3 images as their pass images the images selected generate a string and are stored in a server [16].

Fig. 5. Images with associated string

F. *Select to Spawn: A novel Recognition based Scheme*

In this scheme the users are presented with a set of images, they select an image from the predefined images. The image selected is divivded into 16 (4*4 grid) in a different window. This process is continuous and stops depending on the user. Then the images selected by the user from the different windows form the password. The drawback of this scheme

involves prolonged registration and log in time, one of its strength includes a large password space which is about 270 million (approx.). [17]

G. *A Hybrid Graphical User Authentication Scheme by Swaleha & Sarosh*

This scheme was proposed mainly to build resistance against shoulder surfing attacks. The scheme combines recognition based scheme and dynamic graphics. During registration the user is provided with a 4*4 image grid and ask to select 5 images, the images has a code attached to them, the user enters this codes in order to select the images, upon log in a colored ball is displayed coupled with the image portfolio in login phase 2. The user is expected to remember the color of the ball associated with each image, the log in is in five sessions [18]. The log in process in this scheme is lengthy thereby increasing the log in time, the scheme is also not suitable for those with colour blindness.

H. *Shoulder Surfing Resistant Graphical Passsword Technique*

This technique was proposed in 2016 [4], it is an improvement on the previously proposed technique by [19] "A new graphical password: combination of recall and recognition based password". A user is presented with 25 images and a question set, he picks 3 questions from the question set and pass images as passwords. Upon login the user enters his username and pass images in the correct sequence, the order of questions will be random and the user clicks on the correct ROA's (Region Of Answers).

Fig.6. Step I Registration Phase

Fig. 7. Step II Registration Phase

The registration phase I & II from the images above shows the region of answers by the left and the images to be selected appear by the right, the user first creates a profile, selects images and then three question set.

Fig. 8. Step I Login Phase

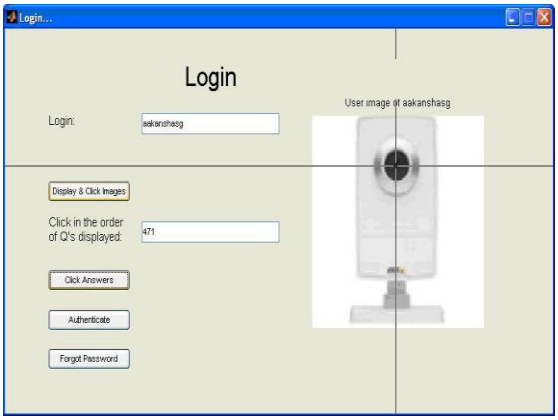


Fig. 8. Step II Login Phase

The login phases I and II provides the user with the 25 set of images and question set, the users are expected to choose accurately the images selected during registration in a sequential manner. To be authenticated the user has to enter a

correct username, for step II login the order of questions are randomized.

In the proposed system by Akansha users are to select pass images not less than 6. A session password is then generated based on the pass images. The pass images selected are put in a panel below the grid which disappears after 5 seconds so it can be remembered easily. This is the improvement made to make the previous system more secured. The other additions to their system include email id, mobile number. The system can be considered as secured but not usable as it takes longer to log in.

I. A Novel Hybrid Password Authentication Scheme Based on Text and Image by Mackie and Yildrim

The proposed system is of texts and images combined aimed at reducing phising attack, if a user is deceived to release his text password it will be difficult to release his image password. This scheme is also aimed at reducing the log in and registration time. During registration the user is expected to memorize the key characters provided. The key characters are associated with their images. Upon logging the user can decide to make the images invisible and just enter the key characters. The drawback of this system includes shoulder surfing, its strength includes resistant against brute force attack. [20]

J. Graphical Passwords: Behind the Attainment of Goals

The proposed approach is a combination of recognition based technique, distorted images, an email-id for recovery and visual cryptography. The registration phase has three sessions, the first session secures the details of users, in the second phase user id is transformed into two images through visual cryptography, one image is stored in the database and the order is sent to the user. The login comprises of four sessions. The user submit the image sent, a distorted 5by5 image grid is displayed, the user selects the pass images. [21] . The strength of this approach includes: no image is highlighted when a user selects images, this aimed at preventing shoulder surfing attack. Its major drawback is its lengthy login process.

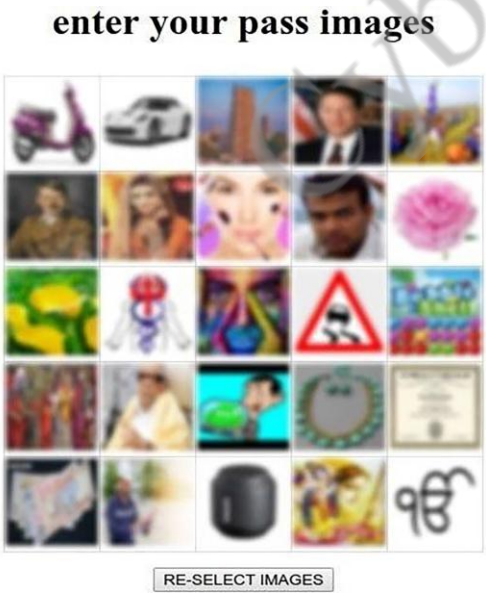


Fig. 6. blurred images presented

VI. *Attacks Common to recognition based graphical Passwords*

This section presents some common attacks and security threats that are common to recognition based graphical passwords.

A. The shoulder surfing attacks

The shoulder surfing attack is also known as the peeping attack, this attack enables an attacker or observer look over the shoulder of an authorized user to gain their password combination, the shoulder surfing attack is one of the major security threat on graphical passwords most especially recognition based graphical passwords. Researchers have tried to come up with approaches to prevent this attack. Randomization algorithms has been one of the best approaches to prevent this attack, although uniform randomization also leads to frequency of occurrence attack.

B. Frequency of Occurrence Attack

The frequency of occurrence attack(FOA) is most common to recognition based graphical passwords with invariable and consistent randomization algorithm. Graphical password approaches with large amount of decoy is exposed to the FOA, the pass images will have to appear at every login with just a limited number of decoy set in every challenge.

C. Social Engineering

In this type of attack an attacker interacts with an authorized user to gain access to their pass images, this form of attack may be particular difficult for some graphical password approach as it is difficult to describe images, but easy on other graphical password schemes such as recognition based, for example PassFaces that uses facial expressions or a people of a particular race.

VII. Usability

Usability according to the ISO standard(ISO 9241-110) is the usage of a system to achieve a specific purpose through effectiveness, efficiency and satisfaction [22]. Usability features from the ISO is shown in table 1 below

Table 1. usability features from the ISO standards

Usability features	Attributes	Attributes for GUA	Abbreviation
Effectiveness	Reliability & accuracy	Reliability & accuracy	R&A
Efficiency	The utilization in real word	Applicable	Applicable
Satisfaction	Easy to use	Use the mouse easily	Mouse usage
	Easy to create	Select simple way to create the password	Create simply
	Easyto memorize	Meaningful	Meaningful
		Memorability	Memorability
	Easy to execute	Select simple steps of registration & login	Simple steps
	Good view	Select good interface	Nice interface
	Easy to understand	Simple training session	Training simply
	Pleasant	Pleasant picture	Pleasant picture

VIII. Comparison on security and usability of the selected recognition based algorithms

Algorithms	Shoulder surfing attack	Frequency of occurrence attack	Social engineering attack	Usability features								
				Satisfaction							effectiveness	efficiency
				Easy to use	Easy to create	Memorability	Easy to execute	Good interface	Easy to understand	Meaningful pictures	Reliability & Accuracy	Applicability
PassFaces (2000)	×	×	√	√		√		×	√	√	√	√
Déjà vu (2000)	×	×	×	√	×	√	√	×	√	×	√	√
Triangule scheme (2002)	√	×	√	×	×	×	×	×	×	√	√	√
Picture password (2004)	×	×	√	√	×	×	√	√	×	√	√	√
watermarking (2011)	×	×	×	×	√	-	×	√	--	√	×	√
Select to spawn (2012)	×	√	√	√	√	√	√	×	×	-	√	√
Swaleha & Sarosh (2015)	√	√	√	×	×	×	×	×	×	-	√	×
Aakansha et al (2016)	×	×	√	×	×	×	×	√	×	√	√	√
Mackie and Yildrim (2018)	√	√	-	√	×	×	√	√	×	-	√	√
Ankitha, et al. (2020)	×	√	-	×	×	√	×	√	×	×	×	√

X: vulnerable √: not vulnerable - : not researched

VIII. CONCLUSION

In this paper, ten (10) recognition based graphical password algorithms are reviewed including hybrid passwords involving text and images. From the comparison table above shoulder surfing attack remains a challenge for graphical password authentication, although researchers have come up with algorithms to combat this challenge, users find it hard to easily create and understand recognition based graphical password scheme. Another aspect researchers should look into is the tradeoff between the usability and security of graphical passwords and find a balance between them. A naturalistic experimental evaluation on graphical password system was carried out and the results showed a trade-off between usability and security [23].After the survey carried out on the ten recognition based graphical password algorithms the ISO standard for usability was used to make a comparison table for the chosen algorithms, together with a survey on some attacks.

REFERENCE

[1] I. Amanul, P. Lip, O. Fazidah and C. ku, "A review on Recognition Based Graphical Password Techniques," *Computational Science and Technology*, pp. 503-512, 2019.

[2] S. Xiaoyuan, Z. Ying and O. Scott, "Graphical Passwords: A Survey," *IEEE*, 2005.

[3] A. Hussain, P. Maria, D. Paul and F. Steven, "Graphical One-Time Password GOTPass: A usability evaluation," *Information Security Journal: A global Perspective*, pp. 94-108, 2016.

[4] G. Aakansha and W. Vijaya, "The Shoulder Surfing Resistant Graphical PasSword Authentication Technique," in *Procedia Computer Science*, 2016.

[5] S. Lionel, "Learning 10,000 Pictures," *Quarterly Journal of Experimental Psychology*, pp. 207-222, 1973.

[6] B. Marios, C. F. P. G. and G. S. , "The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective," *Computers in Human Behavior*, 2017.

[7] M. Hemamalini, A. Nahomiyal and S. R, "Performance Analysis of Graphical Password Authentication Techniques," *Our Heritage, UCG care listed journal*, vol. 68, no. 4, pp. 271-278, 2020.

[8] P. Shikhar, J. Akarsh, A. Yash and S. Bharti, "Survey on Graphical Password Authentication System," in *Springer*, 2021.

[9] J. Jaffar and Z. Ahmed, "Ev aluation of graphical password schemes in terms of attack resistance and usability," in *IEEE*, 2020.

[10] B. Sacha and S. Angela, "Are PassFacess more usable than Passwords?," *Springer*, 2000.

[11] "About Passfaces," 2005. [Online]. Available: http://www.realuser.com.

[12] E. Hadyn, S. John and D. Graham, "identification of familiar and unfamiliar faces from internal and external features: some implications for theories of face recognition," *ResearchGate*, vol. 8, pp. 431-439, 2004.

[13] D. Rachna and P. Adrian, "Deja Vu: A User Study Using Images for Authentication," in *Prooceedings of the 9th USENIX Security Synposium*, Denver, 2000.

[14] L. Sobrado and J.-C. Bridget, "Graphical passwords," in *The Rutgers Scholar:An Electronic Bulletin of Undergraduate Research*, Camden, 2002.

[15] W. Jasen, "Authenticating mobile device users through image selection," *The Internet Society: Advances in Learning, Commerce and Security*, pp. 184-192, 2004.

[16] L. Arash, M. Azizah and M. Maslin, "A Secure Recognition based Graphical Password by Watermaking," in *11th IEEE International Conference on Computer and Information Technology*, Malaysia, 2011.

[17] U. Mohammad and R. Mohammad, "Select-to-Spawn: A Novel Recognition-based Graphical User Authentication Scheme," *IEEE*, 2012.

[18] S. Swaleha and U. Sarosh, "A Hybrid Graphical User Authentication Sheme," in *2015 international conference on communication, control and intelligent system*, 2015.

[19] H. Asraful and I. Babbar, "A new graphical password:combination of recall and recognition based approach," *World academy of science engineering and technology international journal of computer, information, systems and control engineering*, 2014.

[20] I. Mackie and M. Yildrim, "A Novel Hybrid Password Authentication Scheme Based on Text and Images," in *IFIP Annual conference on data and application*, 2018.

[21] V. Ankitha, V. Deepthi, P. Vineetha, P. Raveendra, S. Ji Sun and A. Goutham, "Graphical passwords: Behind the attachment of goals," *Security and Privacy*, pp. 1-10, 2020.

[22] ISO, "Ergonomics of human-system interaction-part110: Interaction principles," 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en.

[23] Z. Moustapha and S. Pascal, "Security and Usability: A Naturalistic Experimental Evaluation of a Graphical Authentication System," in *Congress of the international Ergonomics Association*, 2018.

[24] G. Aakansha and W. Vijaya, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," in *7th International Conference on Communication, Computing and Virtualization*, India, 2016.

A Review of Informative Data Level Resampling Approaches for Solving Class Imbalanced Problem

Dako Apaleokhai Dickson
Computer Science Department
Federal University of Technology, Minna
Minna, Niger State, Nigeria
dako.pg919379st.futminna.edu.ng

John Kolo Alhassan
Computer Science Department
Federal University of Technology, Minna
Minna, Niger State, Nigeria
jkalhassan@futminna.edu.ng

Solomon Adelowo Adepoju
Computer Science Department
Federal University of Technology, Minna
Minna, Niger State, Nigeria
solo.adepoju@futminna.edu.ng

***Abstract*— In the field of machine learning, Imbalanced learning being one among the most challenging classification problems which is also very common among application dataset. Although, imbalanced approach has received increasing attention over the years due to the necessity of handling real world dataset which are usually skewed in nature, possessing various data difficulty factors. The goal of this work is the review of resampling techniques to identify if data intrinsic characteristics were mostly considered during the design of resampling technique. It went further to categorise the techniques into distance, cluster and evolutionary based method, from the result of said process, also presented the advantages and disadvantages of each category and finally, stating general achievements and drawbacks in resampling approaches. The total search that was conducted for this work, yielded 227 papers published within the last two decades, with emphasis on the last. These articles from imbalanced data domains went through different filtering methods, before been finally reduced to 52. It was presented in this work that distanced based methods have received more attention when compared with cluster based and evolutionary based method, this may be due to its merits, which have been presented in this work. From several previous works, data intrinsic characteristics have been found to be more problematic to learning classifier than imbalanced problem. However, from the findings of this work, it was established that despite the report by publications that data intrinsic characteristics are more harmful than imbalanced nature of data, most existing resampling techniques do not regard data intrinsic characteristic in their design, this may be due to the popular nature and attention drawn by imbalanced problem in publications. However, there are some limiting factors that also need to be resolved generally on all the resampling methods such as: lack of consideration of possible relevant examples in undersampling process, lack of outstanding examples interrelationship and similarities evaluation methods. For future work, a robust resampling technique that will critically consider data difficulty factors when evaluating the region and the examples to oversample and undersample. Resampling techniques should also be evaluated against the different types of difficulty factor so as to ascertain the difficulty type it is best used on to achieve great result.**

Keywords—Machine Learning, Imbalanced data, Preprocessing, Data Level Approaches, Data intrinsic characteristics, Data difficulty factors

I. INTRODUCTION

With the advancement of technology and the internet, there have been a copious data generation every day. Therefore, it becomes important to improve the deep understanding of knowledge discovery (KD) and analysis of raw data to enhance decision-making in different industries. An evolution has been done on classification of data through the learning process. This process becomes more complex when the dataset is imbalanced [1]. Among the challenges of supervised machine learning process, one crucial problem is learning from imbalanced data [2]. Imbalanced data is one of the most sensitive problem in data mining and machine learning, which exist in most real-life datasets [3]. Dataset are said to be imbalanced when one or more of its class(es) has a smaller number of examples (minority class) when compared to other class(es) (majority class) in the dataset by a substantial margin; when the dataset consists of two classes or classes above two it is referred to as binary or multiclass respectively. For example, in a sample of 100 patients, the number of patients negative to a particular deadly illness such as covid-19 is 98 and 2 are positive to the illness [4],[5].

When class imbalanced (as in the covid-19 case illustration) is not looked into during classification, learning algorithms or models can be engulfed by the majority class while the minority class tends to be neglected or undiscovered [5]. Knowing that learning task can be complex with class imbalance [6], it is also important to note that the disproportion between class examples is remarkably not solely the main source of potential difficulties [7], [8], [9]. Therefore, it is important that, when considering and processing class examples ratio between minority and majority classes, to also analyse the data complexity and the data intrinsic characteristics such as sub-concepts, small disjuncts, noise, borderline, rare and outlier regions [10], [4], [11]. When these two degrading factors (that is, class imbalanced and data intrinsic characteristics) occurs jointly in a dataset, they severely affect the recognition of the minority class [8].

The objective of this study is the review of resampling techniques to identify if data intrinsic characteristics where mostly considered during the resampling process. It went further to categorise the techniques into distance, cluster and evolutionary based method, from the result of said process, also presented the advantages and disadvantages of each

category and also stating general achievement and drawback in each category. Finally, the methods used to determine the degree of similarities in multiclass imbalanced dataset was also studied. To achieve this objective, an in-depth study of the state-of-the-art resampling techniques will be conducted in order to be able to identify potential aspects that could lead to a breakthrough in the field.

The rest of this publication is organized as follows: Section II, introduces the basic strategies for dealing with class imbalanced problems and related studies. In section III we covered research methodology for this work, whereas Section IV presents the research findings, after that, section V provides the recommendations. Finally, Section VI also state the conclusion that was ascertain from the analysis of the resampling techniques and possible research gap and directions.

II. LITERATURE REVIEW

A. Preliminary

The approaches used for resolving the problem of imbalanced data are either the data level (preprocessing), algorithmic level or cost sensitive learning approaches and some other techniques that can be integrates with any of the aforementioned approaches are the techniques include ensemble and clustering learning. These approaches can be sub-divided into these categories as presented in figure 1

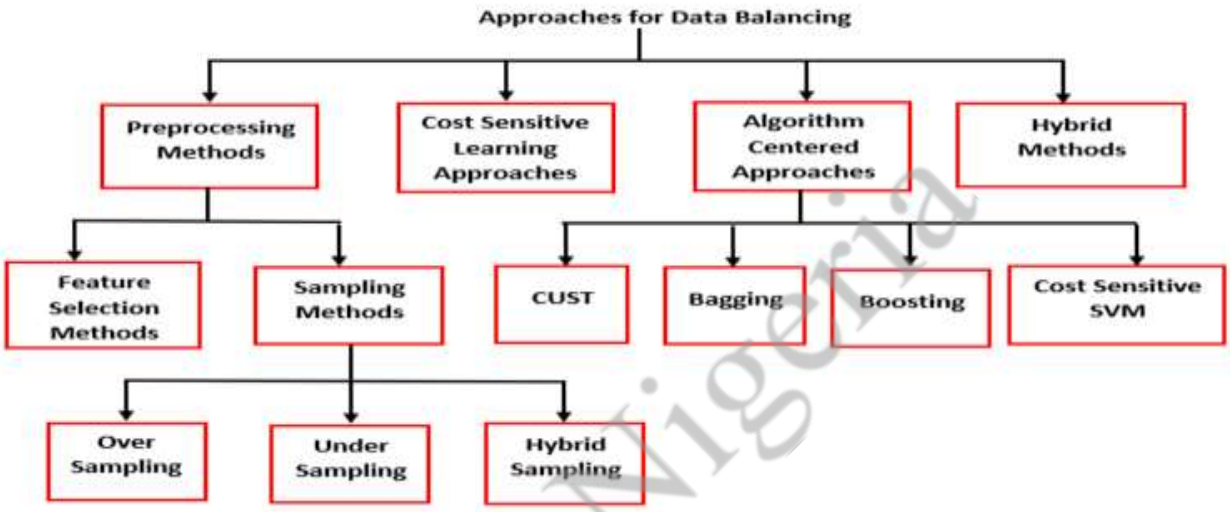


Fig. 1. Approaches to balancing dataset [11].

1) Algorithm Centered Approaches: With the Algorithm Level Approaches, the classification algorithm is modified to ease the learning task more precisely with respect to the minority class [13]. Algorithm level approaches can be perceived as a substitute approach to data preprocessing approach for handling imbalanced datasets. This approach is focused at modifying the classifier learning procedure itself, unlike data level approach that focus on improving the training dataset in order to combat class skew [14].

2) Cost-Sensitive Learning Approaches: Cost-sensitive learning refers to a specific set of algorithms that are sensitive to different costs associated with certain characteristics of considered problems [14].

3) Hybrid Approaches: This approach combine the data and algorithm level approaches to combat the problem of imbalanced data classification task [12]. This method integrates preprocessing methods with inbuilt mechanisms, especially merging classifier ensemble with a preprocessing technique [14].

4) Ensemble Learning: Ensemble learning methods combine ensemble learning technologies with any preprocessing or algorithm-level methods to further enhance classification performance [15]. This approach is known to improve the accuracy when compared with the usage of a single classifier [14].

5) Resampling Approaches: Resampling approaches also known as preprocessing methods: This is the application of techniques to respectively identify or generate a specific number of examples from the majority or minority class in order to rebalance the class examples thereby producing improved dataset for classification [16]. These approaches work by informatively altering the data samples and tries to minimize the imbalance ratio between classes [12]. Resampling method is the most widely used approach to deal with the problem of imbalanced datasets [1]. An edge of the resampling approach over other approaches is that, it can be used as a general method to solve the imbalance problem independent of the classification algorithm that will be used for classification [17].

According to [14], the categories of resampling techniques can be grouped into:

a) Undersampling: This method eliminates subset from the original dataset most often from the majority class examples.

b) Oversampling: This method on the other hand, create new examples by replicating examples or generating synthetic examples from existing minority class examples.

c) Hybrid: Hybrids methods combines both undersampling and oversampling approaches.

B. Data Intrinsic Characteristics (Nature of dataset)

Class imbalance is often the most mentioned causal element that decline classification performance, however, there are situations in which better performance can be reach

by standard classifiers even in the presence of harsh class imbalance, such performance can be obtained if the dataset is considered linearly separable (or of low complexity). The situations that affect the non-linearly separable dataset are most often related to the following data intrinsic characteristics [14], [11].

a) Safe Examples: The safe examples are instances that belong to the same class and are found in an homogeneous region in the input space [14].

b) Borderline Examples: The borderline examples also known as overlapping examples are instances from different classes which are found mostly within the boundary region between classes [4]. This examples types occurs when the input features are not sufficient to rightly differentiate among examples of different classes, and the same regions of the input space consist of examples from different classes [14].

c) Rare (Small Disjoint) Examples:. The rare examples of a class are isolated pairs of instances located within the safe examples of another class and distant from the borderline examples. It is common within real world dataset, that the underlying "concept" underneath a class is split into several sub-concepts, stretch over the input space [14].

d) Noisy (Outliers) Examples : Noisy examples are individual instances of other class(es) located within the safe or homogenous examples of another class [18].

C. Related Studies

As it was noticed in publications before the last two-decade, heuristic duplicating minority class examples and deleting majority class examples were the concept of resampling. Even research work, such as the popular [19] Synthetic Minority Oversampling Techniques SMOTE which only focused on using informative approach to generate synthetic examples. However, there was no informative method used to consider the characteristics of minority examples to be generated or the input space that is more preferred to carry out this process. Adaptive Synthetic Sampling Approach ADASYN [20], also uses weighted distribution for different minority class instances according to their level of difficulty in learning. The wok of [21], SMOTE was not grounded on any solid mathematical theory.

Data intrinsic characteristics have been identified as an input space of examples with different complexity in dataset. [22] in their work also stated that homogenous region examples are more often than not unchallenging for all considered classifiers but borderline, rare and outlier are actual source of difficulties which deteriorate classification to a great degree. As their method was based on a simple analysis of a fixed number of neighbours, checking whether the assigned labels can correctly reflect the known distribution of examples. [22] concluded by stating that it is worth seeking for techniques which are able to evaluate the nature of real-world datasets and their degree of difficulty during class balancing. [4] proposed a method for the recognition of these categories of data intrinsic characteristics examples in real dataset, which is based on the analysis of class distribution in a local neighbourhood of the examined example. The methods used in modeling this neighbourhood have been introduced as: with kernel functions and with k-nearest. [4] analysed that most dataset ordinarily has all types of minority examples, but in dissimilar proportion. It also proposed how one should handle each example type, also stating that the global imbalance ratio and data size are considered not as influential as the mentioned examples types. Finally, stating that the results of this analysis should be exploited for developing new algorithms for learning classifiers and preprocessing methods. Extending the works of [22] and [4], [8] worked on local neighbourhood data intrinsic characteristics in learning classifiers for class imbalanced problem. The types of examples were evaluated using promoted tuning bandwidth of a kernel neighbourhood or k nearest neighbours. However, unlike the earlier studies, [8] have managed to introduce an individual size of neighbourhood for each datasets. As a direction for future work, exploiting information about types of examples present and their data intrinsic characteristics could serve as the basis for designing new class imbalanced algorithms. [23] proposed a new method for examining the data intrinsic characteristics of examples in multiclass dataset. The method evaluates the safe level of examples utilizing the outcome of analyzing the neighborhood of the minority class example and also the additional similarity information of neighboring classes. The oversampling and undersampling process was performed on examples based on the safe level value. The safe level evaluation method could be used to design new preprocessing technique by exploiting safe levels to flexibly adjust resampling, however, this method has not been evaluated against complex relations among classes.

Here are some insights from these papers 1). Data intrinsic characteristic analysis deserves more attention, as much as is resampling techniques, this is because balanced dataset which is complex will still experience difficulty during classification. 2). Other than kernel neighbourhood and k nearest neighbours, safe level which utilized degree of similarities information between examples can also be used to analyse examples to oversample or undersample..

1) Oversampling Approaches:

Earlier days of data level preprocessing have been with the heuristic approaches which involves duplicating the examples of the minority class(es) (that is Random Oversampling (ROS)). The simplicity of implementation has made it the most preferred technique that is commonly used for oversampling [21]. Since non-informative duplication of samples is done, the resulting dataset are likely to suffer from overfitting. The weaknesses of ROS open a research gap for [19], who presented the SMOTE algorithm, that provided solution to ROS overfitting. Instead of just replicating existing examples, the technique give rise to artificial samples. The SMOTE algorithm is a distanced based method that is implemented based on the nearest neighborhood between examples. Firstly, it selects a random minority observation a. Next, among its k nearest minority class neighbors, instance b is selected. Eventually, a new sample x is generated by randomly interpolating the two samples. However, this algorithm has its own shortcomings, one among several is that SMOTE randomly select an example to oversample without considering the data intrinsic characteristic of minority example. SMOTE algorithm may increase rare and noisy examples thereby deteriorating performance. The weaknesses of SMOTE opened another research direction which have led to many derivatives of SMOTE algorithm. Examples of such works includes Borderline-SMOTE, Safe- Level-SMOTE [24], LS-SMOTE [25], Enhanced SMOTE Algorithm [26], Modified SMOTE [27], MW-SMOTE [28], AB-SMOTE, CAB-SMOTE, HCAB-SMOTE [29] and many others.

Despite the success that have been achieved by SMOTE and its derivatives, some researcher and practitioners [9] still

uses ROS for oversampling process. Since overgeneralization, overlapping of minority examples, are shortcomings of ROS and SMOTE. Just like in derivatives of SMOTE, region evaluation, examples and class information analysis and a combination of both have also been applied on ROS [30].

[1], presented a study of the different techniques (modified SMOTE) that are used to solve the imbalanced dataset, and finally proposes a novel oversampling technique to tackle the binary classification of imbalanced dataset problem.

The proposed technique main focus was to generate new synthetic minority examples that reduces the difference in the number between majority and minority dataset. To achieve this goal, majority data samples are considered while generating the new minority data samples. The algorithm gets the k-nearest neighbors of all examples in the dataset. It then calculated the distance between both the nearest majority neighbor and the nearest minority neighbor multiplied by random number. Afterwards, generated the new synthetic examples depending on the randomly selected minority neighbor adding to it the difference in distance between the nearest majority neighbor and the nearest minority neighbor.

This technique is evaluated on different datasets over K-Nearest Neighbors, Fuzzy K-Nearest Neighbors and Support Vectors Machines classifiers against SMOTE method which is the standard oversampling approach in literatures and it out performed the SMOTE method. In this work, the author stated that this technique could be further applied to categorical datasets as it was only applied on only numerical dataset. Another direction is to apply the approach to multiclass datasets. [30].

2) Undersampling Techniques: Random undersampling (RUS) is also the heuristic technique used to reduce majority class distribution in dataset. Set of major instances is randomly chosen and removed from a training dataset. However, RUS has its weaknesses, which is, getting rid of possible useful instances and leave behind noisy instances. This shortcoming of SUP lead to methods like, Tomek Links, Edited Nearest Neighbor (ENN) [31], Neighborhood Cleaning (NCL) [32] in which the work of [33] noted that they are highly timely, reason being, for any example in the datasets, nearest neighbors of the sample must be found, so it is unfeasible for very large datasets and they did not consider examples similarity information. Other methods of such earlier works includes One-Sided Selection and Condensed Nearest Neighbor (CNN). [34] then used Parallel selective sampling and SVM for the undersampling process, which reduces the examples in the safe region which is distanced based. Most of the current undersampling methods are derivatives of ENN, CNN, NCL that are also distanced based. [35] presented a neighbourhood-based undersampling approach for handling binary imbalanced dataset, targeting mainly the overlapped region and examples. Four techniques based on neighbourhood searching with dissimilar criteria to identify possible overlapped instances are proposed in the work. These techniques include Modified Tomek Link Search (NB-Tomek), Recursive Search (NB-Rec), Common Nearest Neighbours Search (NB-Comm) and Basic Neighbourhood Search (NB-Basic). Finally, the searching criteria of this technique can be modified and extended to solve multiclass imbalanced datasets. Another interesting direction would be to apply a global algorithm to roughly separate the overlapping and non-overlapping regions, proceeded by performing a local search.

3) Hybrid Methods: The hybrid method which is a combination of oversampling and undersampling, most often are implemented by integrating already existing oversampling and undersampling technique just as it was used in [36]. Generally, it has been noticed that hybrid methods [37], [1] don't really come up with fresh new resampling technique but improve on already existing oversampling and undersampling method.

4) Multiclass Complexity: In the work of [38], a technique to analyse the classification of imbalanced datasets with multiclass using binarization techniques and ad-hoc approaches. Different methods were used includes the introduction of a preprocessing mechanism based on SMOTE, which iteratively generated new samples from the least represented class at each step, known as Static-SMOTE. Next, presented a global cost-sensitive approach that re-weights the instances from each class according to their ratio. [38] continued by describing Ada-Boost.NC, a novel boosting-based methodology for addressing multiclass imbalance problems.

The paper has provided an empirical analysis of several methods for dealing with multiclass imbalanced problems, most of them based on the combination of binary approaches and OVO and OVA strategies in combination with other ad hoc methods designed for this problem. From the study, some important lessons learned are:

a) Concerning the synergy of binarization and preprocessing techniques, the oversampling methodologies have shown a more robust behaviour than those based on undersampling and cleaning procedures for multiple-class imbalanced problems.

b) Again, considering the OVA versus OVO comparison, OVO methods in general have shown better behaviour, especially according to the average performance obtained. The reason behind this higher quality of results is primarily that the pairwise learning technique confronts a lower subset of instances and is therefore less likely to obtain imbalanced training-sets, which is the disadvantage in this case. Additionally, we must be aware that in this case the decision boundaries of each binary problem may be considerably simpler than the OVA strategy.

c) We must stress that the best of techniques studied are those based on OVO with SMOTE and OVO with cost-sensitive learning.

d) Regarding the comparison between OVO plus strategies for imbalanced classification, and ad hoc approaches, it was stressing several advantages that make the use of the former preferable, such as efficiency, simplicity in the adaptation of existing classification approaches, and the possibility of combining them with new and more sophisticated techniques for addressing data imbalance.

The author identified generally, that binarization techniques with the correct preprocessing or cost-sensitive strategy are useful but easy mechanisms to improve classifiers' performance in imbalanced domains, but still there is still future work that remain to be addressed regarding this topic: Non-competent examples in OVO strategy, Intrinsic data

characteristics, Scalability, the OVO strategy as a decision-making problem. [7], investigated the oversampling of different classes and types of examples in multiclass imbalanced datasets. [7] aimed to determine how the preprocessing (oversampling) of some of the classes and types of examples within each class (that is, safe, borderline, rare or outlier) affect the efficiency of the classifiers built. Firstly, for the dataset, each example within each class changed for its difficulty factor and labeled as safe, borderline, rare or outlier using HVDM distance metric. Secondly, considering all the valid configurations that was found in the previous step. The preprocessing consisted of the application of an oversampling procedure, following a scheme to generate the new synthetic examples similar to that used SMOTE in binary imbalanced problems. Finally, the preprocessed datasets were compared, considering the performance obtained by different classification algorithms, such as C4.5, Nearest Neighbor (NN) rule and Support Vector Machine (SVM).

Attending to the results analyzed, several conclusions can be extracted about the importance of the preprocessing techniques in multiclass imbalanced datasets:

1) Preprocessing some concrete classes and types of examples within these classes (safe, borderline, rare or outliers) can improve the performance of indiscriminately deteriorate caused by preprocessing all the classes. However, if these classes and types of examples to preprocess are not correctly chosen, the results can be deteriorated.

2) Types of examples to be preprocessed: It is important focusing on the data characteristics of each problem, studying the distribution of each class and analysing which types of example should be preprocessed to improve the final result.

3) Selecting the best classes and examples to preprocess. In the case that the best class and types of examples are chosen to be preprocessed, the results obtained show that this preprocessing can cause a significant improvement in the performance against preprocessing all the classes or not consider any preprocessing.

[39], presented a method called dynamic ensemble selection for multiclass imbalanced datasets (DES- MI), in which the competence of the candidate classifiers is assessed with weighted instances in the neighborhood.

The proposed approach DES-MI for multiclass imbalance learning problems based on dynamic selection of classifiers, which consists of two key components as follows:

1) Generation of the candidate classifiers: The inherent mechanism behind DES-based methods is known as diversified classifiers performing differently in different regions. The homogeneous ensemble to generate the candidate classifier pool was used, which considered a preprocessing technique which relied on random balance to restore the balance of the class proportions.

2) Dynamic selection of the most appropriate ensemble: In the classic DES methods, the distribution of instances within the region of competence was not considered, and it made the final decision towards the majority classes. In order to extend the DES approach into a multiclass imbalanced scenario, a weighting method to outstand the competence of a candidate classifier with more power in classifying the minority classes was developed. That is, the instances belonging to the minority classes within the neighborhood of a query example have greater wights when evaluating the level of competence of a classifier in the candidate classifier pool.

It was observed that the proposed DES-MI performs considerably better than the selected state-of-the-art techniques, both in terms of MAvA and MFM performance measures. Concretely, DES-MI achieves the best results on 11 out of 20 datasets when MAvA is used as the performance measure, whereas with MFM as the performance measure DES-MI performs best on 12 out of 20 datasets. With respect to the average performance, DES-MI also outperforms the selected state-of-the-art methods. The proposed method provides a direction for the future research to extend the strategies proposed for constructing a DES classifier system in a multiclass imbalance scenario. In the future, there are several works remaining to be addressed. Among them, the scalability of DES-based method and more specifically, of the DES-MI must be studied. Furthermore, it would be interesting to extend the technique to semi-supervised learning with unseen labels.

[30], proposed a new algorithm named Similarity Oversampling and Undersampling Preprocessing (SOUP) to balanced multiclass imbalanced data, where interrelationships between classes are modeled. The main contribution of this paper is, fining examples difficulty, a new method for identifying the degree of similarity between classes and then applying them on [23], method of evaluating the safe level of examples. This method of evaluating safe level was then used on the SOUP algorithm in oversampling and undersampling process. It was also evaluated by comparing its performance with other well-known methods like Global-CS, Static-SMOTE and Multiclass Roughly Balanced Bagging (MRBB) where it outperformed them; it was also compared on decomposition ensembles OVO and OVA. Despite its performance, the heuristic approach used to determine the similarity level still needs to be evaluated carefully. Nevertheless, as a future research direction, SOUP inspirations in generalizing an underbagging ensemble, such as Neighborhood Balanced Bagging, in order to further improve predictive ability.

In conclusion, the multiclass data level resampling approach cannot be compared with the binary resampling approach in terms of achievement in designed novel resampling technique. There is need to evaluate a mathematical method to derive the degree of similarity from dataset instead of depending on expert for such information.

III. METHODOLOGY

A. Data Acquisition

This study was done considering the papers published mainly within the last two decades with more emphasis on the last decade. The resultant library databases used are: Springer, Elsevier, IGI global, Elsevier, IEEE transactions, Springer and others. To present a whole group of search parameters to cover articles on imbalanced data, a combination of the following phrases was used: class imbalanced, imbalanced techniques, imbalanced methods, resampling techniques, resampling methods, machine learning, data preprocessing methods, class imbalanced problems. Keywords and synonyms for technique and approaches for the class imbalance classification where also used. Different spelling based on America and Britain

spelling and also singular and plural forms were also considered. The total search yielded 227 papers on imbalanced data domains, that were downloaded and again filtered using the following stages. First stage filter was based on title, which then reduced the papers to 184, the next was based on abstract and conclusion, which also reduced the paper to 102. Based on full text, the paper was reduced to 87 and finally, reference investigation and redundancy reduced the papers to 52.

B. Resampling Techniques Analysis Over Data Intrinsic Characteristics

The reviews from previous works have made it clear to us that class imbalance is not just the issue with real world, another critical problem that deteriorates classifier performance is data intrinsic characteristic. Table I, present an analysis on the extent to which previous class imbalanced techniques have paid attention to data intrinsic characteristics.

TABLE I. RESAMPLING TECHNIQUES VERSUS DATA INTRINSIC CHARACTERISTICS

Reference	**Safe region**	**Unsafe Region**		
	Safe Level	**Borderline**	**Outlier**	**Small Disjoint (Rare)**
[40], [3], [26], [1], [41], [42], [43], [44], [45],[46], [47], [48], [49], [50]	✖	✖	✖	✖
[29], [28], [51]	✖	✓	✓	✖
[52], [25], [53]	✓	✓	✖	✖
[24], [54], [55], [56]	✓	✖	✖	✖
[27], [57], [58], [59], [60], [61]	✖	✖	✓	✖
[62], [35], [63]	✖	✓	✖	✖
[37]	✖	✓	✖	✓

C. Resampling Techniques Categorises

In this work also, resampling techniques based on the methods of implementation have been categorized. These categories includes: cluster-based methods (e.g. k-means), distance-based methods (e.g. nearest neighbors) and evolutionary methods (e.g. generic algorithm). The techniques and categories they belong to have been summarised in Table II.

TABLE II. SUMMARY OF RESAMPLING ARTICLES AND METHODS USED

Categories	**Methods**	**Articles**
Oversampling	Cluster-based	[37], [40], [3], [29], [52],
	Distance based (e.g.SMOTE modified)	[25], [28], [26],[29], [52], [27], [1], [40], [62], [24], [54], [60], [55], [63], [64], [56], [50]
	Evolutionary based	[41], [42], [50], [43], [54], [57], [44], [65]
Undersampling	Cluster-based	[45], [37], [58], [45]
	Distance based	[35],[53], [46], [47], [35], [63], [61], [59]
	Evolutionary based	[48], [49], [60], [34], [57]

Despite the uniqueness and efficiency of each category technique, they all have their merits and demerits, which are presented in Table III.

TABLE III. SUMMARY OF RESAMPLING ARTICLES AND METHODS USED

Approach	Pros	Cons
Distanced Based	1. This approach is simple and direct and does not include a complex formulation 2. it can commonly integrate with any other approach	1. Interrelationship or similarities between examples have not been really considered.
Cluster Based	1. Clustering have been proven to increase performance in resampling processes 2. it can easily be integrated with any other approach	1. Interrelationship or similarities between examples have not been really considered. 2. Clustering alone do not improve performance, most be integrated with other methods 3. It is time consuming as sub-clusters are treated independently
Evolutionary Based	1. Evolutionary based uses genetic probabilistic algorithm in resampling process	1. Interrelationship or similarities between examples have not been really considered. 2. Most complex to implement in comparison to the other methods

IV. RESEARCH FINDINGS

After critical study of imbalanced dataset and their data level approaches, the following were drawn out from the analysis.

1) 1. Imbalanced resampling technique have received tremendous attention within the last two decades, with novel techniques such as the recent derivatives of SMOTE and ADASYN. Despite this amazing achievement, in the analysis from TABLE 1, one could easily observe that most of these resampling techniques do not really consider data intrinsic characteristics in the resampling process, even if it has been shown in literatures that data intrinsic characteristics deteriorates classifier performance more than imbalanced problem. Furthermore, overlapping region is the most considered by resampling techniques among the different difficulty factors, but reviews have also shown that small disjoint are also as highly harmful as overlapping examples.

2) Data level Resampling Algorithm should be tested against individual data difficulty factors, to ascertain which is best for a particular difficulty type. This is because every data sample have different levels of difficult, therefore, it will be appropriate to know which technique best solves a particular difficulty type and not just general comparism with other data level resampling techniques.

3) Among the categories of data level resampling technique, distance based have gain more attention from the research community, this maybe because of its simple and direct and does not include a complex formulation and it can easily be integrated with any other category. Most data level techniques focus on designing a new oversampling technique and just adopt the RUS on the majority class example.

4) The degrees of similarity should be made known by an expert or can also come from the domain knowledge [23]. If neither is available, some heuristic approaches could be used. The deductive approach designed by [9] to determine the degree of similarities between classes used class cardinality ratio between class as safe level to evaluate the degree of similarities.

V. RECOMMENDATION

Despite the fact that more works have been done in class imbalance in recent years, however, there are still gaps in this area of imbalanced data in machine learning that need further attention. The data level preprocessing methods will be much more effective using informative approach and examples similarities information. Techniques for evaluating examples similarity information in multiclass dataset should also be explored. Furthermore, there are issues that need to be considered with already existing methods; such as, over-fitting, lack of consideration of possible relevant examples, interrelationship between examples and computation cost are mostly not evaluated.

Below are the basic potential questions to answer when developing a resampling method for imbalanced dataset:

1) Which examples are more preferred to be duplicated or removed to improve performance?

2) What method will best implement the duplication or synthetic process and removal process?

3) How do I ascertain the safer region to carry out the oversampling or undersampling without deteriorating the performance level of the original dataset?

4) What method will best ascertain the best region to carry out the oversampling and undersampling process?

VI. CONCLUSION AND FUTURE WORK

To conclude, this article presents an analysis of the progress that have been made on informative methods for resampling imbalanced dataset based on their data intrinsic characteristics. In addition, the techniques were also analysed based on their categories. This review of the resampling techniques has been able to established that despite the report by publications that data intrinsic characteristics are more

harmful than imbalanced nature of data, most existing resampling techniques do not regard data intrinsic characteristic in their design, this may be due to the popular nature and attention drawn by imbalanced problem in publications. For future work, a robust resampling technique that will critically consider data difficulty factors when evaluating the region and the examples to oversample and undersample. Resampling techniques should also be evaluated against the different types of difficulty factors so as to ascertain the difficulty type it is best used for.

REFERENCES

[1] A. Mahmoud, A. El-Kilany, F. Ali, and S. Mazen, "A Novel Oversampling Technique To Handle Imbalanced Datasets," pp. 177–182, 2020.

[2] J. Blaszczy, "Diversity Analysis on Imbalanced Data Using Neighbourhood and Roughly Balanced," pp. 552–562, 2016.

[3] H. Duan, Y. Wei, P. Liu, and H. Yin, "A novel ensemble framework based on K-means and resampling for imbalanced data," Appl. Sci., vol. 10, no. 5, 2020.

[4] K. Napierala and J. Stefanowski, "Types of minority class examples and their influence on learning classifiers from imbalanced data," J. Intell. Inf. Syst., vol. 46, no. 3, pp. 563–597, 2016.

[5] F. Shakeel, A. S. Sabhitha, and S. Sharma, "Exploratory Review on Class Imbalance Problem : An Overview," 2017.

[6] G. M. Weiss, "FOUNDATIONS OF IMBALANCED LEARNING," 2012.

[7] J. A. Sáez, B. Krawczyk, and M. Woźniak, "Analyzing the oversampling of different classes and types of examples in multi-class imbalanced datasets," Pattern Recognit., vol. 57, pp. 164–178, 2016.

[8] J. Błaszczyński and J. Stefanowski, Local data characteristics in learning classifiers from imbalanced data, vol. 738. 2018.

[9] M. A. Janicka, M. A. Lango, and J. E. Stefanowski, "Using Information On Class Interrelations To Improve Classification Of Multiclass Imbalanced Data : A New Resampling Algorithm," vol. 29, no. 4, pp. 769–781, 2019.

[10] A. Fernández, G. Salvador, M. Galar, P. C, R, B. Krawczyk, and F. Herrera, Learning from imbalanced data Sets, vol. 21, no. 9. 2018.

[11] V. López, A. Fernández, S. García, V. Palade, and F. Herrera, "An insight into classification with imbalanced data: Empirical results and current trends on using data intrinsic characteristics," Inf. Sci. (Ny)., vol. 250, pp. 113–141, 2013.

[12] H. Kaur, H. S. Pannu, and A. K. Malhi, "A Systematic Review on Imbalanced Data Challenges in Machine Learning : Applications and Solutions," vol. 52, no. 4, 2019.

[13] F. Thabtah, S. Hammoud, and F. Kamalov, "Data Imbalance in Classification : Experimental Evaluation," Inf. Sci. (Ny)., 2019.

[14] A. Fernández, S. García, M. Galar, R. C. Prati, B. Krawczyk, and F. Herrera, Learning from imbalanced data, vol. 807. 2019.

[15] Y. Liu, Y. Wang, X. Ren, H. Zhou, and X. Diao, "A Classification Method Based on Feature Selection for Imbalanced Data," IEEE Access, vol. 7, pp. 81794–81807, 2019.

[16] A. De and N. Do, "Techniques to deal with imbalanced data in multi-class problems : A review of existing methods," 2020.

[17] Charte et al, "A First Approach to Deal with Imbalance," pp. 150–160, 2013.

[18] K. Napierała, J. Stefanowski, and S. Wilk, "Learning from imbalanced data in presence of noisy and borderline examples," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6086 LNAI, pp. 158–167, 2010.

[19] N. V. Chawla, B. W. Kevin, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique Nitesh," Ecol. Appl., vol. 30, no. 2, pp. 321–357, 2002.

[20] H. He, Y. Bai, E. A. Garcia, and S. Li, "ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning," no. 3, pp. 1322–1328, 2008.

[21] D. Elreedy and A. F. Atiya, "A Comprehensive Analysis of Synthetic Minority Oversampling Technique (SMOTE) for handling class imbalance," Inf. Sci. (Ny)., vol. 505, pp. 32–64, 2019.

[22] K. Napierala and J. Stefanowski, "Identification of Different Types of Minority Class Examples in Imbalanced Data," pp. 139–150, 2012.

[23] M. Lango, K. Napierala, and J. Stefanowski, "Evaluating Difficulty of Multi-class Imbalanced Data," vol. 2, no. January, pp. 312–322, 2017.

[24] C. Bunkhumpornpat, K. Sinapiromsaran, and C. Lursinsap, "Safe-Level-SMOTE : Safe-Level-Synthetic Minority Over-Sampling TEchnique," pp. 475–482, 2009.

[25] T. MacIejewski and J. Stefanowski, "Local neighbourhood extension of SMOTE for mining imbalanced data," IEEE SSCI 2011 Symp. Ser. Comput. Intell. - CIDM 2011 2011 IEEE Symp. Comput. Intell. Data Min., pp. 104–111, 2011.

[26] S. S. Patil, "Imbalanced Big-Data using Random Forest," pp. 403–408, 2015.

[27] Z. Xu, D. Shen, T. Nie, and Y. Kou, "A hybrid sampling algorithm combining M-SMOTE and ENN based on Random Forest for medical imbalanced data," J. Biomed. Inform., p. 103465, 2020.

[28] S. Barua, M. M. Islam, X. Yao, and K. Murase, "MWMOTE - Majority weighted minority oversampling technique for imbalanced data set learning," IEEE Trans. Knowl. Data Eng., vol. 26, no. 2, pp. 405–425, 2014.

[29] H. Al Majzoub, I. Elgedawy, Ö. Akaydın, and M. Köse Ulukök, "HCAB-SMOTE: A Hybrid Clustered Affinitive Borderline SMOTE Approach for Imbalanced Data Binary Classification," Arab. J. Sci. Eng., no. 0123456789, 2020.

[30] M. Janicka, M. Lango, and J. Stefanowski, "Using Information on Class Interrelations to Improve Classification of Multiclass Imbalanced Data: A New Resampling Algorithm," Int. J. Appl. Math. Comput. Sci., vol. 29, no. 4, pp. 769–781, 2019.

[31] W. L. Dennis, "Asymptotic Properties of Nearest Neighbor Rules Using Edited Data," vol. 2, no. 3, pp. 408–421, 2002.

[32] J. Laurikkala, "Improving Identification of Difficult Small Classes by Balancing Class Distribution," Springer-Verlag Berlin Heidelb. 2001, no. PB, p. 4, 2001.

[33] X. Guo, Y. Yin, C. Dong, G. Yang, and G. Zhou, "On the Class Imbalance Problem," pp. 192–201, 2008.

[34] A. D. Addabbo and R. Maglietta, "Parallel selective sampling method for imbalanced and large data classification," Pattern Recognit. Lett., vol. 62, pp. 61–67, 2015.

[35] P. Vuttipittayamongkol and E. Elyan, "Neighbourhood-based undersampling approach for handling imbalanced and overlapped data," Inf. Sci. (Ny)., vol. 509, pp. 47–70, 2020.

[36] R. F. A. B. de Morais and G. C. Vasconcelos, "Boosting the performance of over-sampling algorithms through under-sampling the minority class," Neurocomputing, vol. 343, pp. 3–18, 2019.

[37] M. M. Nwe and K. T. Lynn, "Effective resampling approach for skewed distribution on imbalanced data set," IAENG Int. J. Comput. Sci., vol. 47, no. 2, pp. 234–249, 2020.

[38] A. Fernández, V. López, M. Galar, M. J. Del Jesus, and F. Herrera, "Analysing the classification of imbalanced data-sets with multiple classes: Binarization techniques and ad-hoc approaches," Knowledge-Based Syst., vol. 42, pp. 97–110, 2013.

[39] S. García, Z. L. Zhang, A. Altalhi, S. Alshomrani, and F. Herrera, "Dynamic ensemble selection for multi-class imbalanced datasets," Inf. Sci. (Ny)., vol. 445–446, pp. 22–37, 2018.

[40] A. Roy, R. M. O. Cruz, R. Sabourin, and G. D. C. Cavalcanti, "A study on combining dynamic selection and data preprocessing for imbalance learning," Neurocomputing, vol. 286, pp. 179–192, 2018.

[41] G. Douzas and F. Bacao, "Effective data generation for imbalanced learning using conditional generative adversarial networks," Expert Syst. Appl., vol. 91, pp. 464–471, 2018.

[42] D. Chetchotsak, S. Pattanapairoj, and B. Arnonkijpanich, "Integrating new data balancing technique with committee networks for imbalanced data : GRSOM approach," Cogn. Neurodyn., 2015.

[43] C. Lu, H. Ke, G. Zhang, Y. Mei, and H. Xu, "An improved weighted extreme learning machine for imbalanced data classification," Memetic Comput., vol. 11, no. 1, pp. 27–34, 2019.

[44] M. R. Pavan Kumar and P. Jayagopal, "A preprocessing method combined with an ensemble framework for the multiclass imbalanced data classification," Int. J. Comput. Appl., vol. 0, no. 0, pp. 1–8, 2019.

[45] W. Lin, C. Tsai, Y. Hu, and J. Jhang, "Clustering-based undersampling in class-imbalanced data," vol. 410, pp. 17–26, 2017.

[46] E. Rendón, R. Alejo, C. Castorena, F. J. Isidro-Ortega, and E. E. Granda-Gutiérrez, “Data sampling methods to deal with the big data multi-class imbalance problem,” Appl. Sci., vol. 10, no. 4, 2020.

[47] A. Anand, G. Pugalenthi, G. B. Fogel, and P. N. Suganthan, “An approach for classification of highly imbalanced data using weighting and undersampling,” pp. 1385–1391, 2010.

[48] B. Sun, H. Chen, J. Wang, and H. Xie, “Evolutionary under-sampling based bagging ensemble method for imbalanced data classification,” Front. Comput. Sci., vol. 12, no. 2, pp. 331–350, 2018.

[49] J. Lee, “A New Under-Sampling Method Using Genetic Algorithm for Imbalanced Data Classification,” p. 6, 2013.

[50] B. S. Raghuwanshi and S. Shukla, “SMOTE based class-specific extreme learning machine for imbalanced learning,” Knowledge-Based Syst., vol. 187, no. xxxx, p. 104814, 2020.

[51] R. A. Sowah, M. A. Agebure, G. A. Mills, K. M. Koumadi, and S. Y. Fiawoo, “New Cluster Undersampling Technique for Class Imbalance Learning,” vol. 6, no. 3, 2016.

[52] G. Douzas, F. Bacao, and F. Last, “Improving imbalanced learning through a heuristic oversampling method based on k-means and SMOTE,” Inf. Sci. (Ny)., vol. 465, pp. 1–20, 2018.

[53] B. Krawczyk, M. Koziarski, and M. Wozniak, “Radial-Based Oversampling for Multiclass Imbalanced Data Classification,” IEEE Trans. Neural Networks Learn. Syst., vol. PP, pp. 1–14, 2019.

[54] F. Kamalov and D. Denisov, “Knowledge-Based Systems Gamma distribution-based sampling for imbalanced data,” Knowledge-Based Syst., vol. 207, p. 106368, 2020.

[55] M. Koziarski, M. Woźniak, and B. Krawczyk, “Knowledge-Based Systems Combined Cleaning and Resampling algorithm for multi-class imbalanced data with label noise,” Knowledge-Based Syst., vol. 204, p. 106223, 2020.

[56] A. Kumari and U. Thakar, “Hellinger distance based oversampling method to solve multi-class imbalance problem,” Proc. - 7th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2017, pp. 137–141, 2018.

[57] S. Cateni, V. Colla, and M. Vannucci, “A method for resampling imbalanced datasets in binary classification tasks for real-world problems,” Neurocomputing, vol. 135, pp. 32–41, 2014.

[58] N. S. Kumar, K. N. Rao, and A. G. K. S. Reddy, “Undersampled K - means approach for handling imbalanced distributed data,” 2014.

[59] M. Imran and M. S. Kouser, “A Novel Algorithm for Class Imbalance Learning on Big Data Using Under Sampling Technique,” Int. J. Comput. Intell. Res., vol. 15, no. 1, pp. 11–32, 2019.

[60] S. Susan, “SSO Maj -SMOTE-SSO Min : Three-step intelligent pruning of majority and minority samples for learning from imbalanced datasets,” vol. 78, pp. 141–149, 2019.

[61] Q. Kang, S. Member, X. Chen, and S. Member, “A Noise-Filtered Under-Sampling Scheme for Imbalanced Classification,” pp. 1–12, 2016.

[62] H. Han, W. Y. Wang, and B. H. Mao, “Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning,” Lect. Notes Comput. Sci., vol. 3644, no. PART I, pp. 878–887, 2005.

[63] D. Devi, S. K. Biswas, and B. Purkayastha, “Learning in presence of class imbalance and class overlapping by using one-class SVM and undersampling technique,” Conn. Sci., vol. 0, no. 0, pp. 1–38, 2019.

[64] X. Yang, Q. Kuang, W. Zhang, and G. Zhang, “AMDO : an Over-Sampling Technique for Multi-Class Imbalanced Problems,” vol. 4347, no. c, 2017.

[65] X. Zhang, D. Wang, Y. Zhou, H. Chen, F. Cheng, and M. Liu, “Kernel modified optimal margin distribution machine for imbalanced data classification,” Pattern Recognit. Lett., vol. 125, pp. 325–332, 2019.

AN ENHANCED BANK CUSTOMERS CHURN PREDICTION MODEL USING A HYBRID GENETIC ALGORITHM AND K-MEANS FILTER AND ARTIFICIAL NEURAL NETWORK

1st **R. Yahaya**
Department of Computer Science
Federal University of Technology
Minna, Nigeria
rahmayahya5@gmail.com

2nd **O. A. Abisoye**
Department of Computer Science
Federal University of Technology
Minna, Nigeria
o.abisoye@futminna.edu.ng

3rd **S. A. Bashir**
Department of Computer Science
Federal University of Technology
Minna, Nigeria
bashirsulaimon@futminna.edu.ng

Abstract—Customer churn prediction is an important issue in banking industry and has gained attention over the years. Early identification of customers likely to leave a bank is vital in order to retain such customers. Predicting churning is a data mining tasks that require several data mining approaches. Churn prediction based on Artificial Neural Networks (ANNs) have been successful, however, they are affected by the noise or outliers present in such datasets. The effect of such noise, and number of training samples on churn prediction was investigated. Two filters were applied to the data, the Genetic Algorithm (GA) and Kmeans filter. The filtered data were used to train an ANN model and tested with a 30% unfiltered data. The performance show that the training performance improved when noise was filtered while the testing performance was affected by the unbalanced data caused by filtering.

Keywords—Customer Churn, Data Mining, Artificial Neural Network, K-means, Genetic Algorithm

I. INTRODUCTION

A customer is identified as a churner via his/her transaction history analysis. any Banking system customers are likely to churn due to poor customer services, unwarranted bank charges and other scenarios. Customer retention is often challenging for organizations as the cost of acquiring a new customer or subscriber is higher than retaining and old one. However, if an organization can easily predict customers that are likely to leave or unsubscribe form their service ahead, customer retention strategies will be directed entirely towards such customers. The bank plays a vital role in influencing a customer's satisfaction which leads to loyalty and continuous patronage, even referral. [1] suggested that monitoring customer behaviours can help organizations predict churners and lead to customer retention strategy creation. Churn prediction allows organizations to improve the efficiency of customer retention campaigns and mitigate the costs of churn. Several approaches have been used for Churn Prediction, including classification, clustering, association and rule-based approaches. Most researchers used two or more algorithms in churn detection, one improving on the other ([2]; [3]). [4] proposed a customer churn prediction model based on XGBoost and Multi-layer Perceptron which resulted in predicting churn better than other state-of-art prediction models. [5] proposed a hybrid model of classification and clustering techniques, experiments were done for each techniques and results were produced and compared, the hybrid model produced more accurate results in comparison to single model. Noise affects data analysis leading to wrong or incorrect results [6]. To deal with noise in data analysis, and achieve a good model, data has to be filtered. [7] proposed a noise filtering approach that combined Tomek-link with distance weighted KNN (TWK) while kmeans clustering have been applied for data filtering due to its successful clustering ability [8]. However,

kmeans clustering algorithms performance is affected by the initial cluster centers which are randomly selected.

In this paper, an enhanced bank customer churn prediction model using a Hybrid Genetic algorithm with K-means (GA-Kmeans) clustering and ANN is proposed. The GA searches for optimal cluster centers of the kmeans while the ANN is used for predicting churning. The effect of data filtering on the performance of ANN was also investigated in this paper. The remainder of the paper is structured as follows: Section 2 presents the review of related works, section 3 presents the materials and methods, while in section 4, the results and discussions were presented. Finally, in section 5, the conclusion and recommendations were presented.

II. LITERATURE REVEIW

There are several churn prediction models in banking industry and other financial institutions. They mostly applied data mining and machine learning approaches to solve the problems. [9] identified churn customers using some criteria before they unsubscribe from a service or leave the business. Customer churn prediction model was developed by analyzing historical behaviour data of defected customers, for early detection and retention purposes. They used random forests to build customer churn prediction models [10]. In a competitive world as ours, existing customer base and their data are priceless assets organizations boast of. According to [11], the cost of acquiring a new customer is usually high than retaining customer likely to churn, hence correctly identifying a churn customer through metrics such as recall, accuracy, precision and F1-score in customer churn detection will save the company from loss and enhance their customer retention strategies. Churn prediction challenges include; Capturing pattern of customer behaviour, especially in financial institutions. Past researches on churn prediction laid emphasis on predicting churn based on monthly, static or dynamic behaviour of customers. [12] claims they are unrealistic, as predicting churn based on monthly traits, might divert focus from churners who decide to unsubscribe at the beginning of the month, and using monthly traits to predict a customer's likelihood of churning might not take daily traits in cognizance, hence reducing the discriminative ability and performance of the model. K-means have been applied for churn prediction in combination with other models such as, C5.0 with and without misclassification cost in addition to logistic regression and ANN. Overall, C5.0 with misclassification cost surpassed all other models in terms of accuracy.

[13]) predicted the customer churn problem on a Nigerian bank datasets using WEKA tool for knowledge analysis. K-means clustering algorithm was used to cluster the data while, JRip algorithm was implemented in rule generation phase. Customer Relationship Management (CRM) helps employees or organization put their customer into consideration by offering them excellent services and satisfaction, which might in turn reduce churning. [14] developed a CRM model comprising of Genetic-based Data Mining (GDM) approach to counter some of the challenges in CRM. They used genetic algorithm and data mining in achieving their aim, by optimizing rules generated from C5.0 algorithm with a genetic algorithm to increase CRM classification time and accuracy, Genetic Algorithm reduced and improved upon C5.0 algorithm. The GDM model was able to find hidden data from a large chunk of data, equipping the researcher with information to serve customers better. [15] developed a robust classification model using Artificial neural network and further applied hyperparameter search space using Genetic Algorithm to detect suitable parameter settings. Results showed that applying hyperparameter optimization on the ANN classification models led to an improved rate of customer churn prediction. [16] designed a Multilayer Perceptron (MLP) model for churn prediction and results are further compared with Support Vector Machine, Naïve Bayes and Decision Tree. MLP-ANN outperformed other classifiers for both PCA and Normalize pre-processing techniques, finally used InfoGainAttribute to identify the highest factor attribute leading to customer retention. [17] applied feature selection aiding him remove irrelevant features which aided in improving the performance of the model and reduced training time and overfitting for model construction. [18] used neural network model within the software package (Alyuda) Neuro Intelligence for customer churn prediction in Banking industry he claimed that neural network was the best fit for pattern recognition, image processing, optimization

problems. From the review works, it is clear that ANN is one of the competitive models for churn prediction. Furthermore, the research works do not consider filtering the data before using them.

III. MATERIALS AND METHODS

The block diagram shown in Figure 1 shows the steps that were taking to achieve the aim of this research paper. It comprises of description of the data collection, description and preprocessing. It also involves the data filtering, model design, training, testing and performance evaluation.

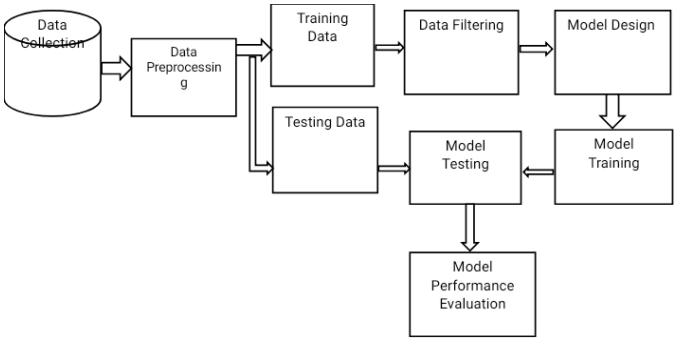


Figure 1: Proposed Methodology

A. DATA COLLECTION AND DESCRIPTION

The Dataset for this research was obtained from Kaggle database. The dataset is a bank dataset used for churn prediction challenge. It comprises of 10,000 bank records with ten (10) attributes of each customer. Table.1 shows a sample of the dataset; 80% non-churn and 20% churn samples. Figure 2 shows the sample dataset with its 10 attributes.

B. DATA PRE-PROCESSING

The dataset will be pre-processed to put the data in appropriate state using the following steps:

i. Filling of any missing value(s) using average filling techniques.
ii. Manual attribute selection.
iii. Data Partitioning: Partitioning the data into training and testing ratio (70:30) respectively.

In this paper, no missing values was found and four attributes were manually removed. The removed attributes are the Row number, CustomerId, Surname and Geography. The dataset was partitioned into training and testing in the ratio 70:30 respectively. Figure 2 shows a sample of the dataset with their attributes.

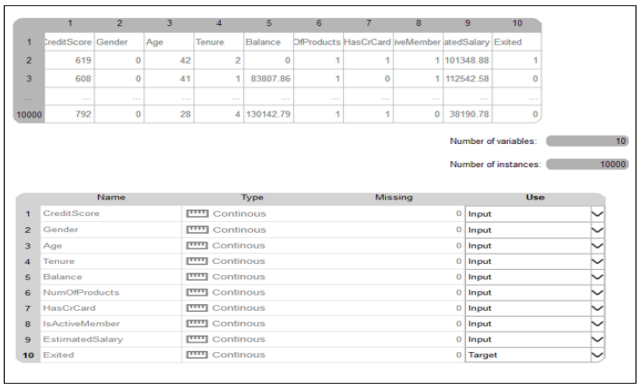


Figure 2: Dataset sample

C. DATA FILTERING

The training dataset was filtered to reduce noise or outliers that may affect the model's performance. An optimized K-means clustering filtering algorithm using Genetic Algorithm (GA) as an optimizer was proposed. It has been established that K-means clustering is sensitive to initial cluster centers which are generated randomly. In this paper, GA was used to search for optimal initial cluster centers. The process of data filtering using GA-kmeans is shown in the flowchart in Figure.3.

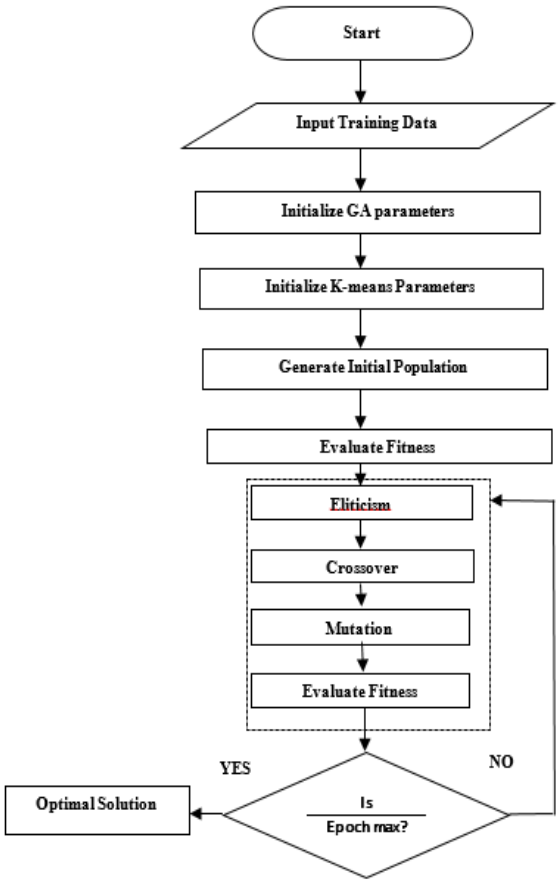


Figure 3: GA-Kmeans Flowchart

D. *MODEL DESIGN:*

An Artificial Neural Network (ANN) model was designed for bank customers churn prediction using MatLab software. The model is a feedforward backpropagation model with 9 input nodes corresponding to the number of inputs, a single hidden layer with 10 hidden nodes and an output layer with one node corresponding to the desired output. Figure 4 shows a designed ANN model. The first layer uses the tansig activation function while the second layer uses the logsig activation function. The scaled conjugate gradient (SCG) training algorithm was used.

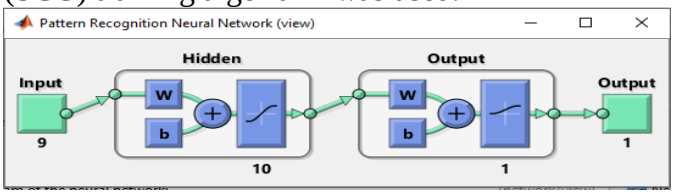


Figure 4: A designed ANN model

Mathematically, the designed ANN model is represented as follows:

Let $Y\{1,t\}$ be the output of the model and $X\{1,t\}$ be the input of the model where, t is the time step. The output of layer 1, layer 2 and the output of the model can be defined as follows:

$$L_1 = \Phi_1(\alpha(b_1,1,Q) + W_1 * \beta) \quad (1)$$

$$L_2 = \Phi_2(\alpha(b_2,1,Q) + W_2 * L_1 \quad (2)$$

$$Y\{1,t\} = L_2 \quad (3)$$

Where, Φ_1 is the tansig activation function and Φ_2 is the logsig activation function, α is the repmat function in Matlab and β is the minmax mapping function between $X\{1,t\}$ and -1.

E. *MODEL TRAINING AND TESTING*

Three models were trained using the designed ANN model. The first model was trained with unfiltered data which has 7000 samples, the second model was trained using 3703 samples from kmeans filter while the third model was trained using 5281 samples from GA-kmeans filter. The 30% reserved data (3000 samples) were used to evaluate the performance of the model and determine the effect of the filtering techniques on the churn prediction.

F. *PERFORMANCE EVALUATION*

The performance of the developed models were evaluated using the following evaluation metrics:

1) ***Accuracy***

The accuracy of a model is the sum of the correctly classified positive instances and the correctly classified negative instances relative to the total number of correctly and incorrectly classified instances and is given as;

$$ACC = \frac{TP + TN}{TP + FP + TN + FN} \times 100\% \quad (4)$$

2) ***Sensitivity***

The sensitivity of a model measures the percentage of correctly classified positive instances and is given as;

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

3) ***Specificity***

The specificity of a model measures the percentage of correctly classified negative instances and is given as;

$$SPC = \frac{TN}{FP+TN} \times 100\% \quad (6)$$

4) ***Precision***

Precision is the fraction of instances that were correctly classified and is given as;

$$PPV = \frac{TP}{TP+FP} \times 100\% \quad (7)$$

5) ***Mean Squared Error (MSE)***

The MSE measures the mean of the squared difference between the model output and target output. It is given as;

$$MSE = \frac{1}{N}\sum_{i=1}^{N} (T_i - P_i)^2 \quad (8)$$

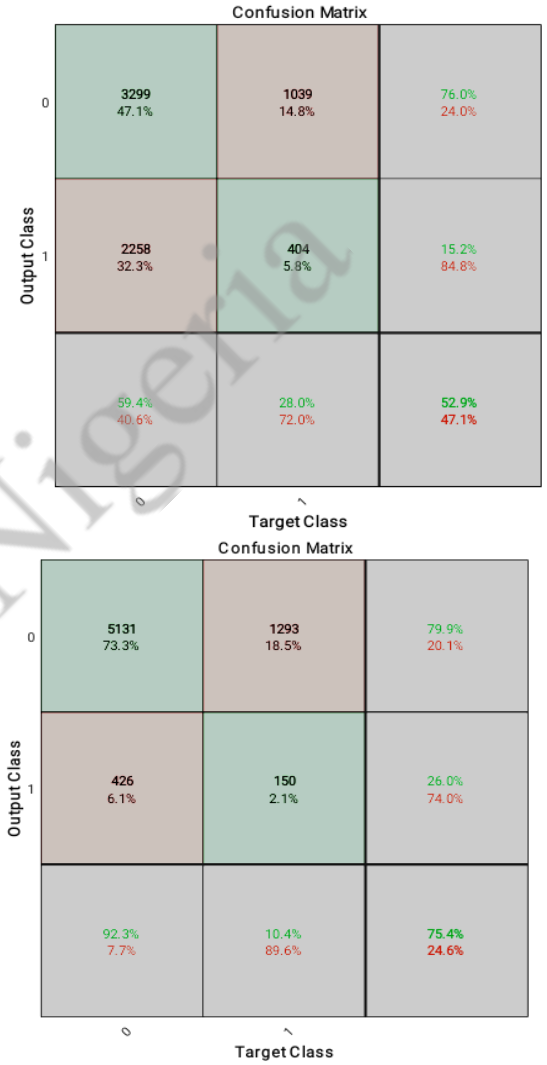
Where, TP (True positive) is correctly classified positive instances, TN (True negative) is correctly classified negative instances, FP (False positive) is incorrectly classified negative instances and FN (False negative) is incorrectly classified positive instances. N is the number of instances, T_i and P_i are the target and predicted values of the i^{th} sample respectively. V

IV. RESULTS AND DISCUSSION

Three categories of results were presented. The Filtering results, model training results and model testing results. The filtering results presented comprises of the kmeans clustering result and optimized kmeans clustering using GA.

A. Filtering Results

Figure 6 shows the confusion matrices of kmeans clustering and GA-kmeans clustering respectively. Kmeans clustering performance shown in Figure 6(a) shows that the TP, TN, FP, and FN are 3299, 404, 2258 and 1039 respectively. Similarly, for GA-kmeans clustering (Figure 6(b)), the TP, TN, FP, and FN are 5131, 150, 426 and 1293 respectively.



a) Kmeans clustering b) GA-Kmeans clustering

Figure 6: Confusion matrices of kmeans and GA-kmeans

The result show that 47.1% of the training data were filtered as noise or outiers when kmeans clustering was used while, when GA-kmeans was used, the only 24.6% of the training data was filtered out. This indicated that the optimized kmeans clustering improved the detection of

outliers due to the optimal initialization of initial cluster centers. Figure 7 shows the convergence curve of the GA used fpr optimizing the kmeans. The curve shows the minimum fitness value obtained and the iteration where convergence too place. The optimum fitness value obtained is 0.2456 at the 11th iteration.

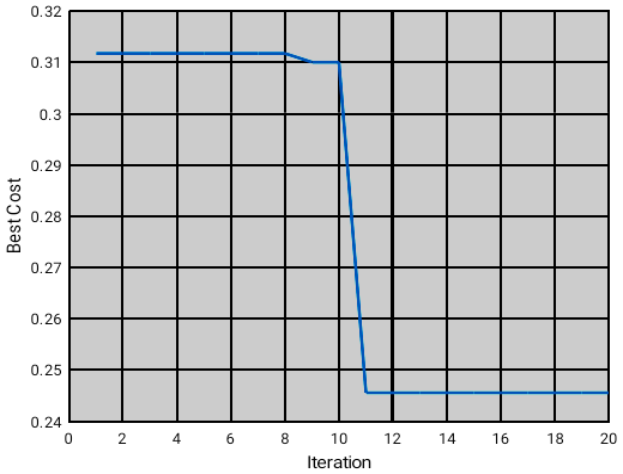


Figure 7: Convergence Curve

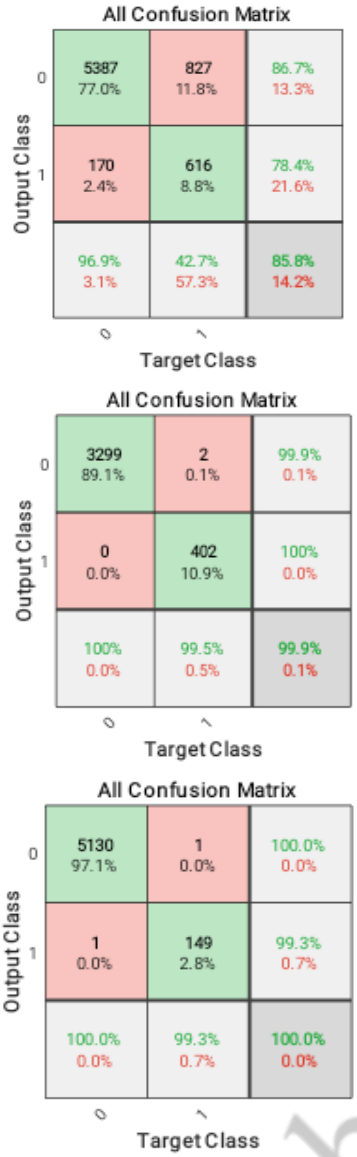
Table 1 is the summary of results obtained by the two clustering techniques evaluated in this work. The result shows the MSE, accuracy, sensitivity, specificity and number of samples. The optimized GA-kmeans filtering achieved an accuracy of 75.4% with an MSE of 0.2456 while kmeans filtering achieved an accuracy of 52.9% with an MSE of 0.4710. The training data after filtering using GA-kmeans is 5281 representing 5131 normal customers and 151 churn customers. For kmeans, 3703 samples were obtained after training representing 3299 normal and 404 churn customers.

Table 1: Filtering Results Summary

stering Algorithm	**SE**	**racy (%)**	**tivity (%)**	**ficity (%)**	**ber of Samples**
Kmeans	456	75.4	30	.4	281
means	710	52.9	40	00	703

B. Training Results

Three models were trained and compared with a view of identifying the best model. The models are ANN model, kmeans-ANN model and GA-kmeans-ANN model. The training results obtained are shown in the confusion matrices in Figure 8 and a summary of the performances of the models are calculated and shown in Table 2. The results show that training the churn prediction models without data filtering (ANN model) obtains a precision and accuracy of 86.7% and 85.8% respectively. Also, kmeans-model obtained a precision and accuracy of 99.99% and 99.90% while the GA-kmeans-ANN model obtained a 100% precision and accuracy. The result indicated that there is a significant increase (14.2%) in training accuracy as the noise of the training data reduced. Furthermore, the improvement in training accuracy for GA-kmeans-ANN against kmeans-ANN indicated that more noiseless training data improves the performance of the models.



a) ANN b) Kmeans-ANN c) GA-Kmeans-ANN

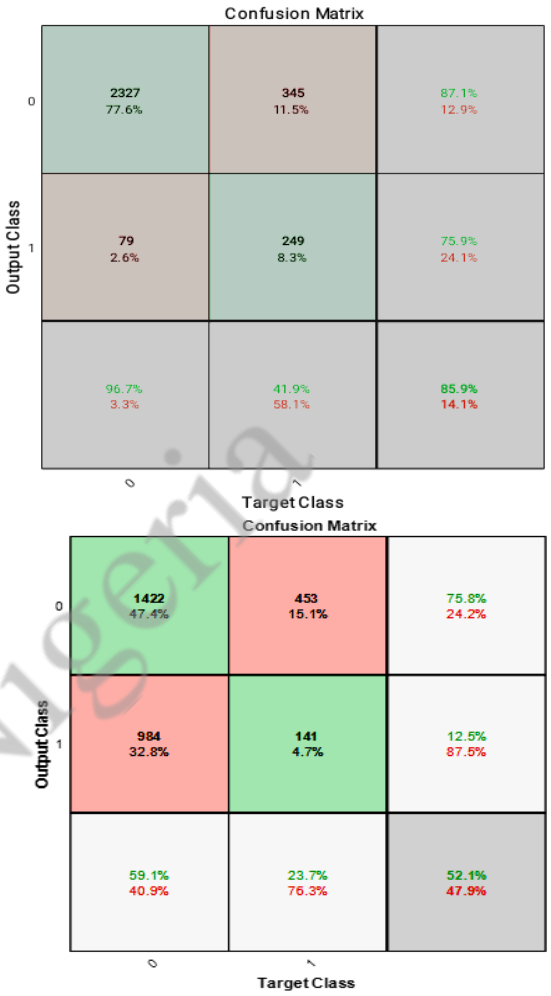
Figure 8: Confusion matrices for ANN, kmeans-ANN and GA-kmeans-ANN

Table 2: Performances of Trained Models

C. Testing Results

Figure 9 show the confusion matrices of the testing carried out on the training models for ANN and Kmeans-ANN respectively and Figure 10 shows the confusion matrix for GA-kmeans-ANN model. Table 3 shows the results calculated from the confusion matrices for the tests. The test

results show that the model trained with ANN performs better in terms of precision, accuracy, sensitivity and specificity followed by the GA-kmeans-ANN model and lastly the kmeans-ANN model. The accuracy of the ANN model is 85.9%, 76.6% for GA-kmeans-ANN and 52.10% for kmeans-ANN model.



a) ANN b) Kmeans-ANN

Figure 9: Confusion matrices for ANN and kmeans-ANN

Models	Precision (%)	Accuracy (%)	Sensitivity (%)	Specificity (%)
ANN	86.70	85.80	96.90	42.70
Kmeans-ANN	99.99	99.90	100.00	99.50
GA-Kmeans-ANN	100.00	100.00	100.00	99.30

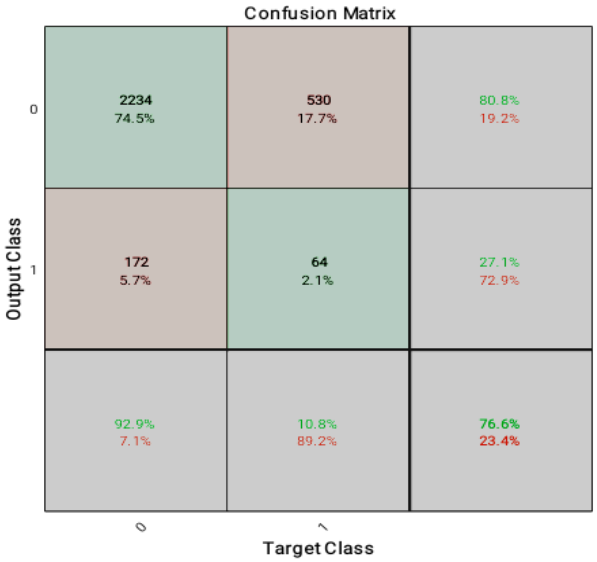


Figure 10: Confusion matrices for GA-kmeans-ANN

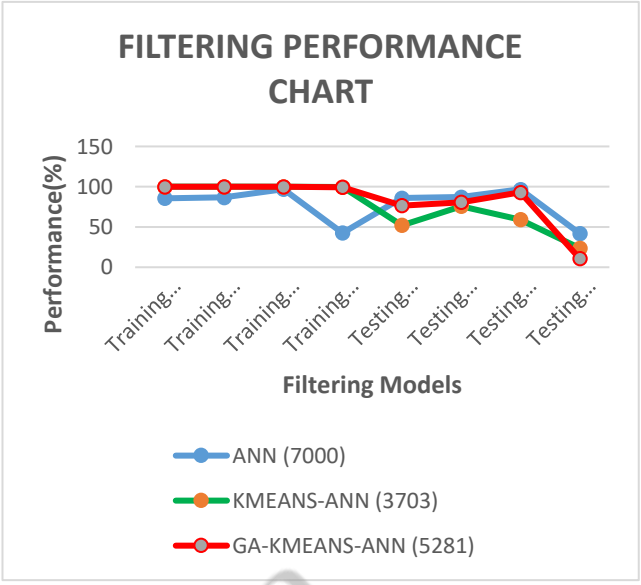


Table 3: Model Testing Results

Models	Precision (%)	Accuracy (%)	Sensitivity	Specificity
ANN	87.10	85.90	96.70	41.90
Kmeans-ANN	75.80	52.10	59.10	23.70
GA-Kmeans-ANN	80.8	76.60	92.90	10.80

D. Discussion of Results

Table 4 shows the combined training and testing results obtained during the experiments. It includes the Number of Training Samples (NTS), accuracy, precision, sensitivity and specificity for ANN, kmeans-ANN and GA-kmeans-ANN respectively. From the results as shown in the model comparison chart in Figure 11, the highest training sample results in the lowest training performance as shown in the blue curve. This is attributed to the noise or outliers present in the training data. In contrast, as the training sample increases, the test performance reduces as shown in the green, red and blue curves respectively. This is attributed to the balance in training and testing samples. The lesser the difference, the better the testing result.

V. CONCLUSION

In this paper, an enhanced bank customer churn prediction model is proposed using optimized (GA-Kmeans) filtering and Artificial Neural Network (ANN). The effects of data filtering on the performance of ANN models for bank customers churn prediction. The dataset was first preprocessed by manually removing attributes that are not useful and partitioning of the data into training and testing in 70:30 respectively. The training data were filtered using kmeans clustering technique and

Table 4: Performance Evaluation Results

MODELS	NTS	Accuracy		Precision		Sensitivity		Specificity	
		Training	Testing	Training	Testing	Training	Testing	Training	Testing
ANN	7000	85.8	85.9	86.7	87.1	96.9	96.7	42.7	41.9
KMEANS-ANN	3703	99.9	52.1	99.99	75.8	100	59.1	99.5	23.7
GA-KMEANS-ANN	5281	100	76.6	100	80.8	100	92.9	99.3	10.8

optimized GA-kmeans clustering technique. The effect of the clustering techniques were evaluated and compared with un-filtered data. The results show that the training performance improved as the noise in the data reduces while the testing results were not improved with filtering. This is because the imbalance between the positive and negative classes affected the testing results. To improve the result of the developed model, the classes of the filtered data will be balanced using an appropriate data balancing technique and the performance will be compared with unbalance dataset.

REFERENCES

[1] Briker, Vitaly; Farrow, Richard; Trevino, William; and Allen, Brent (2019) "Identifying Customer Churn in After-market Operations using Machine Learning Algorithms," SMU Data Science Review: Vol. 2: No. 3, Article 6.

[2] Gde, K., Karvana, M., Yazid, S., Syalim, A., & Mursanto, P. (2019). Customer Churn Analysis and Prediction Using Data Mining Models in Banking Industry. *2019 International Workshop on Big Data and Information Security (IWBIS)*, 33–38

[3] Jeyakarthic, M., & Venkatesh, S. (2020). *An Effective Customer Churn Prediction Model Using Adaptive Gain with Back Propagation Neural Network in Cloud Computing Environment an Effective Customer Churn Prediction Model Using Adaptive Gain with Back Propagation Neural Network In Cloud Computing E*.

[4] Tang, Q., Xia, G., & Zhang, X. (2020). A Customer Churn Prediction Model Based on Xgboost and MLP. *Ieeexplore.Ieee.Org*. Https://Ieeexplore.Ieee.Org/Abstract/Document/9103818/

[5] Vijaya, E. S. J. (2019). Hybrid PPFCM-ANN Model: An Efficient System for Customer Churn Prediction Through Probabilistic Possibilistic Fuzzy Clustering and Artificial Neural Network. *Neural Computing and Applications*, *31*(11), 7181–7200.

[6] Hemalatha, M., & Mahalakshmi, S. (2020). *Predicting Churn Customer In Telecom Using Peergrading Regression Learning Technique*. *6*, 1025–1037.

[7] Li, Y., Wei, J., Kang, K., & Wu, Z. (2019). *An Efficient Noise-Filtered Ensemble Model for Customer Churn Analysis In Aviation Industry*. *37*, 2575–2585.

[8] Mamman J., Aibinu A. M, Abdullahi B. U, Abdullahi I. M, (2015) "Diabetic classification using cascaded data mining technique", International Journal of Computer Trends and Technology, vol. 22, number 2, April 2015.

[9] Arivazhagan, B., & Sankara, S. D. R. S. (2020). Customer Churn Prediction Model Using Regression with Bayesian Boosting Technique in Data Mining. *Ijaema.Com*, *XII*(V), 1096–1103.

[10] Li, W., & Zhou, C. (2020). Customer Churn Prediction in Telecom Using Big Data Analytics. *IOP Conference Series: Materials Science and Engineering*, *768*(5).

[11] Amornvetchayakul, P., & Phumchusri, N. (2020). Customer Churn Prediction for A Software-As-A-Service Inventory Management Software Company: A Case Study in Thailand. *2020 IEEE 7th International Conference on Industrial Engineering and Applications, ICIEA 2020*, 514–518.

[12] Alboukaey, N., Joukhadar, A., & Ghneim, N. (2020). Dynamic Behavior Based Churn Prediction in Mobile Telecom. *Expert Systems with Applications*, 113779.

[13] Kolajo, T., & Adeyemo, A. B. (2015). *Computing, Information Systems & Development Informatics Journal*. *April 2012*.

[14] Makinde, A. S., Oguntuase, A., Vincent, O. R., Acheme, I. D., & Akinwale, A. T. (2020). An Improved Customer Relationship Management Model for Business-To-Business E-Commerce Using Genetic-Based Data Mining Process. *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*.

[15] Fridrich, M. (2017). *Hyperparameter Optimization of Artificial Neural Network in Customer Churn Prediction Using Genetic Algorithm*. *8527*(1), 9–21.

[16] NNA Sjarif, NF Azmi, HM Sarkan, SM Sam, and M. O. (2020). Predicting Churn: How Multilayer Perceptron Method Can Help with Customer Retention in Telecom Industry

Predicting Churn: How Multilayer Perceptron Method Can Help with Customer Retention in Telecom Industry. *IOP Conference Series: Materials Science and Engineering*, 0–5.

[17] Wadikar, D. (2020). Customer Churn Prediction. *Masters Dissertation. Technological University Dublin.*

[18] Zoric, A. B. (2016). *Predicting Customer Churn in Banking Industry Using Neural Networks*. *14*(2), 116–124.

[19] Abbasimehr, H., & Alizadeh, S. (2013). *A Novel Genetic Algorithm Based Method for Building Accurate and Comprehensible Churn Prediction Models*. *2*(4), 1–14.

[20] Ahmad, A. K., Jafar, A., & Aljoumaa, K. (2019). Customer Churn Prediction in Telecom Using Machine Learning in Big Data Platform. *Journal of Big Data*, *6*(1).

[21] Ali, I. (2019). Churn Prediction in Banking System Using K-. *2019 International Conference on Electrical, Communication, And Computer Engineering (ICECCE), July*, 1–6.

[22] Amuda, K. A., & Adeyemo, A. B. (2019). *Customers Churn Prediction in Financial Institution Using Artificial Neural Network*. Http://Arxiv.Org/Abs/1912.11346

[23] Jha N., Parekh D., Mouhoub M., Makkar V. (2020) Customer Segmentation And Churn Prediction In Online Retail. In: Goutte C., Zhu X. (Eds) Advances In Artificial Intelligence. Canadian AI 2020. Lecture Notes in Computer Science, Vol 12109. Springer, Cham. Https://Doi.Org/10.1007/978-3-030-47358-7_33

[24] Liu, Y., & Zhuang, Y. (2015). *Research Model of Churn Prediction Based on Customer Segmentation and Misclassification Cost in The Context of Big Data*. *June*, 87–93.

An Optimized Customers Sentiment Analysis Model Using Pastoralist Optimization Algorithm (POA) and Deep Learning

[1st] Safiya A. Shehu
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
salsaf3637@gmail.com

[2nd] Abdulmalik D.Mohammed
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
drmalik@futminna.edu.ng

[3rd] Ibrahim M Abdullahi
Department of Computer Engineering
Federal University of Technology, Minna
Minna, Nigeria
amibrahim@futminna.edu.ng

***Abstract*—Users usually express their sentiments online which has great influence on the product customers buy. Sentiment analysis is the computational study of people's emotions toward an entity. Sentiment analysis often faces the challenge of insufficient labeled data in Natural Language Processing (NLP) and other related areas. Long Short-Term Memory (LSTM) is one of the deep learning models widely used by researchers in solving sentiment analysis problem. However, they possess some drawbacks such as longer training time, more memory for training, easily overfits, and sensitivity to randomly generated parameters. Hence, there is a need to optimize the LSTM parameters for enhanced sentiment analysis. This paper proposes an optimized LSTM approach using a newly developed novel Pastoralist Optimization Algorithm (POA) for enhanced sentiment analysis. The model was used to analyze sentiments of customers retrieved from Amazon product reviews. The performance of the developed POA-LSTM model shows optimal accuracy, precision, recall. and F1 measure of 77.36%, 85.06%, 76.29%, and 80.44% respectively when compared with the LSTM model with 71.62%, 78.26%, 74.23%, and 76.19% respectively. It was also observed that POA with 20 pastoralist population size performs better than other models with 10, 15, 25, and 30 population size.**

Keywords—*Sentiment Analysis, Natural Language Processing (NLP), Deep Learning, Pastoralist Optimization Algorithm*

I. INTRODUCTION

In recent technology, a huge amount of information, data, reviews, or opinions is being stored in the websites of social media or e-services in the form of raw data. In other to work with those raw data proper methods are required. A study that describes peoples' opinions concerning products, services, and other characteristics is termed sentiment analysis. [1]. Sentiment analysis systematically identifies, quantifies, extracts, and studies affective states and subjective information. It is often used in Web, text, and data mining, and for information retrieval [24]. Sentiment analysis covers other sciences such as; computer, social and management sciences, and so on. To analyze sentiments, objects, and characteristics, viewpoints holder, and direction are the three terms that are used. Sentiment Analysis involves some challenges such as object recognition, opinion orientation classification, and feature extraction. Popular supervised and unsupervised machine learning algorithms have been successfully applied to sentiment analysis [7].

Deep learning, an advanced machine learning model has solved some of the challenges brought about by the lack of vocabulary resources and the improvement of sentiment classification in this field. There are several deep learning models deployed for sentiment analysis. Some of the popular deep learning models include Convolutional Neural network (CNN), Deep Belief Network (DBN), and Recurrent Neural Networks (RNN) [26]. Deep learning has been successful in solving various challenging problems such as Speech recognition, Natural language Processing, (NLP), and Computer vision applications like face recognition. Despite its success, determining the appropriate layers, the number of hidden variables a hidden layer should have, slow training is among the greatest challenge of deep learning [25]. Pastoralist Optimization Algorithm (POA) is a novel metaheuristic inspired by the herding strategies of nomadic pastoralists and developed for optimization [22]. The algorithm has been very successful in solving combinatorial optimization problems and therefore, possesses a suitable candidate for optimizing the deep learning model for sentiment analysis.

In this paper, an optimized sentiment analysis model using deep learning (LSTM) and POA for optimizing the model was proposed. The model will be tested on datasets obtained from the social interactions of users. When developed, the model will improve sentiment analysis tasks by improving the LSTM model and presents an opportunity to explore ideas of audience members and study the state of the product from the opposite perspective. This makes sentiment analysis an ideal tool for expanding product analysis and other market and public business analysis.

The rest of this paper is structured as follows: Section II introduces related works which comprise of sentiment analysis review, deep learning, and POA. In section III, the materials and methods required to accomplish the research objectives are presented. Section IV is a presentation of the expected results and in section V, the conclusion is presented.

II. REVIEW OF RELATED WORKS

A. Sentiments Analysis

The research interest in sentiment analysis has grown over the years due to its importance in various sectors of life. Sentiment analysis can be classified based on some criteria which include; techniques used, dataset structure, and rating level [12]. The figure shows several categories of sentiment

analysis. The various ways in which sentiment analysis can be implemented are;

i. Machine learning-based: This involves training a sentiment analysis model with the existing dataset before deployment [12].
ii. Rule-based: Extracts information from a dataset and tries to assess them according to the polarity of words. There are different rules such as negation words, idioms, dictionary polarity, emoticons [13].
iii. Lexicon-based: Using Semantic orientation in the measurement of opinion and subjectivity of a review or comment generates sentiment polarity either positive or negative [14].

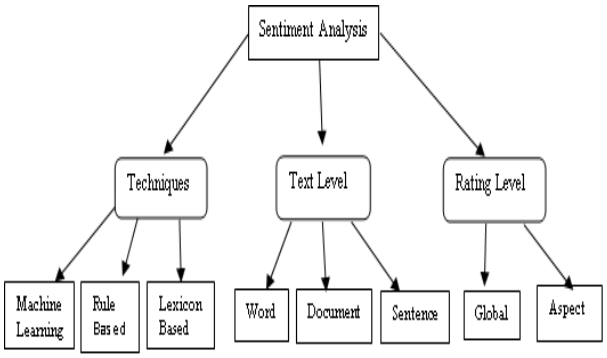


Fig. 1: Categorization of Sentiment Analysis

There are several kinds of research works on sentiment analysis deploying several techniques. This review focuses on reporting the several techniques that have been deployed for sentiment analysis with more emphasis on deep learning architectures. Wang et al. [3] established a bilingual attention network model for sentiment prediction of code conversion. LSTM model was applied for changing each post to its document level representation from which an attention mechanism was used to obtain from different contexts. [4] applied LSTMs to predict sentiments of social media users using multilingual connotation frames as its key method. In [5], an attention-based LSTM for effective sentence recognition.

In [27], a two attention-based two-way LSTM was developed to improve sentiment analysis performance. [6] extends the attention model by distinguishing the attention obtained from the left and right contexts of a given target. They further controlled their attention contribution by adding multiple gates. In [9], a DNN was proposed for information collection. A cascade of LSTM and DNN have constructed document representation and sentiment analysis respectively. Akhtar et al. [7] presented the analysis of ensemble models for emotional grading of financial microblogs and news. In [8], product and user feature and preferences while classifying their sentiments.

B. Deep Learning

Deep learning is an advanced ANN that deployed multiple deep network layers for learning. Due to its ability to solve problems faster than shallow g networks, deep learning has gained more and more attention in recent years. The advancement in computing and big data analytics have made its' deployment feasible [23]. Deep learning models are capable of solving both supervised and unsupervised problems [24]. Popular deep learning models include Convolutional Neural network (CNN), Deep Belief Network (DBN), and Recurrent Neural Networks (RNN) [26]. Deep learning has been successful in solving various challenging problems such as Speech recognition, Natural language Processing, (NLP), and Computer vision applications like face recognition. Despite its success, determining the appropriate layers and number of hidden variables a hidden layer should have has been among the greatest challenge of deep learning [25].

Sentiment analysis is a challenging problem that is being solved using deep learning. Some characteristics of Deep learning include; possessing nonlinear nodes that are arranged in several layers used for transforming and extracting features. [13]. A Deep Coupled Adjective and Noun (DCAN) neural model was proposed by Wang *et al.*, [10]. The key to this technique is harnessing the adjective and noun text descriptions for emotional expressions learning and subsequent sentiment classification. [11] propose a deep neural network model based on LSTM- and CNN-which utilizes word2vec and language embedding to classify claims (classifying sentences to be factual or feeling). [15] proposed a visual sentiment framework using a convolutional neural network and implemented their model on Flickr and Twitter images.

Long Short-term Memory (LSTM) is a special type of RNN used to learn long-term dependencies [23: 25]. Like other RNNs LSTM has a repetitive model, but it is complicated. It has four layers interacting especially together with a hidden state and cell state. Figure 2 shows a typical LSTM model.

.

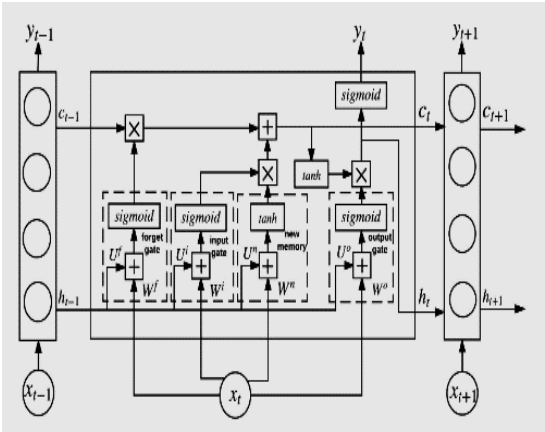


Fig. 2: LSTM deep learning model [23]

Mathematically, LSTM are represented mathematically as follows [23:26]:

$$I_t = \Phi(W_i x_t + V_i H_{t-1} + B_i) \quad (1)$$

$$F_t = \Phi\left(W_f x_t + V_f H_{t-1} + B_f\right) \quad (2)$$

$$O_t = \Phi(W_o x_t + V_o H_{t-1} + B_o) \quad (3)$$

$$C_t = F_t \odot C_{t-1} + I_t \odot tanh(W_c x_t + V_c H_{t-1} + B_c) \quad (4)$$

$$H_t = O_t \odot \tanh(C_t) \quad (5)$$

Where, W and V are the weight parameters and B is the bias vector, x_t and H_t are the input and hidden state vector of LSTM unit at t time respectively while, I_t, O_t, and F_t are the activation vector of input, output, and forget gate respectively. Finally, Φ and C_t are the sigmoid function and memory cell state vector.

C. Pastoralist Optimization Algorithm

Pastoralist Optimization Algorithm (POA) is a novel metaheuristic inspired by the socio-cultural lifestyle of nomadic pastoralists [22]. It mimics the behavior of nomadic pastoralists in the quest for quality pasture, water, and environment for their livestock. In POA, the search agent is called pastoralist and the i[th] pastoralist is represented as:

$$P_i = [P_{1,1}, P_{1,2}, P_{1,3}, \ldots, P_{i,D}] \quad (6)$$

Where D is the dimension of the problem. POA process is made up of two basic phases; the scouting and camping phases. In the scouting phase, pastoralist moves faster with longer step size, and the best scout location is used as camp. The camping phase is characterized by slower movement with a shorter step size. Herding pastoralist split to different locations to minimize local optima entrapment [20]. The initial location of the j[th] pastoralist (S_j) is given in Equation (7) and the new location of the j[th] pastoralist is given in Equation (8) and the evaluation continues until maximum scouting rate is reached [22]

$$S_j = rand([L_b, U_b]^D) \quad (7)$$

$$S'_j = (S_b - S_j) + \varepsilon_j * \eta_j * \zeta \quad (8)$$

Where S'_j is the new location of scout j around the best-found location S_b, ε_j is the energy of scout j ($\varepsilon \in \{-1,1\}$), η_j are the step size of scout j ($\eta \in \{0, (0.001 * \mathrm{Ub})\}$) and ζ is a positive constant that represents the number of times Scouters move faster than herders. The best scout location (S_b) is initialized as the camp location. Splitting by herd pastoralist was achieved using Equation (9) and after each split, the camp size is shrunk using Equation (10).

$$P'_K = P_b + (rand(0, r) * \varepsilon_k * \eta_k) \quad (9)$$

$$r'' = \frac{r'}{nP} \quad (10)$$

Where P'_K is the new location of the k[th] pastoralist, P_b is the best pastoralist so far, $rand(0, r)$ is a random number between 0 and r, $\boldsymbol{r}$ is the camp radius, $\varepsilon_{\boldsymbol{k}}$ is the energy of the k[th] pastoralist ($\varepsilon \in \{-1,1\}$) and $\eta_{\boldsymbol{k}}$ is the step size of the k[th] pastoralist ($\eta \in \{0, (0.001 * \mathrm{Ub})\}$). Also, r'' is the camp radius of current iteration, and r' is the camp radius of the previous iteration. If all locations have been exploited, the best camp location is returned and if all locations have been explored, the best camp location is returned as the global optimum solution, else, the process is repeated with the new scout locations determined using Equation (11).

$$S''_j = rand(L_b, U_b]^D) - S_b \quad (11)$$

Where S''_j is the new scout location, L_b *and* U_b are the lower and upper limit of the search space respectively. POA was evolved using biological evolution strategy and has been very successful when tested on numerical optimization and other combinatorial optimization problems. Other variants of POA with cultural evolution strategy have also been [21], Fig. 3 shows POA steps.

Algorithm 1: Pastoralist Optimization Algorithm
Input: POA Parameters; Search space
Output: Optimal Solution

i. Start
ii. Initialize POA parameters
iii. Select scout pastoralist randomly and initialize scout location
iv. Evaluate the fitness of each scout, update scout locations and normalize scouts' locations within the search space until maximum scouting rate is reached
v. Select best camping location
vi. Evaluate fitness of pastoralist and determine best pastoralist within a camp
vii. Split pastoralist to different locations within camp and evaluate fitness of each pastoralist
viii. Repeat step vii until maximum splitting rate is reached. For each split, divide the current camp radius by the number of pastoralists
ix. Update the best camp pastoralist
x. If all regions within the search space have not been explored,
   a. Update scout location
   b. Repeat steps iv to x and update the global camp best pastoralist
xi. Else, return the global best-found pastoralist
xii. Stop

Fig. 3: Pastoralist Optimization Algorithm (POA) [22]

III. EXPERIMENTAL SETUP

Fig. 4 shows the designed framework to achieve the aim and objectives of this paper. It starts with data collection, preprocessing, and feature extraction. Then, the optimized LSTM model design, training, testing, and finally, the performance evaluation.

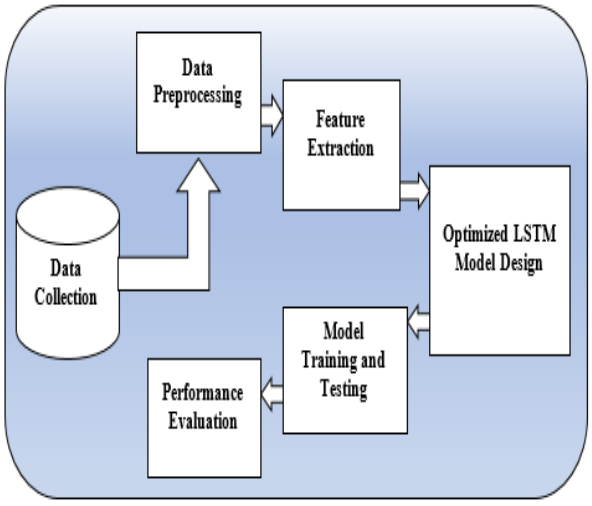


Fig 4: Proposed Methodology

The dataset used for the experiments comprises three review datasets of the Computer dataset which contains 531 sentences. The reviews of all the datasets are from amazon which can be obtained from amazon.com. Table I shows a sample of the computer dataset obtained from amazon. After data collection, the user's post will be preprocessed to transform it from its raw form into a form that enables the machine learning algorithms to understand it. Preprocessing also provides the opportunity to remove noise from the data, which can give more accurate learning algorithms. The pre-processing steps are;

- Removal of URLs

- Removal of special symbols/emoticons
- Removal of stop words from the dataset
- Tokenize the dataset (converting a sequence of strings into pieces of strings/tokens with an assigned or identified meaning).

After data preprocessing, the features required by the learning algorithm for training are extracted. There are two different approaches for text representation which are; word vector representation which represents each word in a document as a vector of N-dimensions. This approach does not capture semantic information and the order or structure of words in a document. It is only concerned with the occurrence of words. The second approach adopted in this paper is word embeddings representation. Word embeddings ensures that the deep learning model receives appropriate syntactic and semantic information by grouping similar words of a text collection in a vector space. Table (I) shows a sample of the dataset.

TABLE I: DATASET SAMPLE

Sentiment	Sentiment Text
1	This item was the most inexpensive 17-inch monitor available to me at the time I made the purchase.
-1	My overall experience with this monitor was very poor.
-1	When the screen wasn't contracting or glitching the overall picture quality was poor to fair.
-1	I've viewed numerous different monitor models since I 'm a college student and this particular monitor had as poor of picture quality as any I 've seen.
-1	A week out of the box and I began to see slight contractions of the screen from time to time , growing more frequent each day.
-1	Display glitches and flashes also occurred.
-1	I could tell this was a `` cheap '' monitor as soon as I set it up.

A. Proposed Model Implementation Steps

Design optimized POA-LSTM and LSTM models by setting appropriate parameters of the LSTM model, such as number of epochs, learning rate, number of hidden units/nodes in the LSTM layer, number of layers, and sequence input. The optimal number of hidden nodes and learning rate are the two parameters that were optimized by the POA. Also, the parameters of the POA, number of pastoralist or population size was investigated.

Six models were trained using 70% of the dataset and tested using 30% untrained data. The first five models are optimized POA-LSTM for 10, 15, 20, 25, and 30 hidden nodes, while the sixth model is the LSTM model. The fitness function (*F*) used by the algorithm for fitness evaluation is the mean squared error given as:

$$F = maximize\ \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

Where, TP (True Positive) is correctly classified as positive sentiments, TN (True Negative) is correctly classified as negative sentiments, FP (False positive) is incorrectly classified as negative sentiments, and FN (False Negative) is incorrectly classified as positive sentiments. Fig. 5 shows the steps in implementing the proposed POA-LSTM sentiment analysis.

Algorithm 2: POA-LSTM Sentiment Analysis Algorithm
Input: Sentiment data; LSTM model
Output: Optimal position; Best model

i. Start
ii. Data collection and pre-processing
iii. Feature extraction
iv. LSTM model design
v. POA parameters initialization and initial population generation
vi. Select scout pastoralist randomly and initialize scout location
vii. Train and test LSTM model
viii. Evaluate the fitness of each scout, update scout locations and normalize scouts' locations within the search space until maximum scouting rate is reached
ix. Select best camping location and initialize pastoralist in the camp
x. Train and test LSTM model using new camp locations
xi. Evaluate fitness of pastoralist and determine best pastoralist within camp
xii. Split pastoralist to different locations within camp
xiii. Train and test LSTM model using new camp locations
xiv. Evaluate fitness of each pastoralist and update local best pastoralist
xv. Repeat step xii – xiv until maximum splitting rate is reached. For each split, divide the current camp radius by the number of pastoralists
xvi. If all regions within the search space have not been explored,
  a. Update scout location
  b. Repeat steps vii - xv and update the global camp best pastoralist
xvii. Else, return the global best-found pastoralist
xviii. Return best model
xix. Stop

Fig. 5: Proposed POA-LSTM implementation steps

B. Performance Evaluation

The performance of the developed models was evaluated using accuracy, precision, and F1 score performance metrics. They are represented mathematically as;

- **Accuracy**

The accuracy of a model is the ratio of all correctly classified samples over all samples and is given as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \tag{13}$$

- **Precision**

Precision is the fraction of samples that were correctly classified and is given as;

$$Precision = \frac{TP}{TP + FP} \times 100\% \tag{14}$$

- **Recall**

Is the ratio of the number of correctly classified positive sentiment and all the positive samples. It is given as:

$$Recall = \frac{TP}{TP + FN} \times 100\% \tag{15}$$

- **F1 Score**

The F1 score is the balance between precision and recall and it is given as:

$$F1 = 2\left(\frac{Precision * Recall}{Precision + Recall}\right) \tag{16}$$

IV. RESULTS AND DISCUSSION

The results obtained for the experiments performed are presented and discussed in this section. Fig 6 shows the convergence curves of the POA-LSTM models for the population size of 10, 15, 20, 25, and 30. The curve indicates the optimum fitness value and the convergence rate for each population size. The result shows that at a population size of 20, the algorithm converges obtaining an optimum value of 0.7736 which is the best value compared to other population sizes. At a population size of 10, 15, and 25, the fitness value is 0.761 and reduces to 0.7484 when the population size was increased to 30. The optimal learning rate and number of hidden nodes selected for 10, 15, 20, 25 and 30 population sizes are; 0.01-17, 0.02-18, 0.01-37, 0.01-5 and 0.02-21 respectively as shown in Table II.

The confusion matrices of the five POA-LSTM models and LSTM models are shown in Fig. 7. The matrix is a count of actual sentiments against predicted sentiments. The matrix shows that the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are; 80, 41, 21, 17 for POA-LSTM (10), 83, 38, 24, 14 for POA-LSTM (15), 74, 49, 13, 23 for POA-LSTM (20), 81, 40, 22, 16 for POA-LSTM (25), 78, 41, 21, 19 for POA-LSTM (30), and 83, 38, 24, 14 for LSTM.

Fig. 8 shows the performance evaluation results of the developed models. It includes the accuracy, precision, recall, and F1 score performance metrics calculated from the TP, TN, FP, and FN values obtained in the confusion matrices in Fig. 7. The accuracy, precision, recall, and F1-Score for the developed models are as follows; for POA-LSTM (10) model, the values are 76.10%, 79.21%, 82.47%, and 80.81% respectively, for POA-LSTM (15) model are 76.10%, 77.57%, 85.57%, and 81.37% respectively. For POA-LSTM (20) model, the values are 77.36%, 85.06%, 76.29%, and 80.44% respectively, for POA-LSTM (15) model are 76.10%, 78.64%, 83.51%, and 81% respectively, while for POA-LSTM (30) model are 74.84%, 78.79%, 80.41%, and 79.59% respectively.

Finally, the accuracy, precision, recall, and F1-Score achieved by the LSTM model trained with 100 nodes is 71.62%, 78.26%, 74.23%, and 76.19% respectively. The performance of the POA-LSTM (20) model outperformed the other models in terms of accuracy and precision, while POA-LSTM (15) outperforms other models in terms of recall, and F1-score. Overall, the optimized models perform better than the un-optimized LSTM model in-terms of all the metrics measured. This could be attributed to training the LSTM models with optimal parameters selected by the POA optimizer.

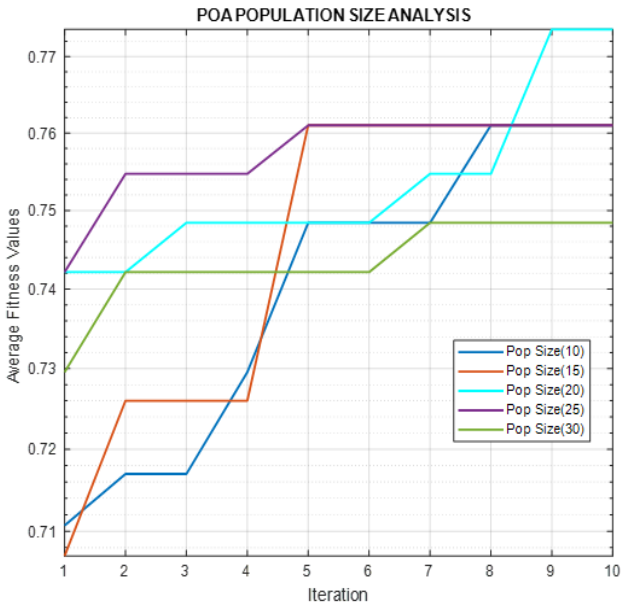


Fig 6: Convergence Curve of POA-LSTM

Table II: POA-LSTM optimization

POA Population Size	Optimal Learning Rate	Optimal Hidden Nodes	Optimal Fitness Value
10	0.01	17	0.7610
15	0.02	18	0.7610
20	0.01	37	0.7736
25	0.01	5	0.7610
30	0.02	21	0.7484

V. CONCLUSION AND FUTURE DIRECTION

In this paper, an optimized sentiment analysis model using Pastoralist Optimization Algorithm (POA) and LSTM deep learning model. The learning rate and node size of the LSTM were optimized and tested on customer's sentiments on a product from Amazon. Then Also, the appropriate population size of the POA algorithm was investigated. The result indicated that the optimized LSTM model performs better in terms of accuracy, precision, recall, and F1-score than the LSTM model. The optimization produces optimal learning rate was found to be 0.02 and an optimal node size of 37 was obtained using POA with 20 pastoralists. This shows that optimized LSTM's can perform better than un-optimized LSTM for sentiment analysis. Furthermore, the POA is capable of being used as a parameter optimizer.

In the future, other sentiment analysis datasets will be explored to evaluate the effectiveness of the developed models. Also, other optimization algorithms such as PSO, ABC, GOA, and BA will be explored to determine their optimization effects on the LSTM model

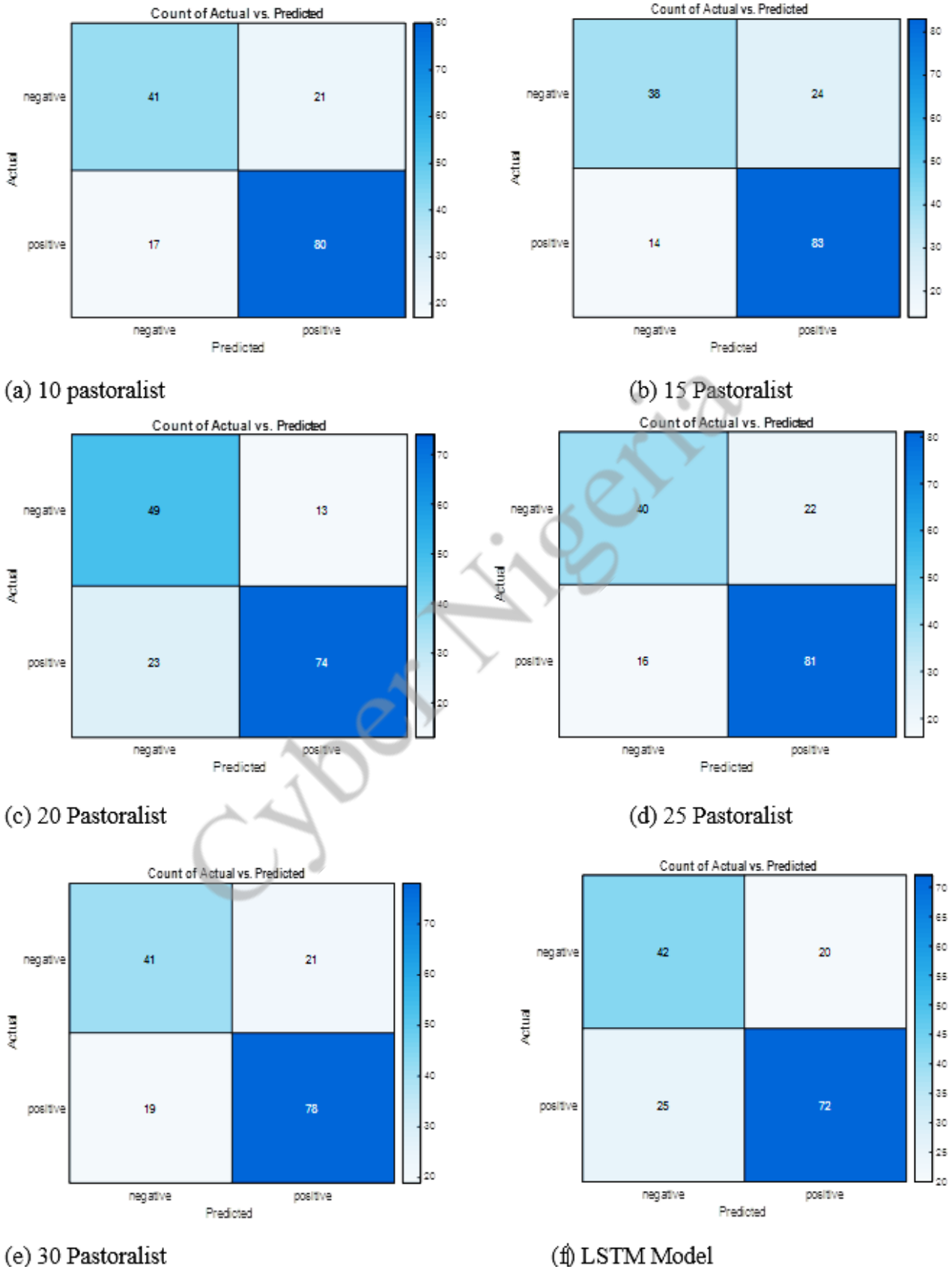


Fig 7: Confusion matrix of POA-LSTM and LSTM models

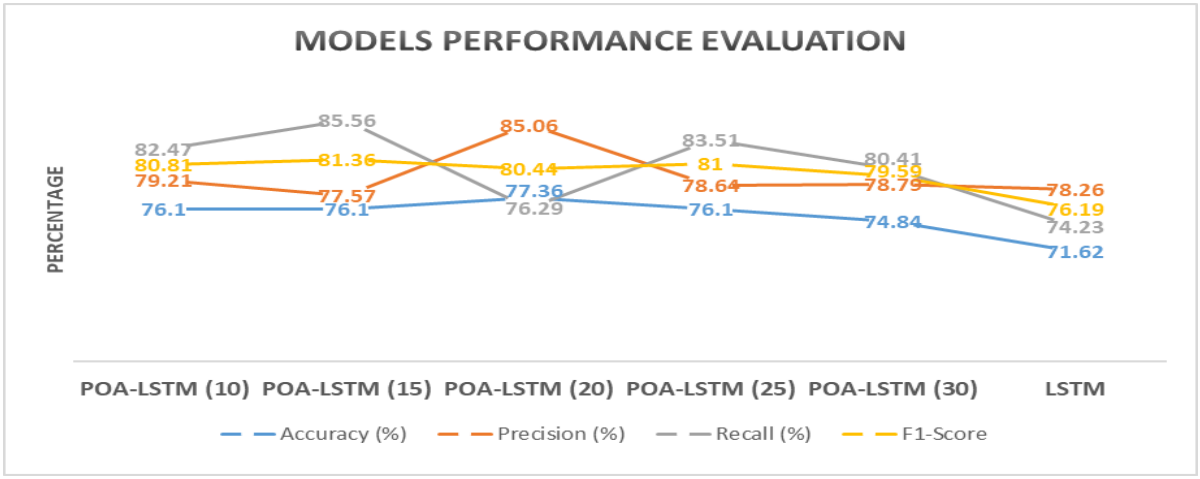


Fig 8: Accuracy, Precision, Recall, and F1-Score graph of all the models evaluated.

REFERENCES

[1] Liu B. Sentiment analysis: mining opinions, sentiments, and emotions. The Cambridge University Press, 2015.

[2] Carlos A. Iglesias and Antonio Moreno. Sentimental Analysis for Social Media, October 2019; Accepted: 19 November 2019; Published: 22 November 2019.

[3] Wang Z, Zhang Y, Lee S, Li S, and Zhou G. A bilingual attention network for code switched emotion prediction. In Proceedings of the International Conference on Computational Linguistics (COLING 2016), 2016.

[4] Rashkin H, Bell E, Choi Y, and Volkova S. Multilingual connotation frames: a case study on social media for targeted sentiment analysis and forecast. In Proceedings of the Annual Meeting of the Association for Computational Linguistics (ACL 2017), 2017.

[5] Wang Y, Huang M, Zhu X, and Zhao L. Attention-based LSTM for aspect-level sentiment classification. In Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP 2016), 2016.

[6] Liu J, Zhang Y. Attention modeling for targeted sentiment. In Proceedings of the Conference of the European Chapter of the Association for Computational Linguistics (EACL 2017), 2017.

[7] Akhtar MS, Kumar A, Ghosal D, Ekbal A, and Bhattacharyya P. A multilayer perceptron-based ensemble technique for fine-grained financial sentiment analysis. In Proceedings of the Conference on Empirical Methods on Natural Language Processing (EMNLP 2017), 2017.

[8] Chen H, Sun M, Tu C, Lin Y, and Liu Z. Neural sentiment classification with user and product attention. In Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP 2016), 2016.

[9] Dou ZY. Capturing user and product Information for document level sentiment analysis with deep memory network. In Proceedings of the Conference on Empirical Methods on Natural Language Processing (EMNLP2017), 2017.

[10] Wang J, Fu J, Xu Y, and Mei T. Beyond object recognition: visual sentiment analysis with deep coupled adjective and noun neural networks. In Proceedings of the Internal Joint Conference on Artificial Intelligence.

[11] Guggilla C, Miller T, Gurevych I. CNN-and LSTM-based claim classification in online user comments. In Proceedings of the International Conference on Computational Linguistics (COLING 2016), 2016.

[12] Z. Xiang and U. Gretzel, "Role of social media in online travel information search. T," Researchgate, 2010.

[13] Lee H, Grosse R, Ranganath R, and Ng A.Y. Convolutional deep belief networks for scalable unsupervised learning of hierarchical representations. In Proceedings of the International Conference on Machine Learning(ICML 2009), 2009.

[14] Collobert R, Weston J, Bottou L, Karlen M, Kavukcuoglu K, and Kuksa P. Natural language processing (almost)from scratch. Journal of Machine Learning Research, 2011.

[15] Kumar, A., &Jaiswal, A. (2019). Systematic literature review of sentiment analysis on Twitter using soft computing techniques. Concurrency ComputatPractExper. https://doi.org/10.1002/cpe.5107.

[16] Salton G, Buckley C. Term-weighting approaches in automatic text retrieval. Inf Process Manag. 1988;24(5):513–23.

[17] Robertson SE, Walker S. Some simple effective approximations to the 2-Poisson model for probabilistic weighted retrieval. In: Proceedings of the 17th annual international ACM SIGIR conference on research and development in information retrieval. New York: Springer Inc.; 1994. p. 232–41.

[18] Heaton, J., Polson, N., & Witte, J. H. (2017). Deep learning for finance: deep portfolios. Applied Stochastic Models in Business and Industry, 33(1), 3–12.

[19] Kraus, M., &Feuerriegel, S. (2017). Decision support from financial disclosures with deep neural networks and transfer learning. Decision Support Systems, 104, 38–48.

[20] Abdullahi I. M., Muázu M. B., Olaniyi O. M., & Agajo, J, (2019), "An Investigative Parameter Analysis of Pastoralist Optimization Algorithm (Poa): A Novel Metaheuristic Optimization Algorithm", Journal of Science Technology and Education 7(3), pp. 267-272. available at: www.atbuftejoste.com.

[21] I. M. Abdullahi, M. B. Mu'azu, O. M. Olaniyi and J. Agajo, (2019), "A Novel Cultural Evolution-Based Nomadic Pastoralist Optimization Algorithm (NPOA): The Mathematical Models," 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf), Zaria, Nigeria, 2019, pp. 1-7, doi: 10.1109/NigeriaComputConf45974.2019.8949635.

[22] Abdullahi I. M., Mu'azu M. B., Olaniyi O. M. & Agajo J. (2018), "Pastoralist Optimization Algorithm: A Novel Nature-Inspired Metaheuristic Optimization Algorithm". *Proceedings International Conference on Global and Emerging Trends, (ICGET 2018)*, Baze University, Abuja, pp. 101-105.

[23] Zhang L., Wang S., Liu B., (2018), Deep Learning for sentiment Analysis: A Survey, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(4), pp. 1-34.

[24] P. Vateekul and T. Koomsubha, A Study of Sentiment Analysis Using Deep Learning Techniques on Thai Twitter Data, 2016.

[25] S. Bengio, L. Deng, H. Larochelle, H. Lee, and R. Salakhutdinov, Guest Editors Introduction: Special Section on Learning Deep Architectures, IEEE Trans. Pattern Anal. Mach. Intell., vol. 35, no. 8, pp. 1795-1797, 2013.

[26] M. Usama, W. Xiao, B. Ahmad, J. Wan, M. M. Hassan and A. Alelaiwi (2019), Deep Learning Based Weighted Feature Fusion Approach for Sentiment Analysis, IEEE Access, 7, pp. 140252-140260.

[27] Yang M, Tu W, Wang J, Xu F, and Chen X. Attention-based LSTM fortarget-dependent sentiment classification.In Proceedings of AAAI Conference on Artificial Intelligence (AAAI 2017), 2017.

Comparative Evaluation of Machine Learning Techniques for the Detection of Diabetic Retinopathy

Rahmat Inuwa
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
rahmatameerah@gmail.com

Sulaimon A. Bashir
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
bashirsulaimon@futminna.edu.ng

Opeyemi A. Abisoye
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
o.abisoye@futminna.edu.ng

Solomon A. Adepoju
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
solo.adepoju @futminna.edu.ng

***Abstract*—Diabetic Retinopathy (DR) is a common diabetes disorder that attacks blood vessels in the light-sensitive tissue known as the retina. It is among the most common causes of loss of vision among patients with diabetes, and it is the leading cause of reduced vision and blindness even among aged adults. Naturally, this occurrence begins with no apparent change in vision. For the identification of DR, ophthalmologists use the retinal image of a patient known as the fundus image, and the blood vessels may also be captured explicitly from the retina. This paper presents a comparative study of five commonly used machine learning techniques: K-Nearest Neighbor, Support Vector Machine and Discriminant Analysis, Naïve Bayes, and Ensembles. The texture characteristics of the fundus image were extracted using the Local Binary Pattern (LBP) descriptor. And this feature extracted using LBP was used to train the classifiers. The proposed method classifies the retina's fundus pictures as "no DR" or "current DR." The Ensemble Classifier (EC) technique generated a better DR detection accuracy of 98.31% than the other four classifiers and existing works based on the classifiers' comparative analysis.**

Keywords— Diabetic Retinopathy, Classification, Feature Extraction, Ensemble Classifier, Machine Learning

I. INTRODUCTION

Diabetes is the most common condition in the human body that causes many complications worldwide [1]. According to estimates from 2014, this disease's incidence rose from one hundred million patients in 1980 to four hundred and twenty-two million patients, with a global prevalence of 4.7% to 8.5% [2]. Patients with a history of diabetes are more prone to diabetic retinopathy [1]. Diabetic retinopathy (DR) is a disease that tends to worsen and is one of the critical causes of blindness and vision loss [3]. DR is a diabetes-related eye condition that arises when the retina's blood vessels swell and leak fluid, leading gradually to vision impairment [4]. Diabetes causes high blood sugar levels that accumulate in the blood vessels, causing damage that impedes or inhibits blood flow to the body's organs, including the eyes, affecting up to 80% of all patients with diabetes for ten years or longer [5]. This assumption facilitates the application of automated diagnostic screening methods to larger populations. DR symptoms include blurred vision, eyespots, and night vision difficulties [6].

The minor disparity between different grades and the existence of many small essential characteristics renders the task of identification very difficult [7]. However, the current approach to detecting DR is a very laborious and time-consuming task that relies heavily on a doctor's capacity [8]. DR automatic detection is necessary to solve these problems. Early-stage identification of DR, which can prevent blindness with appropriate care, is also crucial for diagnosis [9]. The creation of intelligent systems to assist ophthalmologists' decision-making has attracted the scientific community's attention in various works concerning incorrect diagnosis [10][11].

This paper aims to conduct a comparative evaluation of five machine learning methods, namely: Discriminant Analysis Classifier (DAC), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Ensemble Classifier (EC), and Naïve Bayes (NB) classifier utilized for Diabetic Retinopathy (DR) detection and classification. Hence, the significant contributions of this paper include:

1. Classification of retinal fundus images into No DR or Present DR
2. Comparative experimentation of five different classifiers on the features obtained using the LBP feature descriptor.

The rest of this research is structured as follows: a description of related works is given in Section II. Section III explains the methods used for conducting the research. Section IV describes the findings obtained during the experiment and addresses the results presented. In Section V, conclusions have been drawn, and possible studies are presented in Section VI.

II. RELATED WORKS

In the field of computer vision, the task of detecting DR early is a challenging issue. Diagnostic clarity criteria aim to identify clinical characteristics of Diabetic Retinopathy such as haemorrhages, microaneurysms, soft exudates, and hard exudates. It is an essential issue for a proper diagnosis to

extract these signs as they help to determine the actual condition of DR.

Kirange et al. [2] proposed a new method for early-stage identification of DR by recognizing all microaneurysms, the first symptoms of DR, and correctly assigning labels to retinal fundus images grouped into five classes according to the seriousness of lesions. The five grading groups are: No DR, Mild DR, Medium DR, Severe DR, and Proliferative DR. Five standard classifiers were used in this proposed system to perform the classification task. These classifiers are SVM, KNN, Neural Networks (NN), NB, and Decision Tree (DT). The NB classifier was proposed to have surpassed the other four classifiers with an accuracy of 77.86%. Both the Gabor and the LBP descriptor were used for the extraction of features. However, the components extracted using the Gabor descriptor performed much better with an accuracy of 77.86% as compared to the LBP features that provided 41.84% accuracy. A drawback of this analysis is that it focused more on early-stage DR identification without considering the DR proliferation stage.

A graph-based approach to classifying retinal images was suggested by Mangrulkar[12]. The retinal images were pre-processed to eliminate noise and remove irrelevant information. The Canny edge detector was then utilized to identify the edges of the items in the image. Using the kirsch template that defines the presence of an edge, the segmentation process was then performed. The Kirsch model is used for the retrieval of blood vessels from the retinal image. Together with the graph nodes extracted from the image, the Speed-Up Robust Features (SURF) features were extracted by finding the intersection points (that is, pixels with more than two neighbours) and the terminal ends. Using the graph-based method, classification was carried out, and the Artery Vein Ratio (AVR) was measured. The AVR ratio is a realistic measure to classify a diabetes-free or diabetes patient. The proposed process achieved an accuracy of 88%. Without considering a more advanced DR stage, this research only focused on the early phase identification of DR.

A new approach to the diagnosis of Age-related Macular Degeneration (AMD) and DR, as proposed by Morales et al. [13]. The presentation of a new technique for the diagnosis of AMD and DR was the objective of this method. Five experiments were developed and tested using the suggested procedure: separating DR from normal, AMD from normal, pathological from normal, DR from AMD, and the three different classes (AMD, DR, and Normal): The LBP was used as the feature descriptor technique. The most important finding of this study is that the new method can differentiate groups based on an analysis of the retina's spatial texture, thereby removing the retinal lesion's previous segmentation. The results show that using LBP as a texture descriptor for fundus images offers useful retinal disease screening features. This work, however, only investigated the LBP without further searching for more texture descriptors.

A multi-stage transfer learning system and an automated method for detecting the DR stages from a single human fundus image were proposed by Tymchenko et al. [14]. Three Convolutional Neural Network (CNN) architectures (EfficientNet-B4, EfficientNet-B5, and SE-ResNeXt50) were ensemble. CNN was used as a function extractor and as a classifier. The CNNs pre-trained by Imagenet were used for encoder activation. The proposed technique was used for the early detection of DR and achieved a sensitivity and specificity of 0.99.

The Shapley Addictive exPlanations (SHAP) were used to explain characteristics that lead to the disease process evaluation—using SHAP guarantees that the model learns beneficial features during preparation and uses correct characteristics at an inferential time. This approach's main advantage is that it increases generalization and eliminates uncertainty using a network ensemble, pre-maintained on a large dataset and precisely tuned to the target dataset. This analysis can be extended with SHAP calculation for the entire ensemble, not just for a particular network, which can provide a more precise optimization of hyper-parameters.

Li et al. [5] introduced a novel algorithm based on a Deep Convolution Neural Network (DCNN). In this paper, the regular DCNN max-pooling layers were replaced by a fractional max-pooling layer. Two DCNNs with differing numbers of layers were prepared for classification to achieve more discriminatory features. After integrating features from image metadata and DCNNs, the SVM classifier was trained to learn the inherent limits of distributions of each class. The proposed DR method classifies DR phases into five categories, labelled with an integer ranging from 0 to 4. The test results indicate that the proposed technique can reach a recognition rate of up to 86.17%. The dataset used for training in this study had an insufficient number of images of lesions 3 and 4, limiting the proposed method.

Arade and Patil [3] conducted a comparative study of DR using the K-NN and Bayesian classifier. An automated image processing system that detects DR gradation is presented in this paper. Blood vessel segmentation was done using the kirsch process, as it was found that retinal photos effectively differentiated the blood vessels. Differentiated vessels were extracted using moment invariants, grey level features. The DR severity was identified along with K-NN and Bayesian classifier using a feed-forward neural network. To validate the results obtained with an ophthalmologist, it was indicated that the Bayesian classifier generates results comparable to the expert opinion than the K-NN classifier. The accuracy of the Bayesian classifier obtained is 74%, while the precision for K-NN is 66%. It is possible to expand this work by training more classifiers.

III. METHODOLOGY

This section presents the techniques used to achieve the aim of this study. Fig. 1 illustrates the methods used.

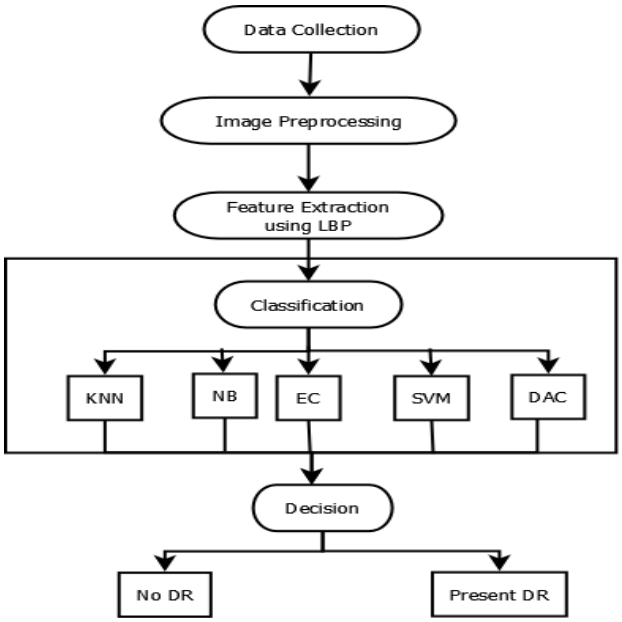


Fig. 1.Proposed System

A. Dataset

The database consists of 130 colour fundus images, 20 of which are regular and 110 showed signs of DR (hard exudates, microaneurysms, haemorrhages, soft exudates, and neovascularization). The photos were collected from the Imageret project [15], and this set of data is referred to as "calibration level 0 fundus images. To train the classification models, 80% of the data set was used, and the remaining 20% was used to test the model."

B. Image Preprocessing

The retinal fundus images were pre-processed to remove noise and correct the uneven illumination. In this proposed process, the input colour image was converted to a grey level image, and the grey-level image was improved using histogram equalization.

C. Feature Extraction

Feature Extraction is a dimensionality reduction method by which the initial raw data collection is reduced to more controllable classes. It also deals with creating variables to get around issues while describing the data with adequate accuracy. In this study, the LBP descriptor was used to extract DR features.

1) Local Binary Pattern (LBP)

Local binary patterns (LBP) is a powerful grey-scale texture operator used in many computer vision tasks due to its computational simplicity[16][17]. In LBP, the first stage is to create a label centred on the local neighbourhood of the pixel defined by the radius, R, and several points, P [13], for each pixel of the image in which the label is placed. The neighbouring pixels are the threshold for the neighbourhood's central pixel's grey value, creating a binary string. The LBP label value is derived for each pixel by summing the weighted binary string with powers of 2 [17].

LBP is an adaptive image texture descriptor that sets the neighbouring pixel thresholds to the current pixel value[18]. Given the neighbourhood of the C sample points on the R radius circle and given a pixel at (xp, yp). It is possible to express LBP, as shown in Equation (1) :

$$\mathrm{LBP}_{\mathrm{C,R}(\mathrm{x_p},\mathrm{y_p})} = \sum_{\mathrm{C}=0}^{\mathrm{C}-1} \mathrm{s}(\mathrm{i_C} - \mathrm{i}_P)2^C \quad (1)$$

where i_c and i_p are, respectively, grey-level values of the central pixel and P surrounding pixels in the circle neighbourhood with a radius D, and function f(x) is defined in Equation (2) as:

$$\mathrm{f(x)} = \begin{cases} 1 & \text{if } \mathrm{x} \geq 0 \\ 0 & \text{if } \mathrm{x} < 0 \end{cases} \quad (2)$$

D. Diabetic Retinopathy Classification

Machine learning's capacity lies in its ability to generalize by correctly classifying unknown data based on models built using the training dataset. The collected retinal fundus images have been categorized into two classes: No DR and Present DR. No DR category implies that the fundus image is a normal image whereas the present DR category means that DR is present in the fundus image. In this research, experimentation was carried out using five classification techniques, and these techniques are discussed in the subsections below.

1) Discriminant Analysis Classifier (DAC)

DAC is a multivariate statistical technique that is used to create a model for group membership prediction. The model comprises discriminating functions that emerge to provide the best group discrimination based on a linear combination of predictive variables. Such functions are derived from a sample of established group memberships [19]. They could then be applied to new individuals with measures related to the same variables and unknown memberships. While in behavioural sciences, discriminatory analysis is not widely used as the assumptions are not always easy to satisfy. DAC is a multivariate statistical and mathematically robust approach used in cases where groups are defined a priori. Each instance must be scored on one or more quantitative indicator measures and scored on a group test. Discriminant analysis is a method of classification. DAC operates when continuous quantities are calculated on independent variables for each measurement[20].

2) Support Vector Machine (SVM)

SVM is an algorithm used in supervised learning. The algorithm is based on statistical learning theory [21]. The algorithm is founded on the structural risk minimization principle; it can compact the array of raw data to a support vector set and learn how to obtain a function for classification decision [22]. The SVM model iterates over a collection of labelled training samples to discover a hyper-plane that, by finding data points, generates an optimal limit for the decision. Support vectors optimize class separation [23]. In the input space, the decision function of a binary SVM is represented in equation (3) below:

$$\gamma = h(x) = sign\left(\sum_{j=1}^{n} u_j y_j K\left(x, x_j\right) + v\right) \quad (3)$$

where x is the feature vector to be categorized, j indexes the training instances, n is the number of training instances, y_j is the label (1 or –1) of training example j, K(,) is the kernel function, and u_j and v are fit to the data to maximize the margin. Training vectors for which $u_j \neq 0$ are called support vectors [24].

3) Naïve Bayes (NB)

The NB Classification illustrates both a supervised learning approach and a statistical classification system. It presumes an intrinsic probabilistic model and helps measure the probabilities of the results, to acquire principled uncertainty about the model [24]. The NB classifier is a probabilistic approach of machine learning focused on using the Bayes theorem with elevated assumptions of feature independence. NB classifiers are highly scalable and need many linear parameters in the number of problem functions for learning [25]. In NB Bayes theorem offers a way of computing the posterior probability $P(x|y)$ from $P(x)$, $P(y)$ and $P(y|x)$. Equation (4) and (5) presented the equation for posterior probability $P(x|y)$.

$$P(x|y) = \frac{P(y|x) \times P(x)}{P(y)} \quad (3)$$

$$P(x|y) = \frac{P(y_1|x) \times P(y_2|x) \times \ldots \times P(y_n|x) \times P(x)}{P(y_1,\ldots,y_n)} \quad (4)$$

4) Ensemble Classifier (EC)

Ensemble learning generates various base classifiers from which a new classifier is obtained that performs better than any of the components classifiers. These base classifiers may differ according to the algorithm, hyper-parameters, representation, or training set used [26]. The principal objective of the ensemble approach is to decrease bias and variance. Ensembles combine multiple hypotheses to establish a more robust inference [27]. An ensemble is a supervised learning technique itself, as it can be trained and then used to make predictions [27]. Therefore, the ensemble classifier reflects a single hypothesis. However, within the model's hypothesis space from which it is built, this hypothesis is not inherently included. Thus it has been shown that ensembles have more versatility in the functions they can represent. Experimentally, where there is a substantial variance between models, ensembles tend to produce better performance [28]. Many ensemble methods, therefore, aim to encourage diversity among the models that they combine.

5) K-Nearest Neighbor (KNN)

K-NN is among the most straightforward algorithms for machine learning tasks. An item is classified by the "distance" from its neighbours, and the item is assigned to the class of its nearest k-distance neighbours that is most prevalent [29]. The algorithm becomes the nearest neighbour algorithm if k = 1, and the object is assigned to the class of its nearest neighbour. This number K specifies the number of neighbours an item has [30].

The Euclidean distance, which is a linear distance between 2 points in Euclidean space, is generally used to measure the distance between 2 vector positions in multi-dimensional space [30]. If two vectors y_i and y_j are given where yi =(y_{i1}, y_{i2}, y_{i3}, …, y_{in}) And y_j =(y_{j1}, y_{j2}, y_{j3}, …, y_{jn}) Then the Euclidean distance between y_i and y_j is given in equation (6) as:

$$D(y_i, y_j = \sqrt{\sum_{k=1}^{n} (y_{ik} - y_{jk})^2} \quad (6)$$

K-NN algorithm can be summarized as follows:

- Step 1: Along with a new sample, specifies a positive integer k.
- Step 2: Pick k entries that are closet to the new instance in the database.
- Step 3: For those entries, the most common classification is found.
- Step 4: This is the classification we give to the new sample.

E. Performance Metric

- **Accuracy:** Accuracy is specified as the rate of correct classifications. This is the number of predictions, divided by the total number of predictions made, that is correct. In equation (7), the exact formula is given:

  Accuracy=(TP + TN)/(TP + TN + FP + FN) (7)

  TP stands for True Positives, TN stands for True Negative, FP stands for False Positives, and FN stands for False Negative.

- **Recall:** Recall: it is also known as sensitivity. Recall is a statistic that calculates the amount of accurate positive predictions that could have been made from all positive predictions. The recall is determined on the basis of the formula in equation (8).

  $$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (8)$$

- **Precision**: Precision: is a metric calculating how many positive predictions are accurately made. The amount of true positive elements is calculated as divided by the sum of true positives and false positives [31]. Precision is defined according to the formula in equation (9).

  $$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (9)$$

- **Specificity:** This is the percentage of true negatives that during testing are correctly detected by the classifier. Specificity is computed using the formula in equation (10).

  $$Specificity = \frac{True\ Negatives}{True\ Negatives + False\ Positives} \quad (10)$$

IV. Result and Discussion

In this work, experiments were conducted on five different machine learning algorithms: DAC, KNN, SVM, EC and NB classifier with respect to DR identification and classification. The LBP feature which was extracted from the pre-processed fundus images was feed to the five classifiers. The results of the different classification techniques are shown in Table 1.

TABLE 1. DIABETIC RETINOPATHY CLASSIFICATION RESULT

Techniques	Accuracy (%)	Precision (%)	Recall (%)	Specificity (%)
Discriminant Analysis Classifier (DAC)	86.76	84	80	91.7
Support Vector Machine (SVM)	94.46	91	89	96.9
Naïve Bayes (NB)	79.08	76	73.6	93
K-Nearest Neighbor (K-NN)	90.62	89.8	88.67	95.5
Ensembles Classifier (EC)	**98.31**	**95**	**100**	**97.3**

Table 1 shows that Ensembles classifier (EC) produced the highest classification accuracy with a value of 98.31% compared to K-NN, SVM, NB, and DAC with classification accuracy 90.62%, 94.46%, 79.08%, and 86.76%, respectively. Based on the precision metric, it can be seen that EC produced a higher precision value of 95% as compared to DAC, NB, K-NN, and SVM with 84%, 76% 89.8%, and 91% respectively. Table 1 shows that EC has a high recall value of 100% inferring that number of correct positive predictions made out of all the positive predictions is better than the positive prediction made by DAC, SVM, NB and K-NN with a recall of 80%, 89%, 73.6 % and 88.67% respectively. Evaluating from the specificity perspective, EC produces the highest specificity of 97.3%, followed by SVM with a specificity of 96.9%. EC classifier is more appropriate for a reliable DR identification compared to the other four classifiers from the results of accuracy, recall, precision, and specificity obtained.

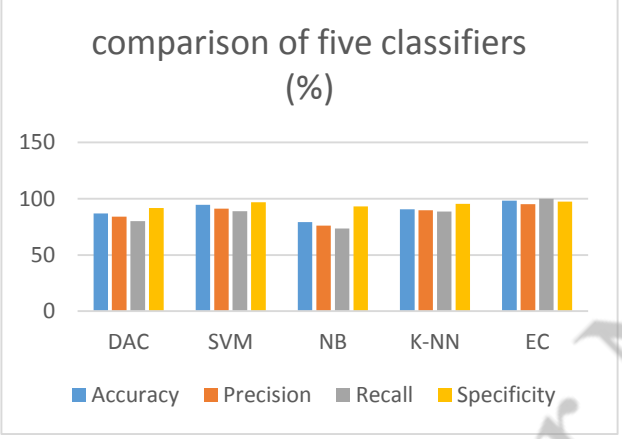


Fig. 2. Comparison of Five Classifiers

Fig. 2 presents a graphical representation of the values of precision, accuracy, recall and specificity depicted in table 1.

TABLE 2. COMPARISON OF ENSEMBLE CLASSIFIER WITH RELATED WORKS

Algorithm	**Accuracy (%)**
Ensemble (proposed method)	**98.31**
Deep Neural Network-PCA-Firefly[31]	97
Artificial Neural Network (ANN)[32]	96

Table 2 shows a comparison of the Ensemble classifier's accuracy (EC) and the DNN-PCA-Firefly and ANN. The proposed method achieved a higher accuracy of 98.31% compared to DNN-PCA-Firefly and ANN, which reached an accuracy of 97% and 96% respectively.

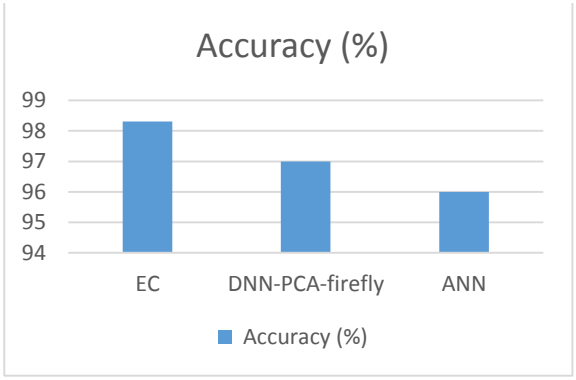


Fig. 3. Comparison with related works

Fig. 3 presents a graphical representation of the values of precision, accuracy, recall and specificity depicted in table 2.

V. Conclusion

This paper produced a comparative result for five classifiers, namely: K-NN, SVM, DAC, NB and EC in respect to DR detection and classification using LBP extracted features. The obtained results demonstrate that using LBP texture descriptors for fundus images provides useful DR disease screening features. From the presented comparative analysis, the investigation of K–NN, SVM, DAC, EC and NB has been executed. The performance metric shows that EC performs better when contrasted with the other four methods. The accuracy estimation of the EC technique was observed to be 98.31% which shows the high effectiveness of EC for DR identification. It can be inferred from the results obtained that the application of the EC technique for the classification of the fundus image produces better results than those provided in current works. In conclusion, a comparative evaluation of five machine learning techniques for diabetic retinopathy identification has been presented.

VI. Future Works

In this study only the LBP feature descriptor was used, hence for future work more feature descriptors such as Histogram of Oriented Gradient, SURF, Scale Invariant Feature Transform etc. can be used or combined to improve the system robustness. In this work, the comparative analysis was focused on five machine learning techniques. The number of machine learning techniques used can be increased to improve the study's flexibility and robustness for future work.

References

[1] J. Amin, M. Sharif, M. Yasmin, H. Ali, and S. L. Fernandes, "A method for detecting and classification of diabetic retinopathy using structural predictors of bright lesions," *J. Comput. Sci.*, vol. 19, pp. 153–164, Mar. 2017, doi: 10.1016/j.jocs.2017.01.002.

[2] D. K. Kirange, J. P. Chaudhari, K. P. Rane, K. S. Bhagat, and N. Chaudhri, "Diabetic Retinopathy Detection and Grading Using Machine Learning," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 6, pp. 3570–3576, Dec. 2019, doi: 10.30534/ijatcse/2019/139862019.

[3] S. P. Arade and J. K. Patil, "Comparative Study Of Diabetic Retinopathy Using K-NN And Bayesian Classifier," *Int. J. Innov. Eng. Res. Technol.*, vol. 4, no. 5, pp. 55–61, 2017.

[4] M. W. Khan, "Diabetic Retinopathy Detection using Image Processing: A Survey," vol. 1, no. 1, p. 6, 2013.

[5] Y.-H. Li, N.-N. Yeh, S.-J. Chen, and Y.-C. Chung, "Computer-Assisted Diagnosis for Diabetic Retinopathy Based on Fundus Images Using Deep Convolutional Neural Network," *Mob. Inf. Syst.*, vol. 2019, pp. 1–14, Jan. 2019, doi: 10.1155/2019/6142839.

[6] R. Rajalakshmi, R. Subashini, R. M. Anjana, and V. Mohan, "Automated diabetic retinopathy detection in smartphone-based fundus photography using artificial intelligence," *Eye*, vol. 32, no. 6, pp. 1138–1144, Jun. 2018, doi: 10.1038/s41433-018-0064-9.

[7] Y. Kumaran and C. M. Patil, "A Brief Review of the Detection of Diabetic Retinopathy in Human Eyes Using Pre-Processing & Segmentation Techniques," vol. 7, no. 4, p. 11, 2018.

[8] F. Arcadu, F. Benmansour, A. Maunz, J. Willis, Z. Haskova, and M. Prunotto, "Deep learning algorithm predicts diabetic retinopathy progression in individual patients," *Npj Digit. Med.*, vol. 2, no. 1, p. 92, Dec. 2019, doi: 10.1038/s41746-019-0172-3.

[9] A. Ahmad, A. B. Mansoor, R. Mumtaz, M. Khan, and S. H. Mirza, "Image processing and classification in diabetic retinopathy: A review," in *2014 5th European Workshop on Visual Information Processing (EUVIP)*, Villetaneuse, Paris, France, Dec. 2014, pp. 1–6, doi: 10.1109/EUVIP.2014.7018362.

[10] A. Pak, A. Ziyaden, K. Tukeshev, A. Jaxylykova, and D. Abdullina, "Comparative analysis of deep learning methods of detection of diabetic retinopathy," *Cogent Eng.*, vol. 7, no. 1, p. 1805144, Jan. 2020, doi: 10.1080/23311916.2020.1805144.

[11] M. Islam, A. V. Dinh, and K. A. Wahid, "Automated Diabetic Retinopathy Detection Using Bag of Words Approach," *J. Biomed. Sci. Eng.*, vol. 10, no. 05, pp. 86–96, 2017, doi: 10.4236/jbise.2017.105B010.

[12] R. S. Mangrulkar, "Retinal Image Classification Technique For Diabetes Identification," p. 6, 2017.

[13] S. Morales, K. Engan, V. Naranjo, and A. Colomer, "Retinal Disease Screening Through Local Binary Patterns," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 184–192, Jan. 2017, doi: 10.1109/JBHI.2015.2490798.

[14] B. Tymchenko, P. Marchenko, and D. Spodarets, "Deep Learning Approach to Diabetic Retinopathy Detection," *ArXiv200302261 Cs Stat*, Mar. 2020, Accessed: Aug. 23, 2020. [Online]. Available: http://arxiv.org/abs/2003.02261.

[15] T. Kauppi *et al.*, "DIARETDB0: Evaluation Database and Methodology for Diabetic Retinopathy Algorithms," p. 17, 2006.

[16] D. Huang, C. Shan, and M. Ardabilian, "Local Binary Patterns and Its Application to Facial Image Analysis : A Survey," *IEEE Trans. Syst. MAN Cybern.*, no. November, 2011, doi: 10.1109/TSMCC.2011.2118750.

[17] N. P. Jeyashree and A. Deepak, "Detection Of Retinal Disease By Local Binary Pattern," *Int. J. Pure Appl. Math.*, vol. 119, no. 15, p. 10, 2018.

[18] D. Sarwinda, A. Bustamam, and A. Wibisono, "A Complete Modelling of Local Binary Pattern for Detection of Diabetic Retinopathy," *Int. Conf. Inform. Comput. Sci.*, p. 4, 2017.

[19] Ş. Büyüköztürk, "Discriminant Function Analysis: Concept and Application," *Eurasian J. Educ. Res.*, vol. 33, 2008.

[20] B. Ghojogh and M. Crowley, "Linear and Quadratic Discriminant Analysis: Tutorial," *ArXiv190602590 Cs Stat*, Jun. 2019, Accessed: Aug. 26, 2020. [Online]. Available: http://arxiv.org/abs/1906.02590.

[21] J. Cao, M. Wang, Y. Li, and Q. Zhang, "Improved support vector machine classification algorithm based on adaptive feature weight updating in the Hadoop cluster environment," *PLOS ONE*, vol. 14, no. 4, p. e0215136, Apr. 2019, doi: 10.1371/journal.pone.0215136.

[22] S. Ghosh, A. Dasgupta, and A. Swetapadma, "A Study on Support Vector Machine based Linear and Non-Linear Pattern Classification," in *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, Tamilnadu, India, Feb. 2019, pp. 24–28, doi: 10.1109/ISS1.2019.8908018.

[23] P. Walsh, "Support Vector Machine (SVM) Learning for ECG Classification," *Smart Healthc. Saf. Syst.*, p. 10, 2019.

[24] A. Sopharak *et al.*, "Machine learning method to automatic exudate detection in retinal images from diabetic patients," *J. Mod. Opt.*, vol. 57, no. 2, pp. 124–135, Jan. 2010, doi: 10.1080/09500340903118517.

[25] V. Sudha and C. Karthikeyan, "Analysis of diabetic retinopathy using naive Bayes classifier technique," *Int. J. Eng. Technol.*, vol. 7, no. 2.21, p. 440, Apr. 2018, doi: 10.14419/ijet.v7i2.21.12462.

[26] M. M. Habib, R. A. Welikala, A. Hoppe, C. G. Owen, A. R. Rudnicka, and S. A. Barman, "Detection of microaneurysms in retinal images using an ensemble classifier," *Inform. Med. Unlocked*, vol. 9, pp. 44–57, 2017, doi: 10.1016/j.imu.2017.05.006.

[27] Deakin University, Australia, A. Rahman, and S. Tasnim, "Ensemble Classifiers and Their Applications: A Review," *Int. J. Comput. Trends Technol.*, vol. 10, no. 1, pp. 31–35, Apr. 2014, doi: 10.14445/22312803/IJCTT-V10P107.

[28] G. Brown, J. Wyatt, R. Harris, and X. Yao, "Diversity Creation Methods: A Survey and Categorisation," p. 28, 2005.

[29] J. Bethanney, S. Divakaran, S. Abraham, G. Meera, and G. UmaShankar, "Detection and classification of exudates in a retinal image using image processing techniques," *J. Chem. Pharm. Sci.*, vol. 8, no. 3, 2015, [Online]. Available: www.jchps.com.

[30] A. Kataria and M. D. Singh, "A Review of Data Classification Using K-Nearest Neighbour Algorithm," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 6, pp. 354–360, 2013.

[31] T. R. Gadekallu *et al.*, "Early Detection of Diabetic Retinopathy Using PCA-Firefly Based Deep Learning Model," *Electronics*, vol. 9, no. 2, p. 274, Feb. 2020, doi: 10.3390/electronics9020274.

[32] U. Sankar, R. Vijai, and R. Balajee, "Detection and Classification of Diabetic Retinopathy in Fundus Images using Neural Network," *Int. Res. J. Eng. Technol.*, vol. 5, no. 4, pp. 2630–2635, Apr. 2018.

A Review on Machine Learning Techniques for Image Based Spam Emails Detection

Muhammad Abdullahi
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
mibnmagaji22@gmail.com

Sulaimon A. Bashir
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
bashirsulaimon@futminna.edu.ng

Abdulmalik D. Mohammed
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
drmalik@futminna.edu.ng

Opeyemi O. Abisoye
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
o.abisoye@futminna.edu.ng

***Abstract*—Sending and receiving e-mails have continued to take the lead being the easiest and fastest way of e-communication despite the presence of other forms of e-communication such as social networking. The rise in online transactions through email has globally contributed to the increasing rate of spam emails relatively which has been a major problem in the field of computing. In this note, there are many machine learning techniques available for detecting these unwanted spams. In spite of the significant progress made in the figures of literature reviewed, there is no machine learning method that has achieve 100% accuracy. Each algorithm only utilizes limited features and properties for classification. Therefore, identifying the best algorithm is an important task as their strengths need to be weighed against their limitations. In this paper we explored different machine learning techniques relevant to the spam detection and discussed the contributions provided by researchers for controlling the spamming problem using machine learning classifiers by conducting a comparative studies of the selected machine learning algorithms such as: Naive Bayes, Clustering techniques, Random Forest, Decision Tree and Support Vector Machine (SVM)**

Keywords—Spam Image, Email Classification, Filtering Techniques.

I. INTRODUCTION

Email almost serves as a requirement for e-transactions. Sending and receiving e-mails have continued to take the lead being the easiest and fastest way of e-communication despite the presence of different types of e-communications. The rise in the applications of email and online transaction through emails has globally contributed to high rate of email spamming which has been a major problem in the field of computing. There are many machine learning methods available for detecting these unwanted spams. In spite of the significant progress made in the figures of literature reviewed, there is no machine learning method that has achieve 100% accuracy [1]. Each algorithm only utilizes limited features and properties for classification.

The successful and increasing use of the internet has encouraged a quick and easy types of online transactions and different ways of e-communication, the common example of this is emailing. However, it has become very common to send and receive emails as a major means of communication [1]. The increasing rate of spam mails is continuous and alarming, i.e. the bulk distribution of unwanted emails mostly of a commercial purpose with unpleasant content has subjected the service providers to a major problem [1] which endangers the confidentiality of the users and causes loss of resources. Since they are causing enormous misfortunes for the organizations, starting with the waist of bandwidth, mail server load to the profitability of clients due to the time spent identifying and handling spam mail senders. Spam messages do not only increase device correspondence and loss of storage facility but also used for numerous attacks and to bridge security measures. This violence can be used to abuse the client data and take their valuable sensitive data such as passwords and financial details [1, 3].

The latest survey study on email server revealed that 60% of all email traffic is spam, therefore making it mandatory to create an anti-spam filters. The current spam filters are developed for detecting different spam mails based on the features. In particular, the technique of text categorization is used to filter email spam. But spammers has employed a new way of succeeding the available filters by attaching a textual based content on image in the mail, experiencing image spam a another trick which is so far the most modern kind spam mail with obfuscation. Notwithstanding, emails have continue to maintain success in the area of online business transaction and are now are now a necessity for other means of online communication. Practically, almost all human uses emails. The author in [12] estimated that by the end of 2020, next to half of the global population expected to use emails.

The emails popularity and increase in its application for electronic communication has resulted to an increase in the amount of spam emails globally. Spam emails which are also known as junk emails are unsolicited message content sent by email to several recipients and not requested. Researchers in [13] opined that the spammers had no previous relationship with the recipient but send the spam mails on destructive purpose after collecting addresses from various sources such as tagged filled forms, phone book and spam messages. Spamming is a rapidly growing means of attack such as phishing, worms and virus as the most dangerous threat to the users of email [14, 15].

Supervised methods such as classification or prediction task aimed at discovering the hidden classes between the independent variable and target class are popularly used method for data processing according to [16]. Classifiers allow the observations to be assigned to tags for supervised learning, so that unobserved data can be classified in accordant with the trained data. Spam detection systems are focused on using estimate of arrangements to quantify messages as either spam or not.

In recent times undesirable business messages such as spam have become a major issue associated with the network. It alludes to the person sending spam messages as the spammers who collect email addresses from various web pages and chat rooms [22]. Spam ensures that the users are

not able to make proper utilization of time and storage space to the maximum rate. The considerable amount of spam mail that flows through computer networks has detrimental impact on email server memory space, bandwidth, user time and processing power [23]. The threat of spam email is growing on annual base and account for more than 77% of the entire traffic of email globally [23].

The rest part of this paper is structured as follows: Section 2 provides a brief review of related literature in the field of classification algorithms for the detection and filtering of spam email. Section 3 demonstrates the emerging spam filtering approaches and the essential description about the selected machine learning techniques for spam email classification. Section 4 conduct a comparison on the areas of their strength and limitations using performance metrics and present the result and discussion and lastly, Section 5 present the conclusion.

II. RELATED STUDIES

In the interest of the global research community, the rapid rise in email spam filtering is attributed to the increase in spam emails which has led many comparative studies by the researchers on the efficacy of spam image based email classification techniques using hybridized metrics. Hence it is important to identify the technique that can work better on a particular metric to support correct separation of emails to either be a spam or not. Here, we take an over view of the related and current scientific research works presented in the literature under the scope of approaches to filtering image spam-based emails that are low-level methods, Optical Character Recognition (OCR) based methods and those that involve both methods.

Chopra et al. [1] applied two stage approach for classifying the textual part of a given image to identify words in the mail as either spam or non-spam. In the first stage, OCR tool was used and Bayesian algorithm was used in the researchers stated in their paper titled "The Image and text spam filtering" that spammers has introduced new technique to embed spam mails into the image attached to the package. In an attempt to deal with this problem, the researchers are led to propose the method. The method was suggested, based on the hybridization of KNN and SVM. The fundamental concept is to classify the nearest neighbors to a verification problem and to prepare a close by SVM for the task of separation on neighbor array. Their work experiment was conducted using Dredze dataset and public dataset which shows that the results are approximately improved to 98% but limited to only accuracy as a performance metric.

Sadat M. and Rahmati in [4] suggested a method in their paper "A process for image spam detection using texture feature" where they used the image texture function to identify the spam image. In this study, the co-occurrence gray level matrix (GLCM) was applied as one of the texture characteristics to each image. Then to identify images with feature that each image acquired. The neighbors classifier k-nearest and the Bayesian naïve are used. The properties obtained are 22 attributes, and then the classifiers evaluate the images obtained from Dredze and Image Spam Hunter datasets. The dataset is divided by cross validation methods in to training set and test sets [4]. The result obtained from the classification covering four performance metrics: accuracy, precision, recall and F-measures in their experiment indicate an improvement in this research domain and compare with previous work, there is a substantial reduction in runtime but the study is limited to using only two classifiers.

Kumaresan T. et al. [5] proposed a solution that removes particularly low-level features such as image metadata and histogram features. Due to the extracted features, a SVM classifier is applied with the aid of a function of kernel to detect image spam, the accuracy obtained with the method is 90% but their work is limited because of the time complexity. In this paper, they used multiple image features to build classifiers for image spam. The classifiers used are the combination of SVM and PSO. PSO improves the output by iteratively scanning candidate solutions and also ensure that the particle in the search space are moved. Again, due to its computational complexity, PSO is conveniently applicable only to the dataset that are relatively small as compared to SVM [5].

Authors in [6] suggested an approach combining the properties of spam images with the density of corner points in the images to filter the spam image. The algorithm's simple idea depends on the images proportion in the corner to determine whether it is a spam or not. The researcher presented that most of the technical approaches available for spam filtering are not effective for test messages imbedded into images and have identify this as a major problem hindering the performance of online transactions. The development of the proposed approach was done involving color edge detection, image binarization, and corner point detection. And after the experimental evaluation of the proposed approach, the result show that the detection rate of spam images is 90.5%. The 8-bit RGB mode is used for the analysis. The major point in this experiment is to identify the corner and conduct a statistical analysis and the limitation of this approach is that, it cannot handle crafty spams.

Meghali D. et al. [7] suggested a method for classifying the embedded image as spam or as a legitimate mail. The technique is based on an interpretation of the image containing only one region of text and the dataset used is Dredze dataset, Classification methods are applied in a hybridized manner. Particle Swarm Optimization is combined with Artificial Neural network for selection of features while the classifier for employed for spam classification and separation is Support Vector Machine. The learning ability of filters is the major strength of this method because every filter is different in terms of the data stored and model learned if every user receives different email but limited by complexity. The proposed framework is designed to handle both low level features and further processing of embedded text extraction. Their approach has been contrasted against other approaches and the result shows that AUC used in the proposed system for performance assessment is better than others methods [7].

Many conventional methods for detecting spam emails including the Bayesian method, the rule based system, Heuristic based filter IP blacklist, DNS black and white list holes have been made known[19]. They applied a neural system strategy where neurons were trained and proposed an efficient techniques based on neural network for spam classification component to enhance the exactness, accuracy and F-review. The proposed system is contrasted with SVM and the result indicate that system is doing relatively better. The performance metrics used for the comparison are precision and accuracy. The approach of the plan is introduced to improve the accuracy quotient of the current methods [19]. Approximately 1000 spam terms is included in the report. Due to the average performance of the proposed algorithm, it can be used with other algorithms to improve the spam detection.

Rathi and Pareek in [20] analyzed many methods of data mining for dataset containg 57 attributes with a single target feature in a discreet mode for the purpose of identifying the best approach for email identification and separation. The researchers analyzed the performance of different techniques for the classification operation in this paper. It was confirm that the result showed a success in terms of accuracy when

the process of selecting the features was incorporated during the experiment. It was also noticed that the best classifier for spam mail detection with the accuracy of 99.72% was Random Tree and Random Forest to be the second in performance with an accuracy of 99.52% [20]. Researchers in [24] also focused mainly on spam email classification using machine learning techniques. The research is centered on concepts, actions, efficacy and patterns in spam filtering as well as the common machine learning approaches employed to combat the threat of spam.

III. METHODOLOGY

A. Research Questions

The purpose of this paper is to conduct a survey on spam detection approaches proposed by various researchers. In this study, two research questions were formulated which are:

- What are the major advantages and limitations affecting the performance of the current machine learning techniques?
- Which of the techniques performs better in terms of accuracy, precision, recall and the F-measure each?
- Does difference in dataset affect the performance of a classifier?

B. Research Objectives

And based on the research questions above, three research objectives were formulated.

- The first objective is to review and identify some common limitations of machine learning techniques.
- The second objective is to discover the technique that have the higher performance in terms accuracy precision, recall and F-measures on spam detection in research domain.
- The third objective is to investigate whether differences in dataset affect the classifiers' performance or not.

Publications on spam image-based detection techniques were searched, reviewed and eleven papers were selected in ascending order based on the number of citations in order to achieve the first, second and third objectives. Here, current machine learning techniques for spam detection are reviewed and their advantages and limitations were identified. The second and third objective was achieved by tabulating the performance result of the selected spam image-based detection techniques from the reviewed literature in tabular form and from which the technique with higher performance was identified with concentration on four major performance metrics such as: accuracy, precision, recall and F-measure was identified.

C. Methods

Here we discussed the methods that are used to recognize spam images, these methods are grouped into three distinct classifications including; header base, contest based and OCR based techniques [4]:

Header Based Techniques

Presently, it is common observed that email users always hide the client's header, however, this is the reason why most people cannot see their email header. Therefore, the header is produced along with the content of email. It is usual for e-mail messages to be used as an alternative to either activate display of e-mail or not. The major logic of this technique is to determine the piece of the email course wasted. The email header involves a number of fields that provide an important information margin [2, 4].

Content Based Techniques

These techniques are based on the extraction of features and the analysis of image content. These types of filters are used to examine and analyze the substance and techniques of the image [4]. The technique is geared towards the analysis of the different properties of the image and these characteristics are undesirably represented by the features of the image. It handles attribute and content such as image shape. The email body check for those properties used by the spammers. Email may be in form of image or text or even an image and a text combined. Text-based filtering approaches are often reliant on all forms of information and are reflective of the primary process and common ways to eliminate spam but spammers always seem to engage in a new tactic to trick the detection measures.

OCR based techniques

These techniques are usually applied to extract text embedding in the image using the OCR tool [4]. OCR is an electronic or mechanical representation of validated images that are manually typed, typewritten or content printed of machine encoded text. It is usually apply to turn books and records into electronic files to a modern record keeping model in an institute or to share the file of the site. OCR is able to find and alter the text, check for word and even phrase, store tightly, display or produce a copy free of scanning artifacts and then, apply techniques such as machine interpretation, text mining and speech text [7].

D. Machine Learning Techniques

In this section we provide description of some selected machine learning methods which have been applied to spam email classification and conduct a comparison on the areas of their strength and limitations.

Naïve Bayes

The classification process of this technique is an example of a learning techniques and also a predictive classification technique. It works as a basic probabilistic method which enable us to capture the clarity of the concept in an ethical manner by analyzing the likelihood of the result. It is applied to provide answers to analytical and quantitative problems [25]. Bayesian technique is named after a researcher who suggested the algorithm in person of Thomas Bayes (1702-1761). Classification provides functional learning methods and advanced information and analytical evidence may be combined. Bayesian classification provides a valuable framework for interpreting ad analyzing a variety of learning approaches. It determines the exact possibility for postulation and is resilient to noise in input data. It is a simple probabilistic method that is developed on the Bayes analysis, with valid assumptions which are independent in nature.

Clustering Technique

Clustering works by aggregating pattern classes in to a related group of classes. Clustering belongs to a category of approaches that divides case studies in to clusters

comparatively. This techniques has call the attention of scientific researchers and academics and have been used in various fields of practice. These techniques are unsupervised learning techniques and are used on the dataset of email spam with a true labels. Given that suitable representations are available, a good number of clustering techniques have the ability to classify email spam datasets in either spam or ham clusters. Whissel and Clarke in [26] have shown this in their research paper which was specifically written on email spam clustering.

Support Vector Machine

Support Vector Machines (CSVM) are controlled learning algorithms which have been established to perform better compared to the other learning algorithms aid. SVM is a category of algorithms that are introduced for handling classification and regression problems. SVM has used application while offering solutions of quadratic programming problems which have inequality weaknesses and sequential equality by differentiating different classes through hyper plane. It utilizes full advantage of the boundary [27]. Although the SVM may not be as swift as other classification algorithms, the algorithm draws it advantage from its high accuracy due to its ability to use multidimensional border of the model which is not linear or sequential.

Decision Tree

A Decision Tree (DT) is a classifier that uses a similar pattern with a tree structure. According to authors in [24, 26], decision tree induction is a distinctive method which contributes to information on classification. Decision tree nodes is either a leaf node that specifies the meaning of the intended function (class) or be a decision node that suggests that a certain verification is to be carried out with one branch and a sub tree as subset of the larger tree representing any likely test output. Decision tree learning is a technique that has been effectively used for filtering spam email. The aim of this approach is to produce a model of DT and train the model so as to predict the value of a target variable based on the total number of input variables.

Random Forest (RF)

This is a popular instance of an ensemble learning technique that is suitable for classification of data in to classes [26]. For the first time, random forest was proposed by researcher in [27]. The technique makes a specialized predictions using a tree structure. At the stage of training, some decision trees are created by the writer of the program. These decision trees are then applied for the task of predicting the group; this is done by considering the chosen groups of each tree and the category. These decision trees are then used for the purpose of predicting the group, this is done by taking into consideration the selected groups in each tree and the group with the highest number of votes is taken as an output. Random forest approach is gaining more prominence these days and has been applied in a number of field and literature to solve the analogous problem according to [26].

IV. RESULTS AND DISCUSSION

A summary of the reviewed machine learning techniques is presented in this section from the literature. Table 1. present a tabular form of the summary after achieving the first objective in section D. The details summaries consist of research year, reference number, classification techniques, advantages and the limitation of each technique.

TABLE 1: SUMMARY OF THE CLASSIFICATION TECHNIQUES.

Pub. year	Ref. No	Techniques	Advantage(s)	Limitation(s)
2017	[25]	Naïve Bayes classifier	-Handling of ambiguity by ethically influencing the probability of the results.	-Dependent on Bayesian filtering assumption (that events occurred independently in nature)
2016	[24]	Decision Tree	-Very short training period.	Not flexible for adjustment.
2016	[26]	Random Forests	-Higher performance with lesser classification error -Efficient mechanism during the data lost.	Longer training period
2015	[27]	Support vector machine	Capacity to modeI muItidimensio naI borderIines that are not sequentiaI or straightforward .	Slow classification,
2016	[26]	Clustering technique	- Ability to process encrypted messages, while preserving confidentiality.	-Inability to locate sensitive comparators. (its success depends on its ability to locate sensitive comparators)

While table 2 present the performance of the techniques relative to the dataset used. In order to achieve the second and third objective of this review, the detail summaries consist of publication year, reference no, dataset employed, the techniques, accuracy, precision, recall and F-measures.

TABLE 2: SUMMARY OF THE TECHNIQUES AS COMPARED FROM THE RELATED STUDIES.

Year	Ref. No	Dataset	Techniques	Accu-racy	Precis-ion	Re-call	F-Measure
2015	[1]	DredzeDataset	SVM and PSO	90%	-	-	-
2015	[3]	Spambase	Naïve Bayes	84%	89%	78%	-
2015	[4]	Dredze	KNN	91/41	87/03	99/53	92/86
			Naïve Bayes	75/49	78/98	82/12	80/52
		ISH Dataset	KNN	93/74	97/96	91/01	94/35
			Naïve Bayes	99/19	98/50	98/52	99/25
2013	[20]	Amazon.com	Random Forest	99.52%	-	-	-
			Random Tree	99.72%	-	-	-
2018	[21]	Spam_base	Random Forest	94.2%	94.2%	94.2%	94%
			Naïve Bayes	88.2%	88.5%	88.5%	88.5%
			Multilayer perceptron	93.2%	93.3%	93.2%	93%
			J48	92.3%	92.3%	92.3%	92.3%
2017	[28]	Dredze	Naïve Bayes classifier	98%	-	-	-
2013	[29]	Spambase	Random Forests	93.89%	95.87%	94.10%	-
2016	[30]	Enron	Decision Tree	96%	98%	94%	-
2015	[31]	Spambase	SVM	79.50%	79.02%	68.69%	-
			Naïve Bayes	76.24%	70.59%	72.05%	-
2018	[32]	Spambase	ANN	92.41%	92.40%	92.40	-

As provided in table 1, this study has investigated the strength and limitations of spam email detection techniques and identified handling ambiguity, short training period, high performance, capacity to modeI muItidimensionaI borderIines and capacity to model encrypted messages as the advantages while, limitations are complexity, slow classification, classification error and longer training period and inability to locate sensitive comparators. Also found that Random Tree has the highest percentage of accuracy of 99.72%, therefore it is the best classifier in terms of accuracy and we also discovered that accuracy is the most used performance metric in the literature. Decision tree has the highest precision of 98%, KNN has the best recall with 99/52 while Naïve Bayes is the best in terms of F-measures with 99/25. The investigation also shows that differences in dataset affect the performance of classifiers.

V. CONCLUSION AND FUTURE WORK

There are many machine learning techniques available for detecting these unwanted spams. In spite of the significant progress made in the volume and figure of literature reviewed, there is no machine learning method that has achieve 100% accuracy. Each algorithm only utilizes limited features and properties for classification. Therefore, identifying the best algorithm is an important task as their strengths need to be weighed against their limitations. It was noted that significant progress have been made based on the volume and figure of literature reviewed, hence, more research is required to improve the performance of hybrid system on Artificial immune system and to focus on the availability of well labeled dataset to ensure effective spam filtering. It has been also noted that there is an increasing use of internet and that, the increase in the use and application of internet is relative to the increasing rise of spam image.

REFERENCES

[1] Chopra, Nisha D., and K. P. Gaikwad (2015). "Image and text spam mail filtering." Int. J. Comput. Technol. Electron. Eng (IJCTEE) 5, no. 3.

[2] Ravikumar K, Gandhimathi P. A (2014) Review on Different Spam Detection Approaches.

[3] Renuka, D.K.; Visalakshi, P.; Sankar, T.J.I.J.C.A. Improving E-mail spam classification using ant colony optimization algorithm. Int. J. Comput. Appl. 2015, 2, 22–26.

[4] Sadat Hosseini M, Rahmati M. (2015)A Method for Image Spam Detection Using Texture Features.

[5] Kumaresan, T., Sanjushree, S., Suhasini, K. and Palanisamy, C., (2015). Image spam filtering using support vector machine and particle swarm optimization. Int. J. Comput. Appl, 1, pp.17-21.

[6] Wang, Jianyi, and Kazuki Katagishi (2014) "Image Content-Based" Email Spam Image" Filtering." Journal of Advances in Computer Networks 2, no. 2: 110-114.

[7] Das, Meghali, and Vijay Prasad (2014). "Analysis of an Image Spam in Email Based on Content Analysis." International Journal on Natural Language Computing (IJNLC) 3, no. 3, pp. 129-140.

[8] Liu, Tzong-Jye, Cheng-Nan Wu, Chia-Lin Lee, and Ching-Wen Chen (2014). "A self-adaptable image spam filtering system." Journal of the Chinese Institute of Engineers 37, no. 4, pp. 517-528.

[9] Foqaha, Mohammed Awad1and Monir.(2016) "EMAIL SPAM CLASSIFICATION USING HYBRID APPROACH OF RBF NEURAL NETWORK AND PARTICLE SWARM OPTIMIZATION.".

[10]. D.Sasikala, R.Roshiniya, Sarishnaratnakaran, Tapati Deb," Texture Analysis Of Plaque In Carotid Artery" International Journal Of Innovations In Scientificand Engineering Research(Ijiser), Vol 4 Issue 2 Feb 2017, Pp.66-70.

[11] J. M. Carmona-cejudo, G. Castillo, M. Baena-garcía, and R. Morales-bueno, "Knowledge-Based Systems A comparative study on feature selection and adaptive strategies for email foldering using the ABC-DynF framework," vol. 46, pp. 81–94, 2013.

[12] R. Group, "Email Statistics Report , 2016-2020," vol. 44, no. 0, pp. 0–3, 2016.

[13] A. Sharaff, N. . Nagwani, and A. Dhadse, "Comparative Study of Classification Algorithms for Spam Email Detection," Springer, no. January, 2016.

[14] A. F. Yasin, "Spam Reduction by using E-mail History and Authentication (SREHA),"Int. J. Inf. Technol. Comput. Sci., vol. Vol.8, no. No.7, p. pp.17-22, 2016.

[15] M. Iqbal, M. A. Malik, A. Mushtaq, and K. Faisal, "Study on the Effectiveness of Spam Detection Technologies,"mInt. J. Inf. Technol. Comput. Sci., vol. Vol.8, no. 1, pp. 11–21, 2016.

[16] S. M. Abdulhamid et al., "A Review on Mobile SMS Spam Filtering Techniques," IEEE Access, 2017.

[17] M. Zavvar, M. Rezaei, and S. Garavand, "Email Spam Detection Using Combination of Particle Swarm Optimization and Artificial Neural Network and Support Vector Machine," Int. J. Mod. Educ. Comput. Sci., vol. 7, no. July, pp. 68–74, 2016.

[18] P. Parveen and P. G. Halse, "Spam Mail Detection using Classification," vol. 5, no. 6, pp. 347–349, 2016.

[19] R. Sharma and G. Kaur, "E-Mail Spam Detection Using SVM and RBF," no. April, pp. 57–63, 2016.

[20] M. Rathi and V. Pareek, "Spam Mail Detection through Data Mining – A Comparative Performance Analysis," Int. J. Mod. Educ. Comput. Sci., vol. 5, no. December, pp. 31–39, 2013.

[21] S. M. Abdulhamid, M. Shuaib, O. Osho, I Ismaila, J. K. Alhassan,"Comparative Analysis of Classification Algorithms for Email Spam Detection", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.1, pp.60-67, 2018.DOI: 10.5815/ijcnis.2018.01.07

[22] M. Awad, M. Foqaha, Email spam classification using hybrid approach of RBF neural network and particle swarm optimization, Int. J. Netw. Secur. Appl. 8 (4) (2016).

[23] D.M. Fonseca, O.H. Fazzion, E. Cunha, I. Las-Casas, P.D. Guedes, W. Meira,

M. Chaves, Measuring characterizing, and avoiding spam traffic costs, IEEE Int. Comp. 99 (2016).

[24] A. Bhowmick, S.M. Hazarika, Machine Learning for E-Mail Spam Filtering: Review, Techniques and Trends, arXiv:1606.01042v1 [cs.LG] 3 Jun 2016, 2016, pp. 1–27.

[25] Available at, Mail Server Solution, 2017, http://telco-soft.in/mailserver.php.

[26] S. Dipika, D. Kanchan, Spam e-mails filtering techniques, Int. J. Tech. Res. Appl. 4 (6) (2016) 7–11.

[27] Z.S. Torabi, M.H. Nadimi-Shahraki, A. Nabiollahi, Efficient support vector machines for spam detection: a survey. (IJCSIS), Int. J. Comput. Sci. Inf. Secur. 13 (1) (2015) 11–28.

[28] Al-Duwairi, Basheer, Ismail Khater, and Omar Al-Jarrah (2012). "Detecting image spam using image texture features." International Journal for Information Security Research (IJISR) 2, no. 3/4, pp. 344-35

[29] Sharma, S.; Arora, A. Adaptive approach for spam detection. Int. J. Comput. Sci. Issues 2013, 10, 23.

[30] Khan, Z.; Qamar, U. Text Mining Approach to Detect Spam in Emails. In Proceedings of the International Conference on Innovations in Intelligent Systems and Computing Technologies (ICIISCT2016), Las Piñas, Philippines, 24–26 February 2016; p. 45.

[31] Karthika, R.; Visalakshi, P.J.W.T.C. A hybrid ACO based feature selection method for email spam classification. WSEAS Trans. Comput. 2015, 14, 171–177.

[32] Bassiouni, M.; Ali, M.; El-Dahshan, E.A. Ham and Spam E-Mails Classification Using Machine Learning Techniques. J. Appl. Secur. Res. 2018, 13, 315–331.

A REVIEW OF DNA CRYPTOGRAHIC APPROACHES

Mohammed Awwal Iliyasu
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria.
awwaliliyasu@gmail.com

Opeyemi Aderiike Abisoye
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria.
o.abisoye@futminna.edu.ng

Sulaimon Adebayo Bashir
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria.
bashirsulaimon@futminna.edu.ng

Joseph Adebayo Ojeniyi
Department of Cyber Security,
Federal University of Technology,
Minna, Nigeria.
ojeniyija@futminna.edu.ng

***Abstract*— Cryptography is described as the encryption analysis of data or secret data writing using logical and mathematical data protection principles. It is an information technology for banking, medical systems, transportation and other Internet of things applications. Cryptography has become more important, and it is subjected to growing security concerns. Each system is built with its own strength in cryptography; symmetric encryption provides an economical data protection solution without compromise but it is important to share or distribute the secret key during encryption and decryption process. In comparison, the asymmetric encryption addresses the issue of secret key distribution; however, the stand-alone technique is slow and needs more computing resources than the symmetric encryption approach. In this context, a study of papers relating to DNA cryptographic approaches are presented and the research was centered from 2015 to 2020. The primary sources of information are Science Direct and Research Gate publication platforms. The existing shortcomings of DNA cryptographic approaches were established and analysis was performed on the most frequently used encryption technique based on the literature. The significant findings of this research reviewed that DNA digital coding is the most adopted cryptographic technique used to improve information security and the most common limitations of the DNA cryptographic approaches are high time complexity and algorithm complexity which is possible to infer from the literature.**

Keywords—: Cryptography, DNA cryptography, One Time Pad, DNA Cryptographic approaches, DNA limitations.

I. CRYPTOGRAPHY

[1], [2] defined Cryptography as the study for encoding and decoding of data using logical and mathematical operations to secure information. This technique has evolved rapidly in providing security to computing technology applications such as medical, financial, transportation services among other Internet of Things (IoTs) applications. Cryptography encryption is mainly intended to protect sensitive data from unwanted changes. To guarantee a safe communication, it requires encrypting the data so that if an eavesdropper successfully intercepts an encrypted message, it will not be useful because an unauthorized person cannot possibly decrypt an encrypted message [3].

Auguste Kerckhoff formulated the first cryptographic engineering principle in 1883 [4]. He asserted that encryption technique maybe known publicly but decryption of encrypted information requires knowledge of the encryption key. This key is paramount at both encoding and decoding processes respectively, and without the key, encrypting or decrypting information is impossible even if the algorithm for the encryption is known. In recent years, the encryption framework is classified generally into symmetric and asymmetric algorithms based on the key roles for each algorithm. The Symmetric Encryption Algorithm (SEA), also known as Secret Key Encryption (SKE) require the sender and recipient of an information to be in possession of a unique private key for encrypting and decrypting of information. The Asymmetric Encryption Algorithm (AES) is also known as Public Key Encryption (PKE), it requires the sender and recipient of an information to be in custody of two keys (public and private key) before encryption and decryption operations can be performed successfully on the desired information. The two encryption techniques have ensured the securing of information against adversaries and vulnerabilities on insecure communication channels [4].

Cryptanalysis is the process of decoding information from encoded or concealed format to understandable form without any slight concept on how the information is transformed from plaintext to ciphertext. Encryption is the stages involved in encoding plaintext information into ciphertext while decryption is the reversed order of encryption process where encrypted information is transformed back to plaintext. Cryptography is mainly concerned with four objectives: confidentiality, integrity, non-repudiation and authentication of an information. The information preventive measures and rules that meet one or more of the objectives are known as Cryptosystems.

The traditional Cryptography security is centered on complex mathematical problems which uses mathematical theories. In advance cryptography, algorithms that are mainly accepted as substitutes of the security techniques are the vocal, elliptic, quantum and DNA encryption algorithms. Elliptic algorithms are techniques for portable devices that have limited processing ability, it uses simple algebra and relatively small ciphers. The quantum cryptography is a technique for creating and distributing of private keys. These techniques are yet vulnerable to the Man-in-the-Middle and DoS attack. The traditional cryptographic methods provide mathematical theory models that were exposed to cipher attacks, the embracing of DNA computing in cryptographic approaches has yielded the possibility of securing communication channels on modern technologies and raises new confidence for unbreakable algorithms [5].

II. DNA CRYPTOGRAPHY

DNA is an acronym for Deoxyribose Nucleic Acid (DNA) which is a hereditary property for the entire living organisms ranging from very tiny viruses to complex human beings. It is an information agent that transports information for all life forms. The DNA consists of double helical structure with 2 strands working in antiparallel form. DNA is a lengthy polymer of small units called nucleotides. The nucleotides consist of three components each; namely: nitrogenous base, five carbon sugar and a phosphate group. The nucleotides are four types and they depend on the nitrogenous type. The four different bases are A, C, T, G called Adenine, Cytosine, Thymine and Guanine respectively. The DNA saves very complex and large volume of information for an organism with the mixture of only these four letters A, C, T and G. The bases form the structures of DNA strands through formation of hydrogen bonds with each other to keep the two strands unbroken. A and T, C and G forms hydrogen bonds with one another [6].

[7] asserted that DNA cryptography is a new rapidly evolving approach within the cryptographic domain and it focused on the DNA sequences. The notion of DNA cryptography is inspired by the DNA molecule which has the ability to store, process and transmit information. It operates on the DNA computing principle which uses 4 bases to conduct computation [6], i.e. Adenine (A), Guanine (G), Cytosine (C), and Thymine (T).

III. DNA CRYPTOGRAPHIC TECHNIQUES

The essential techniques for DNA Encryption are DNA digital coding and Polymerase Chain Reaction (PCR) Amplification. These techniques have been leveraged on by many researchers while other encryption techniques are also used for encryption operations. Below is a brief description of the DNA encryption techniques:

A. DNA Digital Coding

DNA Digital Coding is a mapping technique which uses DNA bases (ACTG) on the notion of binary digital coding to encrypt and decrypt information. The technique plays a vital role in encrypting and decrypting information, it is used to encode information using the binary digits 0 and 1. DNA Digital Coding is basically deployed on four nucleotide bases A, C, T, G [9], [5]. This technology denotes the bases A, C, T, G as 00, 01, 10, 11 and also provide means for swapping the binary values with the bases. This coding procedure forms the basis of the encryption algorithms for DNA Digital coding approaches. The computation of DNA can be accomplished in two forms: through biological operations using human DNA and the other form involves simulation using Digital DNA and Pseudo DNA. DNA Cryptography is manufactured on the basis of DNA computations for encrypting and decrypting information which has been accepted and exploited in many research areas for both Symmetric and Asymmetric encryption technique. The technique has wider coverage due to the bio-computations and security nature of the algorithm [8].

B. Polymerase Chain Reaction

Polymerase Chain Reaction (PCR) amplification is described by [5] as a molecular biological technique of DNA Amplification which is based on the concept of Watson Crick Complementary Model. Two different primers are used for the encoding of information in this technique. Primers are the tiny DNA fragments. The key which is used for PCR amplification is generated from two primer pairs. The plaintext which requires privacy is positioned between the primer pairs to obtain the new encoded sequence. The amplification of the encoded sequence is more once the PCR primer pairs are unknown. The accuracy of the primers of the sequence is needed in this technology to prevent generating different result due to difference in primers lengths as such the actual plaintext can't be ascertained. The biological PCR operation stages are:

First stage: PCR Amplification begins with Denaturation process, a double stranded molecule is divided into two single stranded DNA. For several minute a sample is heated for about 94 to 96 degree Celsius so as to denaturalize (separate) double strand into two single strands.

Second Stage: This stage is for processing of Primer Annealing, the temperature is cooled between 50 to 65 degree Celsius in minute(s) and the primers respective complementary sequences are attached. The essence of the primers is to amplify the DNA surroundings.

Third Stage: This is Primer Extension stage, in this stage temperature elevated to 72 degree Celsius for minute(s). In this phase, the polymerase enzyme augments the shorter strands with nucleotides base on the original DNA strand. The DNA strands between primers are amplified.

DNA-based cryptography is a research method that employs biological structure to encode data. Scientists are rapidly doing research in this area which is based on using DNA computing to depict binary information in various forms. DNA encryption method involves the use of DNA sequence to convert plaintext into ciphertext. [7] has acknowledged only four methods of DNA encryption and [5] emphasized that despite PCR and DNA digital coding techniques are the most vital DNA Cryptographic techniques, there are other four DNA Encryption Techniques, which are:

C. DNA Random One Time Pad (OTP) Based

This technique operates using a randomly, ordered and unique sequence to implement a one-time pad (OTP), and once the OTP is used to generate a ciphertext, it can't be use again. This method increases information security. In this notion, the plaintext size is equivalent to OTP size [5]. DNA OTP scheme is used often to transform short plaintext or part of a plaintext message to ciphertext. The plaintext is substituted using a random and special codebook. Despite the hardware limitations on modern computers, this approach is applicable to short messages. For large size of messages, it uses DNA mapping for complexity and high execution time [10].

D. DNA Chip Based

Microarray is referred to a DNA chip, this DNA chip is designed with nucleic acid and electronic circuit and it's made of semiconductor. This technology depicts outstanding evolvement in DNA cryptography. A DNA-chip is used to store, process and uphold a high volume of genome and other biological information [6], [5]. Information is encoded using biochemical processes, the main setback of this technique is that any environmental change can result to physical factor shift which often yield negative outcome [10].

E. DNA Steganography

The word steganography originates from a Greek word "stegos" implies "cover" and "grafia" signifies "writing", defining it as "covered writing" [11]. DNA Steganography is a method of encoding messages inside digital media such as a photograph, audio, or a video, to preserve huge volumes of information, although data can get lost as a result of sudden changes in an environment [4], [10]. The aim of steganography is to conceal secret information inside a digital media so that only the intended recipient can access the information. This technique doesn't change the information structure, but it will conceal the information inside a digital media so than only the intended recipient can access the information [4].

F. DNA Fragmentation

DNA fragmentation is an approach that uses DNA sequence to build libraries. This technique segments the DNA sequence into bits. Often encryption algorithms uses DNA fragmentation as a second security layer and it is also applied in key encryption [10].

IV. DNA CRYPTOGRAPHIC OPERATIONS

Most biological operations can be operated on DNA molecules to help in solving mathematical and complex computational hitches. The most frequently used arithmetic and logical operations implemented on DNA are as follows.

A. Arithmetic Operations

The most basic arithmetic operations that can be imposed on DNA nucleotides as stated by [9] are:

1) Addition Operation: This operation performed addition on DNA nucleotides based on the traditional binary addition rules. For instance, addition of two binary numbers 10 and 11 will result to 11 binary digits. Furthermore, the four DNA nucleotide bases A, T, C and G are depicted as 00, 01, 10 and 11 respectively and this can be deduced that addition of C and G, will result to T.

2) Subtraction Operation: This operation involved subtraction on DNA nucleotides based on the traditional binary subtraction rules. For example, if 01 is subtracted from 11 the result is 10. Therefore, this can be deduced that subtraction of T from G, will result to C.

B. Logical Operations

The various logical operations that can be applied on DNA sequences are:

1) NOT Operation: This operation is used for inverting DNA sequences. It's referred to as an inverter or negation operation and it's among the simplest DNA-based logic operation. This operation required the supply of a single input while the output is the corresponding complimentary of the sequence. The output will result to true if the input supplied is false and the base combination received or supplied are the representative of true sequence. DNAs are provided to abolish any single stranded sequence. Once a double stranded sequence is detected from the input unit then the result is true, else the result is false.

2) OR Operation: In OR operation, the result is true if at least one of the input provided is true. DNA is used to terminate any single stranded sequence but once a double stranded sequence is detected then the result will be false.

3) AND Operation: The AND operation will result to true if both inputs are true. DNA will put an end to any single stranded sequence in the combination, also if double stranded sequence is noticed, it will lead to true and else it's going to be false.

4) XOR Operation: The XOR operation provides true if and only if one of the input of the sequence is true. In binary, XOR is described as true if the input values are opposite. DNA based XOR logical operation is the simplest method because no base sequence is required or provided to the XOR operation. Opposite input sequences are termed "complementary" and will blend together to form a double stranded sequence. Once the inputs are not opposite, it will lead the sequences not to bind with each other and DNA will terminate the two input sequences.

5) XNOR Operation: XNOR operation evaluates true if the two inputs are the same, it is produced through application of NOT operation on the inputs result of the XOR operation. This operation is like the earlier logical operations, the result is true in the presence of a double stranded sequence while false in the absence of a double stranded sequence.

6) NAND Operation: The NAND operation is used to produce a true result if the inputs (i.e. two or more input) are not true. This operation is similar to the OR operation as depicted above, but the base sequence comprises of the sequence representing the true value somewhat than false. One of the inputs have to be false before it can form a double stranded sequence. The DNA will destroy any single stranded sequence in the combination if a double stranded sequence is observed, the result will be true otherwise the result will be false.

7) NOR Operation: Finally, the NOR operation produces true result when both inputs are false. This operation is implemented through application of NOT operation to the output of the OR logical operation.

V. METHODOLOGY

This study aim to provide a review of DNA cryptographic approaches proposed by various researchers, and the research was centered on the recent literatures. Two research questions were formulated in this study, these are: What are some of the major and most frequent limitation in DNA cryptographic approaches? 2. Which of the DNA encryption technique is proposed most frequent in recent researches? Three research objectives were formulated based on this research questions. The first objective is to review the most recent DNA cryptographic approaches. The second objective is to identify some common limitations of DNA cryptographic approaches. The third objective is to discover the most commonly used encryption method in DNA cryptography research domain. To achieve the first and second objectives, 18 publications on DNA cryptographic approaches were reviewed from 2015 to 2020. The Keyword "DNA cryptographic approaches" and "DNA cryptographic techniques" were searched in Science Direct and Research Gate publication sources (platforms). 36 papers related to DNA cryptographic approaches where found from both sources (platforms) within 2015 to 2020 and eighteen papers were selected randomly. In this research, the most recently proposed DNA cryptographic approaches are reviewed and their limitations were identified. The third objective was accomplished through analyzing the encryption techniques of the selected papers which are derived in tabular form. After tabulation, the most common techniques used are

identified using a chart based on the selected papers reviewed and the result is displayed using a chart in section VI.

A. DNA Cryptographic Approaches

A new DNA-based encryption technique was proposed by [12]. The system combined traditional cryptography and modern methods to improve data security. The plaintext is initially converted into ASCII value, followed by binary strings. The binary strings are also translated into hexadecimal values and a 128-bit key is generated simultaneously with MD5 algorithm. The key is translated into a 32-character hexa-decimal string which is mapped to 16 dynamic values. With support of a mapping table, the binary values are encoded. After encoding, certain mathematical and logical operations occur. For data transmission, an unreliable transmission channel is used for the experiment. It is a very fast and effective technique, the algorithm is implemented on Java. This algorithm does not provide support for multilevel applications.

A new technology for safe transmission of data was developed [13] using XOR operation, One Time Pad (OTP) and DNA cryptography. Here, the OTP technique is used with an appropriate method that has certain specification. Between the OTP and the binary form, XOR operation will be applied. By denoting 00, 01, 10 and 11 for A, T, C and G respectively, then binary numbers are converted into a DNA sequence. After complementing DNA bases, the DNA sequence is reversed from right to left. Then the result of the encrypted data is send to the receiver. This algorithm offers 3 protection levels, i.e. Exclusive OR, OTP and a DNA complementary rule. Further-more, the method is very straightforward and highly safe because it is very difficult for an attacker to guess the randomly generated OTP. Since there are other prerequisite-sites, the system is not so easy to use, as users must take care of the prerequisites before choosing the OTP.

Cloud computing is becoming common due to its features, these includes economic accessibility, sharing and ease of use. However, one of the key issues is the protection offered by cloud data. [14] proposed a new DNA encryption method for enhancing cloud data security. A Symmetric Key is used for the encryption algorithm. The plaintext is initially encrypted and then translated into binary text using a key. DNA sequences are selected and converted to the appropriate cipher for the DNA base pair. Although it looks simple, the algorithm is secure but it may be vulnerable to brute force attack.

[15] presented a method which provides a safe data transmission medium using symmetric algorithm of DNA cryptography. Initially, the input data is converted to ASCII value and then it is again converted into its binary equivalent bits. This now transforms the binary value into DNA code. The resultant DNA code is assigned randomly to the ASCII code based on a private key. In conclusion, the information is encoded with the DNA code and a private key is used to conduct clinical permutation. The implementation of the system is on Java programming and is known as a modern technique for symmetric encryption. DNA chromosomes are to be used with a deep algorithm analysis during data transmission. Conclusively, this method em-ploys an encoding system more efficiently than traditional cryptographic techniques. This method can be adopted to enhance the wireless network security process. The use of DNA chromosome raises the total expense of the algorithm's implementation.

A DNA cryptographic algorithm was proposed based on one-way public key technique. The keys are obtained using ODN mixture and solid mixture for PkB and PkA respectively, denoted as public keys A and B. The plaintext is stored using one public key in a DNA sequence. In addition, both the DNA synthesizer and the remaining public key are synthesized and linked. PCR amplification is done using a coded sequence to decipher the DNA content. It is a highly safety asymmetric system, but it is very costly to deploy [16].

A modified Shamir Secret Algorithm, DNA based encryption and decryption technique was proposed by the researcher [17] which involved a group rather than a single user in the recipient end. The algorithm includes some added stability. In this technique, all clients have to be involved in the decryption process before the secrete message can be decoded. To translate the message into ASCII values, mathematical computations are performed. The ASCII values are then modified to form DNA bases. The message is sent to the entire clients involved via a group platform, then the message is decrypted with DNA encoding to improve message transmission security for multicast applications. Python and Java can be used to implement the proposed protocols and the method may be used in future in trust-based image encryption. The method is only suitable and also appropriate for one party. Furthermore the message cannot be decrypted if any client is absent from the group.

[18] proposed a technique to improve data hiding security with double sequences of DNA. The main concept behind the built framework is that secret message should be encrypted to ensure protection and robustness. The encryption takes place in two steps, the DNA reference sequence covers the encrypted message. Generally, a new data encryption algorithm which focused on DNA sequences was recommended. Hiding of data with repeated characters reduces the alteration rate of the encryption algorithm. After studying the security measures of this algorithm, the attacker can find it hard to identify the private message but yet if the intruder somehow succeeded in accessing the transmitted secret message then the message can be broken.

A new DNA algorithm technique has been proposed for encryption [19]. This encryption technique combined the XOR operations with the symmetric key exchange. The algorithm is very simple and efficient, where plaintext messages are encrypted to DNA cipher. The message will be reviewed at the end of the recipient to increase the security. Sender uses the symmetric key method to encrypt plaintext into a DNA sequence. The message is then sent via various insecure channels such as the Internet to the recipient. At the recipient unit, cipher text is obtained by decrypting the message through the means of the DNA. DNA hybridization principles and matrix computation are performed to reduce the complexity of the running time. DNA sequences have the ability to store large volume of messages in solid form, which is one of these algorithms' key advantages. Application of this approach is extremely uneconomical.

DNA computer-based cryptography algorithm is proposed for encryption and decryption of plaintext message [20]. The algorithm consists of two stages, namely: encryption and decryption. In the first stage, data is converted and then sends to the receiver in an appropriate ciphertext form. The code is deciphered to the original data at the receiver end. The plaintext is provided through PS 2 keyboard to the Field Programmable Gate Array (FPGA). The message is

interpreted with FPGA as codes values in ASCII form. Then a table of codons given by the researcher is used to convert the ASCII values. For encryption of codon, Vigenere cipher processing method is used. The algorithm contributes a notion of a symmetrical key for double layer security. The main distribution is not mentioned here, which means that the algorithm might have a hectic problem.

[21] proposed a unique procedure for the production of ciphertext and a new key generation method. There are two rounds in the key generation process. An intermediate ciphertext is produce using traditional cryptographic technique and the intermediate cipher is converted into the DNA cipher text finally. The approach misled an attack with an invented false DNA sequence. The algorithm increases time and space complexities unreasonably because the application requires a single security layer.

In [22], a proposed biotic pseudo DNA encryption system, for splicing, a device is used in the technique to improve encryption algorithm security. A random technique is used to generate the key of the algorithm, which increases its degree of uncertainty, making it difficult to decipher the resulting ciphertext. The method is robust and analysis demonstrates that the method is more secured from common ciphertext attacks. High-tech bio-computing labs is required to implement this algorithm.

[23] have proposed a new approach for developing a hybrid DNA encryption technique. The technique consists of traditional encryption of DNA and Elliptic Curve Cryptography (ECC). The plaintext is first translated to ASCII and then to binary. A DNA nucleotide is derived from publicly available sender-and-receiver sequences. The DNA encoding scheme transforms these bases into binary form. Many pairs of binary numbers are generated, all of which are combined to produce a long binary number. Encoding is achieved through several tables provided by the researcher. The Koblitz method is used as an elliptical curve points for converting the decimal numbers. With the help of the ECC encryption these points are again encrypted at another elliptical curve point. The encrypted points are ciphertext points sent to the receiver. This hybrid approach of DNA ECC is safer than the existing techniques of DNA encryption. This has a limited key size and two layers of protection simultaneously. On FPGA-based embedding framework, the method proposed can be achieved. Due to small key size, the algorithm may not be secured much in terms of brute force attack.

[24] proposed a modern and secure encryption algorithm based on DNA which uses big data. An unauthorized person can access the message(s) ciphertext in this system without it being necessary that no one can read or understand this cipher. Using big data, this algorithm is used to encrypt a great deal of data. The encryption process employs DNA encoding table and PHP language in this system. This algorithm solved important data problems and the study of big data.

[25] introduced a new cryptographic technique system that focus on encrypting client-side data until they are processed on the cloud. This is a symmetric key cryptography scheme that uses cryptography based on DNA. In addition to presenting the detailed nature of this approach and contrasting it with the existing symmetric-key algorithms (DNA, AES, DES, and Blowfish), the experimental results show that this method leaves behind the conventional algorithms based on ciphertext size, encryption time, and transmission. This new method is therefore much more effective, and performs better.

[26] proposed cryptography based on DNA, which uses hamming code and a block cipher to protect a key. Its critical symmetric cryptography, used to refine a technique based on DNA. The maximum-length matching technique was also developed in this technique to protect against various attacks.

[27] proposed a scheme where ECC was given the DNA mapping technique. In this system the DNA code is random, and alphabets are distributed with non-repetitive subsections. These alphabets are then used at the two ends for encoding and decoding. This system was successfully used in the internet of things apps and used in real-time but not reliable due to algorithm complexity.

[28] suggested a DNAA mapping technique using Elliptic Curve Cryptography. This technique adopted random and non - repetitive allotted of subsections to alpha-bets. At both encryption an decryption end, the alphabets are used for encryption and decryption of information. This method has been deployed and used effectively in real - time internet of things devices.

[29] proposed a form of encryption that has two rounds. This scheme is the same as the latest technique called the algorithm Data Encryption Standard (DES). In this step, the plaintext is encoded using two keys. These two keys consist of the Elliptic Curve Cryptography (ECC), and the Gaussian Kernel Function (GKF) and another key is generated on the second characters replicated in the first key based on random injective mapping. Finally, in the second DNA sequence, the encryption message arbitrarily hides, based on GKF numbers.

VI. RESULT AND DISCUSSION

After achieving the first objective in the previous section, a summary of the reviewed DNA cryptographic approaches are presented in this section. Table 1 present a tabular form of the summary. The detailed summaries consist of research year, algorithm used for the approach, cryptographic method, DNA encryption technique and the limitation of the research.

Table 1: Summary of the DNA Cryptographic Approaches

S/N	Publication year	Algorithm used	Cryptographic method	Technique used	Limitations
1	2016	DNA based, MD5 algorithm [12]	Symmetric cryptography	DNA Digital coding	Lack support for multi-level application
2	2016	XOR, OTP, DNA complimentary rule [13]	Symmetric cryptography	OTP based	Not flexible to implement due to algorithm complexity

3	2016	DNA encryption [14]	Symmetric cryptography	DNA Digital coding	Vulnerable to brute force attack
4	2016	DNA encryption [15]	Symmetric cryptography	DNA Digital coding	High implementation cost
5	2015	DNA encryption [16]	Symmetric cryptography	PCR Amplication	High implementation cost
6	2016	DNA encryption [17]	Symmetric cryptography	DNA Digital coding	Message can't be decrypted
7	2015	DNA encryption [18]	Symmetric cryptography	DNA Steganography	Not secured once a third party is aware of the message medium
8	2015	XOR, DNA Hybridization, Matrix computation [19]	Symmetric cryptography	DNA Digital coding	High execution time, algorithm complexity
9	2016	DNA based, Vigenere [20]	Symmetric cryptography	DNA Digital coding	Inappropriate documentation for implementation, algorithm complexity
10	2017	Traditional algorithm, DNA based [21]	Symmetric cryptography	DNA Digital coding	High time and space complexity
11	2016	OTP. DNA based [22]	Symmetric cryptography	Pseudo DNA	Required high tech bio-computing for implementation
12	2015	Traditional encryption, DNA ECC [23]	Asymmetric cryptography	DNA Digital coding	Vulnerable to brute force attack
13	2015	DNA based [24]	Symmetric key cryptography	DNA digital coding	High time complexity
14	2018	DNA based [25]	symmetric-key cryptography	Binary DNA	High time complexity
15	2017	DNA based Cryptography [26]	Symmetric key cryptography	Hamming code and a block cipher mechanism	High time complexity
16	2017	DNA based cryptograph	Symmetric key cryptorapy	DNA Digital coding	Algorithm complexity
17	2018	DNA - Based ECC for IoT Devices [28]	Asymmetric key cryptography	DNA Elliptic curve cryptography (ECC)	High time complexity
18	2019	Artificial DNA sequences based on Gaussian kernel function(GKF) [29]	Asymmetric key cryptography	ECC, and Gaussian kernel function (GKF) cryptography	High time complexity

Figure 1 present the DNA cryptographic approaches limitations and their frequency.

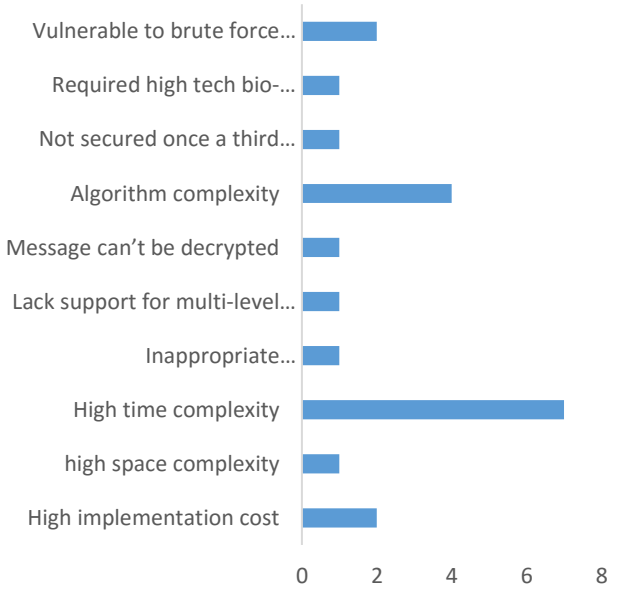


Figure 1: Summary of reviewed DNA cryptographic approaches limitations and their frequency

As depicted in figure 1, this study has investigated and identified high time complexity and algorithm complexity as the most common limitations of DNA cryptographic approaches. Other limitations are high implementation cost, unreasonable expansion of encrypted messages, Lack of support for multi-level application, algorithm vulnerable to brute force attack, and so on.

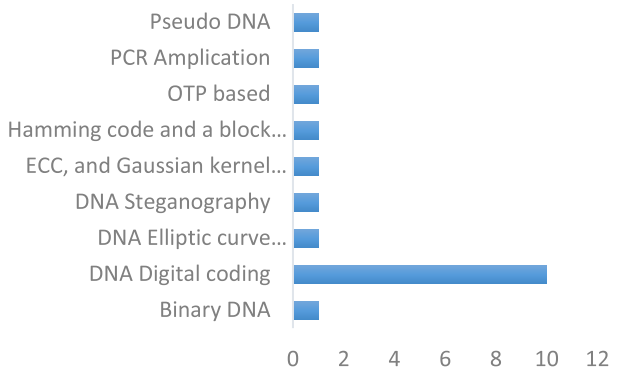


Figure 2: Summary of reviewed DNA Cryptographic techniques and their frequency

Based on Figure 1, it can be concluded that the DNA cryptographic approaches are mostly implemented in DNA Digital coding encryption technique and the technique is implemented often with OTP encryption technique and/or XOR operation.

VII. CONCLUSION

Most articles on DNA OTP based encryption technique did not present security analysis or mathematical proven methods for the encryption approaches. The researchers mostly demonstrated the proposed system model and developed web page for testing the approaches. Notwithstanding, our literature reveals that high time complexity and algorithm complexity are the major limitations of DNA encryption approaches, as presented in section VI. This study will serve as a reference for further research in future. Therefore, researchers can exploit this paper to improve more on the current DNA cryptographic limitations.

REFERENCES

[1] M. A. Saleh and H. Hashim, "HYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OF," vol. 3, no. 3, pp. 279–319, 2020.

[2] A. Sharma, "Security and Information Hiding based on DNA Steganography," vol. 5, no. 3, pp. 827–832, 2016.

[3] M. Rathi, S. Bhaskare, T. Kale, N. Shah, and N. Vaswani, "Data Security Using DNA Cryptography," vol. 5, no. 10, pp. 123–129, 2016.

[4] M. S. Taha, M. Shafry, and M. Rahim, "Combination of Steganography and Cryptography : A short Survey Combination of Steganography and Cryptography : A short Survey," 2019, doi: 10.1088/1757-899X/518/5/052003.

[5] M. A. Athitha, M. A. Akshatha, and B. Vandana, "A Review on DNA Based Cryptographic Techniques," vol. 3, no. 11, pp. 2819–2824, 2014.

[6] B. Anam, W. Yorkshire, W. Yorkshire, W. Yorkshire, and W. Yorkshire, "Review on the Advancements of DNA Cryptography."

[7] Y. Niu, K. Zhao, X. Zhang, and G. Cui, "Review on DNA Cryptography," in Communications in Computer and Information Science, 2020, vol. 1160 CCIS, pp. 134–148, doi: 10.1007/978-981-15-3415-7_11.

[8] S. C. Sukumaran and M. Mohammed, "DNA Cryptography for Secure Data Storage in Cloud," vol. 20, no. 3, pp. 447–454, 2018, doi: 10.6633/IJNS.201805.20(3).06.

[9] A. Hazra, S. Ghosh, and S. Jash, "A Review on DNA Based Cryptographic Techniques," vol. 20, no. 6, pp. 1093–1104, 2018, doi: 10.6633/IJNS.201811.

[10] P. Dixit, M. C. Trivedi, A. K. Gupta, and V. K. Yadav, "Video Steganography using Concept of DNA Sequence and Index Compression Technique," no. 5, pp. 408–417, 2019.

[11] G. Hamed, M. Marey, S. A. El-sayed, and M. F. Tolba, "Comparative Study for Various DNA Based Steganography Techniques with the Essential Conclusions about the Future Research," no. December, 2016, doi: 10.1109/ICCES.2016.7822003.

[12] L. Gehlot, R. Shinde, "A survey on DNA-based cryptography," International Journal of Advanced Research in Computer Engineering and Technology (IJARCET'16), vol. 5, no. 1, pp. 107-110, 2016.

[13] N. Gulati, S. Kalyani, "Pseudo DNA cryptography technique using OTP key for secure data transfer," International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 5657-5663, 2016.

[14] A. Kumar, V. K. Pant, "DNA cryptography a new approach to secure cloud data," International Jour- nal ofScientific and Engineering Research, vol. 7, no. 6, pp. 890-895, 2016.

[15] T. Mahalaxmi, B. B. Raj, J. F. Vijay, "Secure data transfer through DNA cryptography using symmet- ric algorithm," International Journal of Computer Applications, vol. 133, no. 2, pp. 19-23, 2016.

[16] A. Okamoto, I. Saito, K. Tanaka, "Public key system using DNA as a one way function for distribution," Biosystem, vol. 81, no. 1, pp. 25-29, 2015.

[17] T. Purusothaman, K. Saravanan, "DNA-based secret sharing algorithm for multicast group," Asian Jour- nal of Information Technology, vol. 15, no. 15, pp. 2699-2701, 2016.

[18] H. M. Abdelkader, F. E. Ibrahim, M. I. Moussa, "Enhancing the security of data hid- ing using double DNA sequences," in Industry Academia Collaboration Conference (IAC'15), 2015. (https://www.researchgate.net/publication/278028006_Enhancing_the_Security_of_Data_Hiding_Using_Double_DNA_Sequences).

[19] T. Anwar, A. Kumar, S. Paul, "DNA cryptography based on symmetric key exchange," International Journal of Engineering and Technology (IJET'15), vol. 7, no. 3, pp. 938-950, 2015.

[20] M. Bhavithara, A. P. Bhrintha, A. Kamaraj, "DNA- based encryption and decryption using FPGA," In- ternational Journal of Current Research and Modern Education (IJCRME'16), pp. 89-94, 2016.

[21] K. Chiranjeevi, S. L. Kumar, R. Paspula, "Hidden data transmission with variable DNA technology," International Journal ofElectronics and Information Engineering, vol. 7, pp. 41-52, 2017.

[22] E. S. Babu, M. H. M. K. Prasad, C. N. Raju, "In- spired pseudo biotic DNA based cryptographic mech- anism against adaptive cryptographic attacks," In- ternational Journal of Network Security, vol. 18, no. 2, pp. 291-303, 2016.

[23] P. Barman, B. Saha, "An efficient hybrid elliptic curve cryptology system with DNA encoding," In- ternational Research Journal of Computer Science, vol. 2, no. 2, pp. 33-39, 2015.

[24] S. S. Basha, I. A. Emersonand, R. Kannadasan. Survey on molecular cryptographic network DNA (MCND) using big data. In Procedia Computer Science of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), vol. 50, pp. 3-9, 2015

[25] Sohal and Sharma. BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. Journal of King Saud University in Computer and Information Sciences, 2018. Available online 29 September

[26] Z. Yunpeng, L. Xin, M. Yongqiang, C. C. Liang. An Optimized DNA Based Encryption Scheme with Enforced Secure Key Distribution. Springer Science+Business Media, LLC, 2017.

[27] H. D. Tiwari, Jae Hyung Kim "Novel Method for DNA - Based Elliptic Curve Cryptography for IoT Devices.ETRI Journal, Volume 40, Number 3, June 2018.

[28] E. I. Abd El-Latif & M. I. Moussa "Information hiding using artificial DNA sequences based on Gaussian kernel function" Journal of Information and Optimization Sciences ISSN: 0252-2667, 2019.

AUDIO STEGANALYSIS METHOD BASED ON HIGUCHI FRACTIAL DIMENSION AND CONVOLUTIONAL NEURAL NETWORK (CNN)

J. A. Lawal, A.F. Thompson, and O. Owolafe
Department of Cyber Security, Federal University of Technology, Akure.

Abstract - **The rate at which secret messages are been transmitted through various digital signal media is alarming, so may operations like introduction of virus, data poisoning, and others are performed in an unsuspicious manner. Audio steganalysis is an art and science that deals with detecting the presence of a secret message in a digital signal. Other researchers have used so many steganalysis methods which are with the knowledge of the steganography methods (e.g. spread spectrum, LSB, etc) used in embedding the hidden message, also with a particular file format e.g. WAV, MP3, MP4 etc. This research work focus on having a steganalysis method that works without having the prior knowledge of the steganography method used in embedding the secret message using Higuchi algorithm method of reducing fractal dimension for feature extraction and convolutional neural network and the classifier. The result from this research shows that it is possible to detect the hidden message without knowing the steganography method used.**

Keyword: Steganalysis, Covers, Stegos, Convolutional Neural Network (CNN)

I Introduction

Improvement in technology has greatly help and increase the rate at which information is transmitted over the internet, there is serious need to secure and protect the information from any authorized access. For this purpose, two efficient approaches have been devised: watermarking and steganography [7]. The goal of watermarking is to conceal a message within a cover media so that it cannot be detected and any intruder cannot delete or replace the hidden message. watermarking methods are mainly characterized by resistance to attacks. On the other hand, the goal of steganography approaches is to conceal a message so that the least detectable changes are made to the cover media. In other words, the existence of a hidden message in the media should not even be possibly detected. Every steganography system has an insertion algorithm which is able to insert a message into a cover signal and create a stego signal. On the contrary, steganalysis methods aim at detecting or retrieving a hidden message in different types of cover media, such as image, audio, video and text [5]. According to previous studies, audio dealt with less often than other steganography systems, even though the human auditory system is very sensitive.

These methods coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as images, audios and even videos. Although, data transmission has been made very simple, fast and accurate using the internet, one of the main problems that still remains with transmission of data over the internet is that it may pose a security threat. This means, personal or confidential data can be stolen or hacked in many ways. Users may be reluctant to distribute data over the internet due to lack of security; copyright material can be easily copied and spread without the owner's consent. Therefore, it becomes very significant to take data security into consideration, as it is one of the essential factors that need attention during the process of data distribution.

Cryptography and steganography are the two important aspects of communications security although cryptography is a primary method of protecting valuable information by rendering the message unintelligible to outsiders, steganography is a step ahead that makes the communication invisible. Steganography is the art of hiding the presence of communication by embedding secret messages into innocent, innocuous looking cover documents, such as digital images, videos and sound files. Obviously, the purpose of steganography is to avoid drawing suspicion to the transmission of hidden information. Creative techniques have been devised and used for hiding process to reduce the detectable artifacts of the embedded message.

Steganography was used by the Ancient Greeks to hide information about troop movements by tattooing the information on someone's head and then letting the person grow out their hair. [1][3].

. The basic idea behind cryptography is that you can keep a message secret by encoding it so that no one can read it. If a good cryptographic cipher is used, it is likely that no one, not even a government entity, will be able to read it. The fact however, is that an encrypted message does not resemble anything else but an encrypted message. Indeed, merely communicating in secret can sometimes trip up alarms and make others suspicious. The double edge nature of cryptography lies in the fact that, while it may very well be unbreakable by all available standards, an encrypted message is easy to see and tag. Therefore, once a third party determines the existence of secret communication, they may feel compelled to try to find out the content of such covet communication.

This is where steganography comes in. Unlike cryptography, the purpose of steganography is to hide the existence of a message. All that steganography requires is a cover media (which is where data will be hidden), a message that is made up of data, an algorithm that decides

how to hide the data, and usually, a key that will be used to randomize the placement of the data and perhaps even encrypt it.

Due to rapid progress in the field of information technology in the form of smart gadgets, communications, and digital content, an extensive environment with the capability to transfer, copy, duplicate, and share information over the Internet has been built. However, this revolution in the digital world and the online distribution of digital media also implies that harmful messages can be hidden and transmitted through this means. Among the grossly affected parties are governmental organizations and the forensic departments of various military outfits as they face the challenges of detecting terrorist prone hidden and harmful messages.

Addressing the above issue, hidden information detection techniques like steganalysis have shown some promising solutions. However, there are some rising concerns when using this approach. For instance, the research works presented by [2] as well as [6] in which their research work suffers the limitations of low prediction accuracy, inability to give significant differences between covers and stegos.

Ref. [4] was able to show that calibrated features based on re-embedding technique improves performance of audio steganalysis, but still suffers low detection ratio. The research therefore developed an audio steganalysis system based on fractal dimension using Convolutional Neural Network as a classifier; and evaluated the system using precision, accuracy and computational time.

II Research Methodology

Architecture of the Proposed System

The architecture of the proposed system is shown in Figure 2.1. The main components of the architecture are:

1. Acquisition of audio files
2. Preprocessing
3. Ratio selection
4. Training
5. Testing
6. Prediction

Audio Acquisition

There were two types of audio used in this research: cover audios and stego audio

The sources of the dataset are:
https://github.com/Charleswyt/tf_audio_steganalysis/tree/master/papers

https://pan.baidu.com/share/init?surl=rYCzJRksHkgbOOYI9MqQjA

Pre-processing

Data Preprocessing is the step in which the data is being transformed/ encoded so as to be parsed by the machine which makes the features of the data to be easily interpreted by the algorithm.

Feature extraction

Steganography algorithms cause irregularities and intangible changes when applied to audio signals.

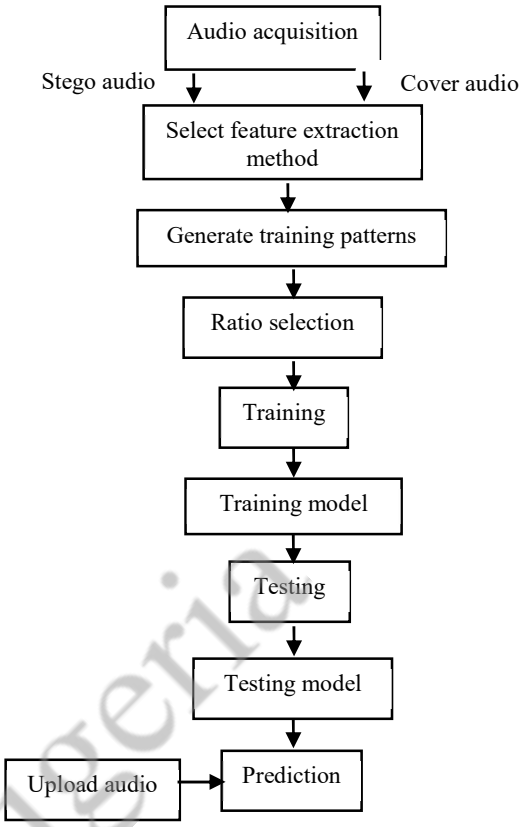


Fig.1. Architectural framework for Audio Steganalysis

Applying features that can accurately reflect the differences between clean and stego audio signals is an important step in steganalysis area. The use of many common features in audio steganalysis systems cannot properly distinguish clean signals from stego signals. The fractal dimension as features was used because these features are able to capture well the irregularities in the audio signals. Since the fractal dimension of an audio frame depends greatly on sample values, the smallest change of samples will change the value of the respective fractal dimensions. As a result, such an attribute can have a great effect on the steganalysis problem. Higuchi's algorithms were employed to extract fractal dimensions from audio frames as shown below

The algorithm was based on a finite set of time series observations $X(1), X(2), X(3), \dots, X(N)$ taken at a regular interval. Based on this series, a new time series, x_k^m was constructed as follows;

$$x_k^m; x(m),\ x(m+k),\ x(m+2k) \dots, x\left(m + \left[\frac{N-m}{k}\right].k\right) \quad (m = 1,2,\dots,k)$$

where k and m are integers, m and k indicate the initial time and the interval time, respectively. For a time interval equal to k, k sets of new time series was obtained. x_k^m, which was the length of the curve and defined as follows:

$$L_m(k) = \frac{\left[\sum_{i=1}^{\frac{N-m}{k}} \left(X(m+ik) - X(m+(i-1)k)\right)\right]p}{k} \qquad (1)$$

N is the total length of the data sequence x and the normalization factor for the curve length of subset time series is defined in equation (2):

$$p = \left(\frac{N-1}{\left[\frac{N-m}{k}\right]k}\right) \quad (2)$$

The length of the curve for the time interval k, (L(k)) is the average value over k sets of $L_m(k)$. If $(L(k)) \propto f^{-D}$ then the curve is fractal with the dimension D. To test that the method for determining a fractal dimension is valid, the numerical application to simulated data was demonstrated. An average length was computed for all-time series having the same delay (or scale) k, as the mean of the k lengths $L_m(k)$ for m = 1, …, k. This procedure was repeated for each k ranging from 1 to k_{max}, which yielded the sum of average time series lengths $L(k)$ for each k as indicated in equation (3):

$$FD_{Higuc} = \sum_{m=1}^{k} L_m(k) \quad (3)$$

Fractal dimension helps to reduce the dimensionality of the audio. The fractal dimension was used as features because these features were able to capture well the irregularities in the audio signals. Since the fractal dimension of an audio frame depends greatly on sample values, the smallest change of samples will change the value of the respective fractal dimensions. As a result, such an attribute can have a great effect on the steganalysis problem.

Ratio Selection

The ratios were 30/70 and 70/30. The ratio 30/70 means taking the first 30% audios of the dataset for testing and the remaining 70% for training and 70/30 means taking the first 70% audio of the dataset for training and the remaining 30% for testing

Training

The architecture of the CNN had six layers: Input Layer, convolution Layer, ReLU Layer fully Connected Layer, softmax Layer and classification Layer. The input layer gets the audio into the model, a layer was created to 2D convolution with height 50, width 1 and a filter followed by a ReLU (Rectified Linear Unit) layer. The extracted features were fed into a binary classifier, which consists of a fully connected layer and a softmax layer followed by a classification output layer. However, all the weights in the CNN architecture can be automatically determined from the training data, without the interference of human. 182 cover and stego files were used altogether, about 128 used for training which is the 70% for training.
The analytical expression of the convolution within the CNN architecture is given in equation (4):

$$h_j^{(n)} = \sum_{k=1}^{k} h_k^{(n-1)} * w_{kj}^{(n)} + b_j^n \quad (4)$$

where $*$ denotes a 2-D convolution operation, $h_j^{(n)}$ is the jth feature map output in the nth hidden layer, $h_k^{(n-1)}$ is the kth channel in the (n−1)th hidden layer, $w_{kj}^{(n)}$ is the kth channel in the jth filter in the nth layer and b_j^n is its corresponding bias term.

Training Model

To generate a training dataset, it is necessary to label every fractal dimension vector to determine the audio frame type. A zero label was allocated to clean frames, whereas a one label was allocated to stego frames.

Testing

During this testing, it returns the label 0 or 1 base on the knowledge from the trained model. Performance metrics (prediction accuracy, precision and recall) was also calculated in testing phase

Prediction

Different audios were predicted based on the training model from the training phase. If the audio has any secret message embedded it will assign 1 to it and return STEGO as the output, and likewise if the message is clean it will assign 0 and return COVER as the output.

Experimental setup

System Requirements

Two types of requirements are specified. They are hardware and software requirements.

a. **Hardware Requirements:** 4 GB RAM, 1.6GHz

b. **Software Requirements:** The system was implemented using MATLAB (R2017a version) programming language on windows 10 Operating System platform

In this designed system, different folders containing different numbers of audio files were used as the stego files to train the CNN.

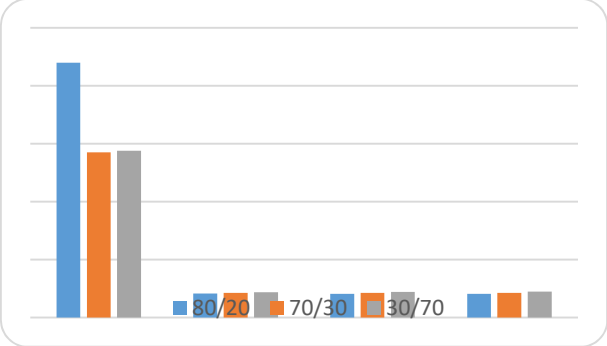


Figure 9: Chart showing variations between the three ratios 80/20, 70/30, 30/70

CONCLUSION

Data transmission has been made very simple, fast and accurate using the internet, one of the main problems that still remains with transmission of data over the internet is that it may pose a security threat. It becomes very important to take data security into consideration, as it is one of the essential factors that needs attention during the process of data distribution. This research work developed an audio steganalysis system to detect the presence of hidden messages in audio file.

REFERENCES

[1] Alese, B. K., Philemon, E. D. ., & Falaki, S. O. (2012). Journal of Engineering Comparative Analysis of Public-Key Encryption Schemes. *International Journal of Engineering and Technology*, *2*(9), 1552–1568

[2] Chen, B., Luo, W., & Li, H. (2017). Audio steganalysis with convolutional neural network. *IH and MMSec 2017 - Proceedings of the 2017 ACM Workshop on Information Hiding and Multimedia Security*, 85–90. https://doi.org/10.1145/3082031.3083234

[3] Gabriel, A. J., Alese, B. ., Adetunmbi, A. ., & Adewale, O. S. (2013). Post-Quantum Crystography based Security Framework for Cloud Computing. *Journal of Internet Technology and Secured Transaction*, *4*(1), 351–357. https://doi.org/10.20533/jitst.2046.3723.2015.0044

[4] Ghasemzadeh, H., & Arjmandi, M. K. (2017). Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. *IET Signal Processing*, *11*(8), 916–922. https://doi.org/10.1049/iet-spr.2016.0690

[5] Gutub, A., & Al-juaid, N. (2018). Multi-bits stego-system for hiding text in multimedia images based on user security priority. *Journal of Computer Hardware Engineering*, *1*(April), 1–9. https://doi.org/10.63019/jche.v1i2.513

[6] Mohtasham-zadeh, V., & Mosleh, M. (2019). Audio Steganalysis based on collaboration of fractal dimensions and convolutional neural networks. *Multimedia Tools and Applications*, *78*(9), 11369–11386. https://doi.org/10.1007/s11042-018-6702-1

[7] Mosleh, M., Latifpour, H., Kheyrandish, M., Mosleh, M., & Hosseinpour, N. (2016). A robust intelligent audio watermarking scheme using support vector machine. *Frontiers of Information Technology and Electronic Engineering*, *17*(12), 1320–1330. https://doi.org/10.1631/FITEE.1500297

Analysis of Cybercrime in Nigeria

***Abstract*— Nigeria has both the largest economy and population in Africa, and this contribute to the growth and fast expansion of ICT and the use of Internet in Nigeria. Like other technologies, Internet has been used by both good and bad actors. The use of internet and computer to commit crime is costing global economy the loss of billions of dollars. In Nigeria, the majority of the population use the Internet for good but some few are using it to commit criminal activities such as Fraud. Cybercriminals in Nigeria, widely called Yahoo Boys in the country specialize in Internet fraud that target mostly International victims. The Nigeria government is stepping efforts to bring an end the activities of these criminals as their actions tarnishes the image of the country. While the efforts of the government had yielded some positive results, the threat of Cybercrime in Nigeria is still high, as criminals continue to take advantage of flaws in the law enforcement tactical approach in addressing the crime. This paper discusses an overview of Cybercrime in Nigeria, the common types of Cybercrime that is perpetuated from the country and the reason of doing so. It also discusses the government's success and areas of strength in its fight against Cybercrime and highlight the areas of weaknesses. Recommendations and suggestions are made on how law enforcement and the government at large can improve to tackle Cybercrime better in Nigeria.**

Keywords*— *Cybercrime, Internet Fraud, Internet Scam, Nigeria

I. INTRODUCTION

It is evident that the spate of cybercrime have continue to grow globally as report from the United State Federal Bureau of Investigation (FBI) Internet Crime Complain Centre (IC3) shows that the sum of $2,700,000,000 was loss to cybercrime in 2019 alone [1], this amount which only reflect Cybercrime reported to the centre showed an increase both in the amount of money loss and number of complain received relating to cybercrime from the previous year's [1]. Business email compromise a form of Internet fraud tops the list of cybercrimes by victim loss in 2019 according to FBI report which cost victims a loss $1,776,549,688[1]. This indicate that the sum of $468,746,199 was lost more by victims to BEC than last year. BEC have been evolving and becoming more sophisticated with cybercriminals deploying latest technology in order to evade detection and deceive victim [1-2].

A group of 80 Cybercriminals were arrested and charged by the FBI in the United States of America on 22nd of August 2019, and 78 of them were Nigerians. They were charged for committing Cybercrime (specifically Business Email Compromise, BEC, and Romance fraud) along with money laundering [3].

To some, this is a serious case and big news but to those that have insight knowledge into the world of Internet fraud, the participation and role of Nigerians playing in it, one can rightly say that this case is just a tip of the iceberg.

In some places the name Nigeria has become synonymous to Internet fraud. Several Internet frauds have been named or directly associated with the country as the majority of the fraudsters that commit such specific crime originate or reside in Nigeria [4][5].

The Australian Competition and Consumer Commission categorically list Nigerian scam as part of a known fraud in the country and according to their statistics that in two months only the sum of $46,544 was lost to that scam [6]. Another form of Internet Fraud is called 419, which is synonymous to Advance Fee Fraud. The name 419 is a reference to the section of the Nigerian Constitution that deals with the crime and is been internationally recognised as a form of fraud that originates from Nigeria [6].

Agari Cyber Intelligence analysed 10 organized crime groups and 59,652 unique email messages and found out that 9 out of the 10 groups were based in Nigeria forming the majority of the email messages [7].

Cybersecurity Intelligence report 2018 showed that a large number of Nigerian gangs are involved in Internet fraud, researchers for the Cybersecurity firm Crowdstrike gathered intelligence for 12 months on BEC fraud and reported that majority of the emails IP address come from Nigeria [8].

A Nigerian, Osondu Victor Igwilo, was in the FBI most wanted list as of January 2020, for defrauding multiple US financial agencies of approximately $100million [9].

Another Nigerian Ayodele Abraham Saliu with three other men were arrested in South Africa in 2012 by Interpol on request from the US, as he was accused of fraud to the tune of $500,000 and also other Cybercrime including intrusion into National Aeronautics and Space Administration (NASA) headquarters computer system [10].

Emmanuel Ekhator was extradited from Nigeria to

the US and sentenced in 2013 to 100 months in prison by US district court middle of Pennsylvania for committing fraud of $70million [11].

Two Nigerian men were arrested by FBI and prosecuted in court where they pleaded guilty for defrauding a Texas woman of $2,000,000 through Romance fraud [4].

A joint operation between the Malaysian and Singapore police arrested 13 Nigerians in Malaysia involved in Romance Fraud that cheated their victims $6,900,000. Malaysian authorities confirmed that the fraud was masterminded by Nigerians in the country on student visa, and sometimes recruit the Malaysians women to act as money mule, whose bank account are used to deposit proceed of the fraud [12]. Similarly, Nigerian gangs of Internet fraudsters residing in Malaysia have been attributed to Romance Fraud in Hong Kong [13].

US Department of Justice on 25th of April 2019 arrested and prosecuted 9 fraudsters responsible for Business Email Compromise and Romance Fraud, of the 9 arrested, 7 were Nigerians [14].

The City of London arrested and convicted 6 Nigerians based in London for committing various types of Internet Fraud. They defrauded their victims of more than £10million [15-16]. The examples can continue to go on and on, unfortunately.

Most of the victims of these fraudsters are not residing in Nigeria but mostly in English speaking countries in the Western world and Asia, countries like UK, US, Australia, Canada, Hong Kong, Malaysia, and Singapore.

The activities of those criminals do not only stop in causing financial losses and psychological trauma to their victims, they as well affect the image of Nigeria. Because law enforcement agencies were able to trace the origin of some of those scams, it happened that Nigeria have been recognised as one of the dens of Internet Fraudsters and Cybercriminals. A research conducted in the UK to trace the geographic origins of Romance Fraud listed Nigeria as number one, the largest single origin of Romance Fraud in the world, and the same result was found with Advance Fee Fraud [17]. This had consequences to the country reputation and its citizens at large especially the issuing of travel visas, because even people going to study or with legitimate business dealings sometimes has to face extra security screening and checks because of the bad reputation the Cybercriminals have caused to Nigeria.

II. Internet Fraud linked to Nigeria

A. Advance Fee Fraud

Advance Fee fraud which is also referred to as Inheritance, West Africa or Nigerian Fraud; happens when a victim is promised a huge sum of money that will be made as a result of either a legal or illegal activities like transferring money of a late African dictator, or claiming that inheritance have been left in the victim's name by an unknown relative, or some kind of lucrative business, etc. but with the demand of some advance payment to facilitate the transaction or activity. Advance Fee Fraud victims are mainly contacted via email which is sent to targeted mostly English-speaking people who have names common to that country [18-21].

B. Origins of Romance and Advance Fee Fraud

In 2015, the FBI ranked Nigeria as number 3 globally in origin of reported cases of Internet fraud [22]. The vast majority of Romance Fraud aimed at the US originated from Nigeria [4].

Research by [23] analysed scam emails to identify the geolocation of the sender using a honeypot. They collected IP addresses to explicitly confirm the geolocation of the scammers. The research result showed that more than 50% of the scam emails originated from Nigeria ranking as number one globally followed by the US and the UK.

While a more recent research by [17], analysed IP address from email headers of Romance and Advance Fee Fraud emails, the research results also ranked Nigeria as number one globally with respect to the origin of these types of fraud. West Africa in general accounts for over 50% of the same location, and the proportions closely reflect that of Advance Fee fraud as well.

TABLE I. A summary of global IP Geolocation of scam emails [23]

Country	Scam email IP Geolocation	Global ranking
Nigeria	50.3%	1
USA	37.6%	2
UK	3.0%	3
Ghana	2.0%	4
Netherland	1.3%	5
Sweden	1.2%	6
Poland	1.0%	7
Germany	0.9%	8
Canada	0.6%	9
Benin	0.3%	10
South Africa	0.3%	11
Malaysia	0.2%	12

C. Business Email Compromise Fraud

This type of fraud is carried out when Cybercriminals carefully spoof the email address of an employee (mostly the senior executive) and then use it to send a payment request to the finance staff (or any staff responsible for making payment) within the organisation. The email usually instructs the targeted staff to make wire transfer to an account supplied by criminal. Cybercriminals in such attacks carefully spoof the email address of the employee they intend to impersonate and even the writing style making it difficult to easily spot and sometimes even evading detection from anti-malware software which turns to classify it as legitimate email [20-21][24-25].

Nigerian fraudsters have adopted the use of advanced technologies and sophisticated malware like Keyloggers (such as Predator pain, Hawkeye) and Remote Access Trojan (RAT) (such as Netwire) to commit their crime [8][26][27].

TABLE II. Nigerian Business Email Compromise Fraudsters

ARRESTED IN THE US FROM 2015 TO 2017 [8]

Name	Amount lost in $million	Year of Arrest	Sentence term
Amechi Colvis Amuegbunam	$3.7	2015	46 mths
Obinna Kelvin Obioha	$6.5	2017	51 mths
David Chukwuneke Adindu	$25	2017	3 yrs

TABLE III. BUSINESS EMAIL COMPROMISE/EMAIL ACCOUNT COMPROMISE LOSSES IN US FROM 2014 TO 2019 [21]

No. of cases reported	Amount lost in $	Year
2,417	$226,000,000	2014
7,837	$246,226,016	2015
12,005	$360,513,961	2016
15,690	$676,151,185	2017
20,373	$1,297,803,489	2018
23,775	$1,776,549,688	2019

D. Romance

Romance Fraud (also known as Dating fraud) is when a fraudster creates fake online profiles and engage in a deceptive and fake relationship with their victim in order to defraud them. The fake profile is created usually on some popular dating websites and apps and later transfer their victims to start personal unmonitored communication using either email, SMS, or social media platforms like Instantgram, WhatsApp, Facebook messenger etc. Then after some time in the relationship will start to request money for personal use from the victim either as loan (which will never be paid back) or financial assistance. Sometimes the fraudsters will deceptively ask the victims of their account details and then start withdrawing money from the account. In some instances, victims of Romance Fraud are blackmailed especially if fraudsters are in possession of intimate pictures or videos of the victims that they deceptively acquired from the victims. Some victims of Romance Fraud are turned into money mules by the fraudsters, where fraud money will be deposited into their account and then ask them to withdraw and send it to them (mainly to overseas using instant money services) or wire transfer the money to their account [24][28][29].

The following table shows the statistical figures of losses as a result of Romance and Advance Fee Fraud from Australia, UK, and US.

TABLE IV. ROMANCE AND ADVANCE FEE FRAUD LOSSES FROM AUSTRALIA, UK, AND US [30-35]

Country	Fraud Type	Amount lost	Reports No.	Year
Australia	Romance Fraud	$25,480,351	4,109	2016
Australia	Nigerian Advance Fee	$1,404,108	1,498	2016
Australia	Romance Fraud	$20,530,578	3,763	2017
Australia	Nigerian Advance Fee	$1,665,373	1,287	2017
Australia	Romance Fraud	$24,648,024	3,981	2018
Australia	Nigerian Advance Fee	$1,379,285	878	2018
Australia	Romance Fraud	$11,019,068	1,950	2019 June
Australia	Nigerian Advance Fee	$536,972	341	2019 June
UK	Romance	£27,344,814	2,824	2013
UK	Romance	£32,259,381	3,295	2014
UK	Romance	£25,882,339	3,363	2015
UK	Romance	£39,000,000	3889	2016
UK	Romance	£41,000,000	3557	2017
UK	Romance	$12,600,000	1,404	2018
UK	Advance Fee	$14,000,000	8,133	2018
US	Romance	$219,807,760	14,546	2016
US	Advance Fee	$60,484,573	15,075	2016
US	Romance Fraud	$211,382,989	15,372	2017
US	Advance Fee	$57,861,324	16,368	2017
US	Romance Fraud	$ 362,500,761	18,493	2018
US	Advance Fee	$ 92,271,682	16,362	2018

III. NIGERIAN FRAUDSTER'S POTENTIAL TARGETS/VICTIMS

Internet Fraudsters from Nigeria are mainly targeting rich, western and mostly English-speaking countries, although recent findings revealed that the fraudsters are present in some Asian countries which are mostly English-speaking countries as well like Singapore, Malaysia and Hong Kong [4]. This may not be unconnected with the language barrier, as Nigeria was formerly colonized by Britain, English was made the official language. That makes it easier for fraudsters to target English-speaking countries but more difficult to target non-English speakers.

In addition, most fraudsters from Africa target people with common names such as John, Michael, Anne, Sarah, Mary, etc. in place of names from the old Eastern European block as those are not all expected to speak English [4]. Many of those fraudsters are posing as professionals from European or American countries with jobs as Engineers, Managers in multinationals corporations, Military servicemen, Ship captains etc. [35-36].

IV. USE OF EMAIL BY FRAUDSTERS IN NIGERIA

Analysis and information from the EFCC revealed that fraudsters prefer to use email to communicate with their victims because

- Sending email is cheap and affordable.
- Creating a new email address is easy.
- Ability to reach wider targets.
- Managing email account does not need special technical knowledge.
- Spoofing email addresses of people is easy.
- Flexibility of using and operating email.
- Anonymity, such that sender can hide their true identity from the receiver.

- Difficult to spot deception and discrepancy in language as it is written not spoken.

V. Nigerian Government Effort in Fighting Cybercrime

The Economic and Financial Crime Commission (EFCC) was established in 2004 with the responsibility of fighting economic crime in Nigeria. The EFCC is Nigerian agency that is empowered to prevent, investigate, prosecute, and penalise economic and financial crimes and is responsible for law enforcement with regards to others and regulation relating to financial crimes including all forms of Internet fraud, and other fraud related offences. It is within EFCC mandate to deal with Cybercrime and Fraud. The commission has been fighting and combating Internet fraudsters in Nigeria known as Yahoo Yahoo boys with many arrests and successful convictions [37].

A training school for Internet fraudsters was recently shut down in Lagos, Nigeria, with both proprietor and students arrested by the EFCC in Nigeria [38]. On 10th July 2019, EFCC arrested thirty Internet fraudsters aged between 18 to 27 years in the city of Ado Ekiti, Ekiti state, Nigeria [39]. Almost all the fraudsters declared wanted by the FBI had been arrested and extradited to the US among which is Obinwanne Okeke popularly known as Invictus Obi, a well-known fraudster that claims to be a successful businessman. The FBI had awarded certificate of appreciation to EFCC officers that assist in the FBI Internet fraud raid [40].

The EFCC has published a list of successful arrests and convictions of Internet fraudsters within July 2019 [41].

VI. Challenges and Recommendations

As part of its mandate, the EFCC has risen up against Cybercrime in Nigeria, especially Internet Fraud. Its beyond doubt that the EFCC are recording success in this fight against Internet Fraudsters popularly known as Yahoo Yahoo, Yahoo Boys or recently Yahoo Plus (+). The number of arrests and subsequent convictions will make one to realise an d also see the successes recorded in this fight against those Cybercriminals. However, despite those successes one may not fail to notice some of the short coming and challenges the EFCC facing.

- The EFCC mostly rely on human intelligence to go after those criminals, its people within the neighbourhood or community of those fraudsters that monitor and suspect their extravagant life style and with no reasonable explanation to the source of their wealth, those people then tip up the EFCC before they swing into action and arrest them. Sometimes referral from international collaborating law enforcement agencies like US FBI, UK NCA, that give the EFCC tipoff. Even the during investigation and questioning the EFCC rely on human resource instead of using technology. In this regard, after applauding the EFCC for recording success in the fight against Cybercrime, there is need for the agency to invest in training and re training it staff on the use of technology to combat this crime, and also the need to deploy latest technological solution to tackle these crimes.
- Beyond the EFCC there is also need for the Nigerian Communication Commission (NCC) to step up to it mandate and expectation and equally play it part in combatting Cybercrime. As the name says, this crime is done online using Internet which is provided by the ISP companies and those companies are in theory supposed to be regulated and monitored by the NCC, if and when the NCC choose to give security emphasis in its mandate and operation not only revenue generation, the commission through the ISP can as well play a vital and key role in stopping, mitigating and arresting of those Cybercriminals. The Federal Ministry of Communication and Digital Economy (FMCDE) as the mother ministry that oversee the NCC have a vital role to play as well but it seems the ministry is more concern with the economic aspect than security which is not helping matters. Furthermore, the Nigerian Computer Emergency Response Team (NgCERT) responsible for the protection of Nigeria cyberspace under the Office of National Security Adviser (ONSA) can as well play a vital role in tackling cybercrime in Nigeria, but their presence is hardly notice in the country, another reason why EFCC effort in combating Cybercrime needs to be appreciated.
- While embracing and deploying technology, a partnership between the EFCC, NCC, FMCT and the NSA office can drastically reduce Cybercrime and other IT related crimes bedevilling the country. Harmonization and Intel's sharing between the law enforcement and other government agencies will help improve the success of the fight against Cybercrime.
- There is lack of academic and scholarship input in the fight against cybercrime in Nigeria, not many Universities offer courses on Cybersecurity and that results to few academic research and publication on how to combat Cybercrime in Nigeria.
- Lack of dedicated team of police to handle Cybercrime in the country is not helping matters, therefore there is need to have special police unit dealing with Cybercrime and forensics.
- The availability of smart phones and laptops makes it much easier to have internet access but still some of these fraudsters use commercial the Internet café, a law under the Nigeria Cybercrime Act 2015 requires Internet café to keep logs of customers, compliance to this law will help law enforcement in identifying and arresting Cybercriminals. Also, Internet service providers (ISP) can as well keep log of private users of broadband.
- From the legal perspective, the Nigerian judiciary

need to support the EFCC and the government at large by sentencing these found guilty of Internet fraud to a reasonable prison term or fine, but not a sentence that will prove Internet fraud is profitable and worth doing. Imagine a Yahoo Yahoo guy found guilty of defrauding someone thousands of dollars only to be sentence to one year in prison with an option of fine of N50,000. This is the case of one Isaac Dark Obozokhai who defrauded one Lynn Dianna Bowel $5,000, but after the EFCC arrested and successfully prosecuted him, on 9th July 2019 he was found guilty and sentenced to one year in prison with an opinion to pay fine of N50,000 which is less than $200. The question arises here as to how can young people that are determined to join Yahoo be deterred by such a sentencing when someone is found guilty of $5000 fraud but asked to pay a fine of less than $200. Asking fraudster to pay small amount of money as fine in exchange for prison sentence will not serve as deterrence to cybercriminals, especially if the case which they are being prosecuted is not the first and only fraud they have committed, in which case they can pay the meagre fine keep enjoying the remaining money, hence the Internet fraud have proven a lucrative business to them. The Nigeria Cybercrime Act 2015, have specified some strict penalty for committing Internet fraud, it is therefore recommended that Nigerian Judiciary refers to such section of the act for sentencing Cybercrime in Nigeria.

- To successfully cub young people from going into Internet fraud (Yahoo Yahoo), the government has to make sure their business is non-profitable. One way is to make sure the cost to those found guilty of such crime pay by far out weight the benefit. Even in the instance were fine is an option, the fine should be by far more than what the fraudster defrauded from their victims. This will make them end up in loss, but in a situation where the fraudster is asked to pay a fine less than what he defrauded their victims, definitely they will pay and keep their balance and it has proven to them that it is a lucrative and successful money making business.
- Many of the fraudsters are technically savvy, while some very few are sophisticated, however pending on the level of their technical capacity, the government should try to create opportunities either in the form of job in both public and private organisation or support them to start up IT businesses for those young IT minded people to get engaged in something positive and be distracted away from Cybercrime.
- As part of the government effort to curb Cybercrime there is still a need for societal reorientation. The government should engage influential figures in the community like religious leaders, traditional leaders, and scholars to sensitise the public against youth participation in Cybercrime. This becomes necessary as the youth are already getting the opposite, such that some people in society praise these fraudsters for this dubious activity, with even some influential musicians have repeatedly praised, justified, and encouraged youths participation in Internet fraud through the lyrics of their songs, as far back as 2007 songs like Yahooze by the Nigerian musician, Olu Maintain, who was in direct reference to the Internet fraudsters in Nigeria and their exotic life style which was flagrantly displayed in his video [42]. Another young Nigerian musician by the stage name, Naira Marley, is a promoter, supporter, and defender of Internet Fraudsters in Nigeria, as clearly stated and shown in the lyrics and videos of some of his tracks like “Am I A Yahoo Boy” and “Soapy” [43-44]. Naira Marley was arrested by the EFCC on suspicious of Internet fraud himself and is standing trail as of February 2020. Nkem Owoh, a popular Nigerian actor and comedian, not only justified the act of Internet fraud but also clearly discussed how the fraud is done, and repeatedly praised and justified the crime in one of his lyrics which says “*Oyinbo Man I go chop your dollar. I Go Take Your Money Disappear*” meaning he will take the white man dollars, and runaway [45]. Obinwanne Okeke, popularly known as Invictus Obi, had been a role model for many young Nigerians, and was even named by Forbes magazine in 2016 among Africa’s under 30 most promising entrepreneurs [46]. Only to be indicted by the FBI for Internet fraud, and had been remanded in prison in the US while awaiting trial for stealing $11million [47].

VII. Related Research work

Ongoing research by the authors of this paper is working on the application of artificial intelligence techniques for email classification, detection, and prevention of Internet fraud originating from Nigeria. The research focuses on two of the three most common Internet fraud originating from Nigeria (Advance fee fraud, and Romance fraud). The research seek to analyse and extract unique pattern from content of Advance fee fraud and Romance fraud email sample that originate from Nigeria. Email classifier design using machine learning

The research is analysing the text content of an email to extract and identify unique characteristics common in fraudulent emails originating from Nigeria. The research proposed the use of MATLAB analytic software, using supervised learning Machine learning algorithm the extraction of features is carried out, then using the features the classifier is train by labelling the sample created from bag of words, during testing of the classifier comparison is made to classify email as legitimate or fraudulent. Data set used to extract feature and training of the classifier were collected from the EFCC and Kaggle.

An earlier work published by [48], looked at “Fortune from the Dead (FFD)” a type of Advance Fee Fraud. The researchers proposed the use of ontology base information extraction method to recognize fraud

evidence from texts samples of Nigerian fraud emails using RegEx, a free and open source machine learning software programmed in Java [48].

Nigeria was identified as the largest origin of Romance scam by Geographic location from a research work carried out [17]. The research try to find the real location of Romance scammers by analysing the online scammers profile from popular dating site.

[23] carried out research to understand targeted Nigerian scam on craigslist, a popular online market website that have more than 60 million visitors in US alone. The research attempted to analyse scam emails responding to fake advertisement posted intentionally to attract Nigerian scammers. Using a honeypot, they collect IP addresses of scammers to explicitly confirm their geolocation.

Another research conducted by [49] proposed the detection of fraudulent emails using Waikato Environment for knowledge analysis (WEKA) data mining software and employ TF-IDF for feature extraction. The research used Nigerian emails as part of their dataset.

The research result showed that more than 50% of the scam emails originated from Nigeria, analysis carried out by the researchers focus on identifying the geolocation of the sender, working time of the scammers, response time to advert, degree of automation, and the analysis of IP and shipping address [49].

VIII. CONCLUSIONS

In this paper, we present analysis of Cybercrime in Nigeria. With discussion about the Internet fraud, specifically Advance fee fraud, Business Email compromise and Romance fraud, these are the three most common cybercrimes committed in the country. Cybercriminals from Nigeria know as Yahoo Boys target international victims especially English speaking countries with the intension to defraud them either by promising huge return after investment as in Advance fee fraud, or Business email compromise, where fraudsters will deceptively request for payment via wire transfer to a fraudulent account oversee by forging company executives email to request for payment, or in Romance fraud where fraudster will establish a false relationship pretending to love victim but end up defrauding them.

Nigerian government through the law enforcement agencies have continue to fight Cybercrime in the country and successes had been achieved in certain areas, however cybercriminals have continue to carry on with their malicious activities. This paper review the success of the government and also highlight the areas where law enforcement agencies need to improve in order to effectively tackle cybercrime in Nigeria.

Finally the attitude of celebrating and promoting of Cybercrime was discuss. In some instances Cybercriminals are not only glorified and praised in songs but are celebrated in their villages and communities as bread winners. Some are even conferred with traditional tittles while some engage in spending spree to people of the community. Therefore it is strongly suggested the need for Nigerians denounce this crime and come together collectively to support the government and law enforcement agencies in the fight against Cybercrime in the country.

ACKNOWLEDGMENT

The authors wish to acknowledge the EFCC for having access to some cases of arrest and prosecution, and also in providing part of the data set used in the ongoing research which stated in the related work.

REFERENCES

[1] FBI IC3, "2019 Internet Crime Report", 2019. [Online] Available at: https://pdf.ic3.gov/2019_IC3Report.pdf [Accessed 16 Feb 2020].

[2] BBC News, " Cyber-crime profits reached $3.5bn in 2019, says FBI ", 12 February 2020. [Online] Available at: https://www.bbc.co.uk/news/technology-51474109?intlink_from_url=https://www.bbc.co.uk/news/topics/c1xp19421ezt/cyber-crime&link_location=live-reporting-story [Accessed 20 February 2020].

[3] BBC News, "US names Nigerians in massive fraud investigation", 23 August 2019. [Online] Available at: https://www.bbc.co.uk/news/world-africa-49446845 [Accessed 24 Aug 2019].

[4] A. Brenoff, "How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts". HuffPost., 2017. [Online] Available https://www.huffingtonpost.co.uk/entry/romance-scams-online-fbi-facebook_n_59414c67e4b0d318548666f9?guce_referrer=aHR0cHM6Ly9jb25zZW50LnlhaG9vLmNvbS8&guce_referrer_sig=AQAAAEIQc2oZZgY0aojwEad0jzGsayrW4MuO5rA01HIG8XSfcVKWHHHqDaeOe4BJLgqGYGbq1SxePdERrQ23mkRqXQUGKKmrTwOf0MJJda_CQFCIfMMJlMLkkLnAIVvc1JhkDxpt0aNdXHCIPZxzzlRKpfCgR0nyrDiH0IBYzVGEx8E1&guccounter=2 [Accessed 14 Aug 2019].

[5] US-CERT, "Recognizing and avoiding email scams". Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), 2008. [Online] Available at: https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf [Accessed 15 Apr 2017].

[6] Australian Competition and Consumer Commission, "Nigerian scams", 2019. [Online] Available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams [Accessed 13 Apr 2019].

[7] Agari, "Agari Cyber Intels", 2020. [Online] Available at: https://www.agari.com/cyber-intelligence-research/whitepapers/behind-the-from-lines.pdf. [Accessed 12 Feb 2020]

[8] Crowdstrike, "Crowdstrike", 2020. [Online] Available at: https://www.crowdstrike.com/wp content/brochures/reports/NigerianReport.pdf. [Accessed 12 Feb 2020]

[9] Federal Bureau of Investigation, "FBI Most Wanted". 2020. [Online] Available at: https://www.fbi.gov/ wanted/wcc/osondu-victor-igwilo/ [Accessed 17 Jan 2020].

[10] South Africa Police, "Nigerian and Tanzanian fugitives extradited to U.S.A.", South African Police Service. 2016. [Online] Available at: https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=7040 [Accessed 12 Feb 2020]

[11] FBI IC3, "2014 Internet Crime Report", 2014. [Online] Available at: https://pdf.ic3.gov/2014_IC3Report.pdf [Accessed 12 Feb 2020]

[12] T. Leong, "27 love scam suspects nabbed in KL-S'pore joint operation". The Straits Times. 14 February 2017. [Online] Available at: https://www.straitstimes.com/asia/se-asia/27-love-scam-suspects-nabbed-in-kl-spore-joint-operation [Accessed 15 Aug 2019].

[13] I. Stenger, "Lonely Hong Kong women are being swindled huge

sums of money by fake lovers". Quartz, 24 September 2018. [Online] Available at: https://qz.com/1398075/romance-scams-dupe-lonely-hong-kong-women-of-millions-of-dollars/ [Accessed 15 Aug 2019].

[14] US Department of Justice, "Nine Defendants Arrested In New York, Florida, And Texas For Multimillion-Dollar Wire Fraud Scheme", April 2019, [Online] Available at: https://www.justice.gov/usao-sdny/pr/nine-defendants-arrested-new-york-florida-and-texas-multimillion-dollar-wire-fraud. [Accessed 12 Feb 2020]

[15] Action Fraud, "Gang of fraudsters jailed for 43 years by the Metropolitan Police after reports to Action Fraud". 2019. [Online] Available at: https://www.actionfraud.police.uk/news/gang-of-fraudsters-jailed-for-43-years-by-the-metropolitan-police-after-reports-to-action-fraud [Accessed 13 May 2019].

[16] Samuel Ogundipe, "Internet Fraud; Six Nigerians, Others get 43 years in the UK Jail". Premium Times, 10 May 2019, [Online] Available at: https://www.premiumtimesng.com/news/headlines/329320-Internet-fraud-six-nigerians-others-get-43-years-in-uk-jail.html. [Accessed 12 Feb 2020]

[17] M. Edwards, G. Suarez-Tangil, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty, "The Geography of Online Dating Fraud". Workshop on Technology and Consumer Protection, San Francisco, USA, 24 May 2018.

[18] Action Fraud, "Advance fee fraud", 2019. [Online] Available at: http://www.actionfraud.police.uk/node/290 [Accessed 13 Mar 2019].

[19] Australian Competition and Consumer Commission, "Australian business hit hard by email scams", 2019. [Online] Available at: https://www.scamwatch.gov.au/news/australian-businesses-hit-hard-by-email-scam [Accessed 09 Jun 2019].

[20] Federal Bureau of Investigation, "Internet Fraud", 2019. [Online] Available at: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/ [Accessed 13 Mar 2019].

[21] Internet Crime Complaint Centre, "Internet Crime Schemes", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2018. [Online] Available at: https://www.ic3.gov/crimeschemes.aspx#item-12. [Accessed 12 Feb 2020]

[22] Internet Crime Complaint Centre, "2015 Internet Crime Report". US US Department of Justice, Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2015. [Online] Available at: https://pdf.ic3.gov/2015_IC3Report.pdf [Accessed 15 Apr 2017].

[23] Y. Park, J. Jones, D. McCoy, E. Shi, and M. Jakobsson, "Scambaiter: Understanding Targeted Nigerian Scams on Craigslist", 2014 Network and Distributed System Security (NDSS) Symposium. ISBN: 1-891562-35-5, 22 February 2014. [Online] Available at: https://www.ndss-symposium.org/ndss2014/programme/scambaiter-understanding-targeted-nigerian-scams-craigslist/ [Accessed 13 Aug 2019].

[24] Action Fraud, "Types of fraud", 2019. [Online] Available at: http://www.actionfraud.police.uk/a-z-of-fraud [Accessed 13 Mar 2019].

[25] US Secret Service, "Fraud Alert-Business Email Compromise Continue to Swindle and Defraud US Businesses", USA, 2019. [Online] Available at: https://www.secretservice.gov/data/investigation/BEC_Joint_Product.pdf. [Accessed 12 Feb 2020]

[26] Anon, "NetWire RAT", New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) Journal, 2016. [Online] Available at: https://www.cyber.nj.gov/threat-profiles/trojan-variants/netwire-rat. [Accessed 12 Feb 2020]

[27] Megan Roddie, and Limor Kessem, "New NetWire RAT Campaigns Use IMG Attachments to Deliver Malware Targeting Enterprise Users", Security Intelligence Journal, 2020. [Online] Available at: https://securityintelligence.com/posts/new-netwire-rat-campaigns-use-img-attachments-to-deliver-malware-targeting-enterprise-users/ [Accessed 12 Feb 2020]

[28] Scotland Police UK, "Main Electronic Fraud Types", 2019. [Online] Available at: http://www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/fraud/main-electronic-fraud-types. [Accessed 12 Feb 2020]

[29] European Cybercrime centre, "Money Muling", 2020. [Online] Available at: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling. [Accessed 12 Feb 2020]

[30] Australian Competition and Consumer Commission. "Scam cost Australians half a billion dollars", 2019. [Online] Available at: https://www.scamwatch.gov.au/news/scams-cost-australias-half-a-billion-dollars [Accessed 10 Jun 2019].

[31] Scott Smith, "2016 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2016. [Online] Available at: https://pdf.ic3.gov/2016_IC3Report.pdf. [Accessed 12 Feb 2020]

[32] Scott Smith, "2017 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2017. [Online] Available at: https://pdf.ic3.gov/2017_IC3Report.pdf. [Accessed 12 Feb 2020]

[33] Matt Gorham, "2018 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2018. [Online] Available at: https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf. [Accessed 12 Feb 2020]

[34] L. Graham, "Cybercrime costs the global economy $450 billion: CEO". CNBC, 7 February 2017. [Online] Available at: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html [Accessed 12 Feb 2020]

[35] UK Finance, "Fraud The Facts 2019: The definitive overview of payment industry fraud", 2019. [Online] Available at: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf [Accessed 12 Feb 2020]

[36] BBC News, "Online dating fraud victim numbers at record high", BBC News, 23 January 2017. [Online] Available at: https://www.bbc.co.uk/news/uk-38678089 [Accessed 13 Aug 2019].

[37] EFCC, "EFCC News and Information", 2020. [Online] Available at: https://efccnigeria.org/efcc/news. [Accessed 12 February. 2020].

[38] Punch News, "Proprietor, Students of Yahoo Yahoo School arrested in Lagos - EFCC", Metro Plus, 28 May 2019. [Online] Available at: https://punchng.com/proprietor-students-of-yahoo-yahoo-school-arrested-in-lagos-efcc/. [Accessed 12 Feb 2020]

[39] EFCC, "EFCC Arrests 30 Suspected Yahoo Boys in Ado-Ekiti", 2019. [Online] Available at: https://efccnigeria.org/efcc/news/4575-efcc-arrests-30-suspected-yahoo-boys-in-ado-ekiti. [Accessed 12 Aug 2019].

[40] EFCC, "EFCC Officers get FBI certification", 2020. [Online] Available at: https://efccnigeria.org/efcc/news/5408-efcc-officers-get-fbi-certification. [Accessed 12 Feb 2020].

[41] EFCC, "EFCC News and Information", 2019. [Online] Available at: https://efccnigeria.org/efcc/news. [Accessed 12 August. 2019].

[42] YouTube, "Olu Maintain's Official Video "Yahooze", 2007. [Online] Available at: https://www.youtube.com/watch?v=0MW7kcZnaiA [Accessed 12 Feb 2020]

[43] YouTube, "Naira Marley - Soapy [Official Video]", 2019. [Online] Available at: https://www.youtube.com/watch?v=_Q6Rixmvujc [Accessed 12 Feb 2020]

[44] YouTube, "Naira Marley x Zlatan - Am I A Yahoo Boy (Official Video)", 2019. [Online] Available at: https://www.youtube.com/watch?v=vvBZk4a871I [Accessed 12 Feb 2020]

[45] YouTube, "Osuofia - I Go Chop Your Dollar", 2006. [Online] Available at: https://www.youtube.com/watch?v=D_YjvC4ndzM [Accessed 12 Feb 2020]

[46] Kerry A. Dolan, "Africa's Most Promising Entrepreneurs: Forbes Africa's 30 Under 30 For 2016", Forbes, 2016. [Online] Available at: https://www.forbes.com/sites/kerryadolan/2016/06/06/africas-most-promising-entrepreneurs-forbes-africas-30-under-30-for-2016/#424f580f1f43 [Accessed 12 Feb 2020]

[47] BBC News, "Letter from Africa: Why Nigeria's internet scammers are 'role models", 23 September 2019. [Online] Available at: https://www.bbc.co.uk/news/world-africa-

49759392 [Accessed 12 Feb 2020]

[48] Gao Yangbin, and Gang Zhao. "Knowledge based information extraction: A case study of recognizing emails of Nigerian fraud". Natural language processing and Information systems, NLDB 2005, Alicate Spain, June 15-17, 2005, Proceedings.

[49] Sarwat Nizamani, Nasrullah Memon, and Mathies Glasdam, "Detection of fraudulent emails by employing advanced feature abundance". Egyptian Informatics journal, Vol. 15, pp. 169-174, 2014.

A Review of Autism Diagnosis/Screening Expert System and Mobile Application

Amina Sani Adamu
Department of Computer Science
Nile University of Nigeria Abuja
FCT, Nigeria
email:amina3sani@gmail.com

Saleh El- Yakub Abdullahi
Department of Computer Science
Nile University of Nigeria Abuja
FCT, Nigeria
email:saleh.abdullahi@nileuniversity.edu.ng

Abstract: **Autism is a neuro developmental disorder affecting individuals from Childhood mostly characterized by abnormal behavior, inadequate social interaction, lack of proper communication and repetitive behaviors. Before now, Autism was classified into 3 classes (Infertile Autism, Asperger's disorder and Pervasive Developmental Disorder not otherwise specified) as in the Diagnostic of Statistical Manual of Mental Disorders 4 (DSM 4) but in the year 2013 DSM 4 was upgraded to DSM 5 making all classes be in one class namely Autism Spectrum Disorder (ASD). In this paper, we did a literature review of some Autism Diagnosis Expert Systems and Mobile applications. From our research, we found out that most system/tools have adopted the DSM 5 criteria, most tools have either used the existing assessment tools or used Augmented reality for diagnosis. And also most of the expert system is mostly designed to diagnose children very few considered adult. None of the tools or expert system can give the level of Autism based on the DSM 5 diagnosis therefore there is need for tools to be developed for making such diagnosis.**

Keywords: ASD, Expert System, Diagnosis, DSM 4, DSM 5

I. INTRODUCTION

Autism Spectrum Disorder (ASD) is a complex developmental disorder that affects the brain of an individual from childhood up to Adult age[1]. Most individuals with ASD do have problems with social communication, language development and repetitive behaviors. Diagnosis relies upon matching the child's behavior patterns and development mentioned earlier with the diagnostic criteria. ASD usually emerges in early infancy, and most diagnosis of autism can be reliably made from two years of age[1].

Individuals with developmental disabilities are mostly at higher risk of vulnerability because they rely mostly on others to survive. Early intervention is very important for individuals with developmental delays, because it do affects them both academically and socially, from reaching their developmental potential[2]. Regular screening during health care visits for autism or DD offers an easily administered means of early detection, while enabling referral for further evaluation and intervention where needed, Screening requires adequate financial and human resources for implementation.

Pediatric providers should use screening and surveillance to provide accurate and early identification, cost- effective and timely diagnosis, prompt implementation of evidence-based interventions, and elimination of disparities to access to care for children with ASD. Clinicians should respond appropriately to family or clinical concerns and results of screening to avoid delays in diagnosis and treatment[3]. For this reason, researchers all over the world are trying to develop diagnostics tools that are faster and easier for clinicians to use for such diagnosis.

One of the tools developed based on research for diagnosis are the expert systems which can mimic the human expert in a particular field[4].Expert system have contributed to the medical field and researchers are encouraged to continue to build expert system in the field[5]. They help in solving issues that are very complex and where experts in a particular field are limited or unavailable[6][4]. Though they are said to be prone to errors, not up to date and limited to a particular domain they are developed for [7].

This research paper is divided into four sections: section one is the introduction, section two is related work reviewed, section three is the main literature Review and section four is the conclusion of this work. This research is aimed at reviewing the methodologies adopted for the development of the diagnosis tools, the data use, the type of Knowledge base use for the development of the system and the criteria adopted for the diagnosis (DSM 4 or DSM 5).

II. RELATED WORK

Some of the related works reviewed that are similar to this research are mentioned in this section. The first paper reviewed is our paper [8] titled "*A Survey on Software Applications use in Therapy for Autistic Children*", which we found out that most software applications used in therapy of Autistic children use pictures and some incorporate music. And over the years many have advanced in pictures and cards to human computer interaction, augmented reality and cloud computing as well. Second is a survey on using Assisted Technology for Autism Intervention by Jaliaawala and Khan[9]. Though methods such as Computer Vision Assisted technologies, Computer Aided systems and Virtual Reality have been used for the therapy of individuals on the Spectrum as mentioned in [8], there is still need for further research based Technologies to be developed to help individuals on the spectrum. They suggested a collaborated research with

the scientist and Clinicians so as to provide good performing systems.

Watson [10] also reviewed Computer Assisted Learning for individuals on the Spectrum, he reviewed how Computer Aided Learning has helped in both the therapy and Education of Children on the Spectrum. Other important feature in the research is the review on the design, implementation and Evaluation of the technologies. He concluded that there is no proper methodology used in developing these technologies and evaluating them [10]. Bartolome and Zapirain [11] also did a review on technologies as Support tool for Autistic Children, very few reviews are on Tools for Autism Diagnosis and Assessment.

One of the papers that review Autism Diagnosis/ Assessment tools is [12]. It reviewed Early Autism diagnosis tools based on their reliability, accessibility, efficiency and also tried to identify those that diagnose based on the new DSM 5 ASD criteria of diagnosis of 2013. In their research a total 37 tools were reviewed with very few of them considering the DSM 5 Criteria and most of them have low sensitivity, low specificity, not freely available for use and not very easy to use. They suggested more intelligent systems to be designed in the feature for diagnosis which should be available to both the parents, clinicians, caregivers and individuals on the spectrum.

The second paper reviewed on tools for screening is that of Marlow et al [2] which focused on screening tools for both Autism Spectrum disorder and Developmental delay in Infants and young children. Their review found out that only 6 ASD screening tools were developed specifically for use in low/medium income countries (LMIC) out of the 99 that were reviewed in the research though they only considered research papers published in English language so there might be a possibility of a few not included. This shows how the LMIC have limitation to ASD screening tools, there is need for researchers in these countries to build ones we can use especially in our country Nigeria where these tools are said to be limited for use in our health care centers[13][14] and also in Africa as a whole [15][16].

In a survey paper presented by Abu-nasser [5], he presented 33 experts systems developed for solving various health problems over years which are researched based on Artificial intelligence and expert system in particular [5]. While Bhandari et al [17] also reviewed some medical expert systems for diagnosis of various diseases, they considered the type of technology used for the development, the input as in the symptoms given to the system and also try to find out whether or not the system were evaluated after the development. Most of the expert system were rule based and Knowledge based technologies, very few used Artificial Neural Network (ANN), Fuzzy and neuro Fuzzy Technology.

The methodology adopted is to review related applications used for Autism diagnosis that are developed based on research. In this paper, we have also reviewed the technologies used for the development, the data used, the age range the expert system or mobile application can diagnose and the DSM criteria considered for the diagnosis.

III. Literature Review of Autism Diagnosis Expert System

This section presents the main work of this paper and the Table 1 below summarizes the whole work. All papers reviewed are arranged according to the years of Publication as shown in the table 1.

The first paper reviewed is titled "*Development of a diagnostic expert system for autism disorder*" by Sajjad et al [18].They developed a rule based expert system for Autism diagnosis where the user answers questions, the inference engine designed with prolog, no machine learning method was used, it uses DSM 4 criteria for diagnosis and the system was validated after the development. The system was developed for use in Pakistan which is why is named Pakistan Childhood Autism Diagnostic Expert System (PCADEX) and they used Autism Treatment Evaluation Checklist (ATEC) as the questionnaire of the system.

The second paper by Mahmoudi and Akbari-zardkhaneh [19], also developed an expert system named ASES (Autism Screening Expert System) which is also a rule based system for screening Autism of children between the ages of 2years -6 years, the knowledge based was developed from data collected after which machine learning methods (random forest and support vector machine) were used on the data, the system accuracy was measured and it was concluded to have a very good accuracy as compared to other systems in the literature.

The third paper we reviewed is titled "*A Belief Rule Based Expert System to Assess Autism under Uncertainty"*[20] by Alharbi et al. They also developed a rule based expert system for Autism diagnosis using the DSM 4 criteria and a Belief Rule-based inference methodology using the evidential reasoning approach (RIMER) was used because of the uncertainty of data collected. The system can be used to measure the state of the Autistic individual over time apart from making diagnosis and its validity has been tested and is said to perform better when compared to expert opinion and fuzzy based systems.

The next paper reviewed is titled "*Behavior Imaging solution, an innovative technology to enable remote autism diagnosis"* by Nazneen et al [21]. This application is named Naturalistic Observation Diagnosis Assessment (NODA) which is a solution for Diagnosing autism remotely by using home videos of a child. Two interfaces are said to be used for the procedure: One is the NODA smart capture used by parents

with specification for capturing the video. And the second is the NODA Connect which is the portal where clinicians can access the videos uploaded by parents to view and make assessment. No machine learning technology was involved in the development and in diagnosing, instead the clinician tags behaviors that are related to autism based on the DSM 5 criteria of diagnosis. Clinicians can ask parents for particular scenarios of videos to be uploaded as prescription. NODA was tested on few individuals who were previously diagnosed and 91% of accuracy was obtained.

In a paper by Cho et al titled "*A Quantitative Screening Approach to Autism Spectrum Disorders*"[22]. They presented a screening method named Gaze-Wasserstein which is a quantitative screening approach for diagnosing Autism Spectrum Disorders. It is a home based screening method that uses the front camera of a mobile device to measure the Gaze pattern of Individuals with ASD using the Wasserstein metric. K Nearest Neighbor (KNN)algorithm was used for classification and Leave One out Validation. A pilot study was conducted on few individuals with ASD and Non ASD and the method seems promising, cost effective and less time consuming for ASD diagnosis. The method is based on the DSM 5 criteria.

Another mobile device reviewed in this work is that of Bardhan et al [23] named Autism Barta. This is smart device based automated screening tool developed for diagnosis of Autism in Bangladesh. The MCHAT tool was translated in Bengali for screening Autism in children. This is similar to [24] which is also a mobile based tool but a Bengali version of Childhood Autism Spectrum Test (CAST). It is used for screening Autism for children of 16 to 30 months of Age. No machine learning methods was used.

"Aquabot" [25] is the only chatbot reviewed for Autism diagnosis by Mujeeb et al. This is a user friendly chatbot developed for diagnosis of Autism and Achluophobia. It is a rule based system and Decision tree algorithm was adopted for making fast and accurate decision. The system was tested and it achieved a good performance for both diagnoses. For the diagnosis of Autism, the system can diagnose individuals of different ages including adult. It's not clear the type of diagnosis criteria used in the work, Either DSM 4 or 5.

Tariq et al [26] also developed a mobile application which uses home videos for Autism detection. In their research work, 8 machine learning methods were used for identifying if an individual has Autism or not, DSM 5 diagnosis criteria was used for this research and the system is said to achieve an accuracy of greater than 90%. The mobile application can screen Autism in children between 1year to 17years.

Kanimozhiselvi [27] proposes machine learning algorithms as alternative technique for grading Autism and Diagnosis. Real life Childhood Autism Rating Scale (CARS) data were collected from a hospital for 100 individuals and 4 different machine learning algorithms (SVM, KNN, Naïve bayes and Decision Tree) were used for classifying the patients as having Severe, Moderate, Mild or No Autism. Out of the four algorithms, decision tree algorithm provides the greatest accuracy of 1.00 for training set and 0.96 for test set though there was no standard data set available for comparing apart from the local data set. This technique uses a DSM 5 criteria of diagnosis and data from Childhood Autism Rating Scale (CARS) which is a tool for Children not for Adults.

Thabtah [28] also developed an Autism screening application named ASD Test App. It is a mobile application developed for Screening/Diagnosis of Autism. It has 11 different languages that a user can choose from and can diagnose individuals of all ages. It consists of four different age range a user can choose which are the Toddler, Child, the adolescence and the Adult with different question suited for each age range. It was developed using the AQ10 questionnaire and has the ability to store data for feature analysis and research. Two machine learning algorithms were used on the data to test the accuracy and the efficiency of the application as feature analysis and they both gave high promising result.

Augmented Reality and Novel Virtual Sample Generation Algorithm Based Autism Diagnosis System [29] was developed by Weyden. This is a PhD Thesis that designed a new, friendly and improved Autism diagnosis tool that uses Augmented reality. This method is said to be a novel work that uses the upper limbs movement that is said to be child friendly for diagnosis. Real data sets were collected and used for this research. Deep neural networks were used for the classification.

Wingfield et al [30] developed a model for predicting Autism which will model for pediatric autism screening easier. Data was collected using Pictorial Autism Assessment Schedule (PAAS). Several experiments to developed the model were conducted using WEKA with six machine learning algorithms so as to find which embedded on the application for Autism diagnosis which uses the PAAS questionnaire as questions. Feature selection test was also conducted on the data obtained to find the features in PAAS that best describes individual with ASD. Random forest was chosen to be the best classifier to be embedded on the application for Autism Diagnosis which uses the PAAS questionnaire as a question.

Satu et al in a paper titled *"A Smart Phone Based Mobile Application to Detect Autism of Children in Bangladesh*" [24] developed a mobile application for screening Autism named Prottoy. This application performs best in predicting ASD. The application can be used for screening Autism in children for Ages 3 to 11 years based on DSM 5 criteria of Diagnosis. The application is in Bengali language, so it can only be used in Bangladesh. Pictures were used for demonstration of conditions for easy use and understanding. The application has a database for storing the information recorded by a user and no machine learning method was said to be used.

TABLE 1. SUMMARY OF LITERATURE REVIEW

S/No	Paper	DSM 4 / DSM 5	Country developed For	Age Diagnosis (in years)	Machine learning uses (Yes/No)	Questionnaire used	Data used
1	[18]	DSM 4	Pakistan	5-12	No	ATEC	Nil
2	[19]	DSM 4	Iran	2 - 6	Yes	238 questions.	170 parents
3	[20]	DSM 4	Bangladesh	Nil	No	Nil	Few
4	[21]	DSM 5	N/A	2-6	No	Nil	5 Families
5	[22]	DSM 5		2-10	Yes	ADOS	32 participants
6	[23]	-	Bangladesh	18-30 months	No	M-CHAT	Nil
7	[25]	N/A	N/A	1-7	Yes	Nil	40 participant
8	[26]	DSM 5	N/A	1 – 17	Yes	Nil	193 videos
9	[27]	DSM 5	N/A	Nil	Yes	CARS	100 instances
10	[28]	DSM 5	N/A	For all ages	Yes	AQ10	Over 1400 instances
11	[29]	-	N/A	Children	Yes	Nil	30 Instances
12	[30]	DSM 5	Sri Lanka	N/A	Yes	PAAS checklist	228 Instances
13	[24]	DSM 5	Bangladesh	3-11	No	CAST	Nil

IV. CONCLUSION

In this paper, we did a literature review on some expert systems and mobile applications developed based on research for Autism Diagnosis and screening. From our review we were able to find out that most of the expert system was developed to diagnose based on DSM 5[21][22][26][27][28][30][24]which shows that researchers have adopted the recent diagnosis criteria in developing diagnosis tools. Most of the Expert system used rule based technology for their knowledge base and have given good accuracy[18][20][19]. Machine learning methods were also used in most of the development of the tools as shown in table 1 for proper identification of individuals with Autism from normal ones, but none has used the machine learning for ASD classification into sub classes based on the DSM 5 criteria. Most of the diagnosis was built for diagnosing of children, only [26] and [28] for individuals older than 17years of age. We have also seen that most of the tools/applications were based on existing Autism screening tools and questionnaire, different questionnaires were used as shown in table 1 and some applications are just translated to other languages such as [23][24]. And most of the screening tools that were translated are translated to be used for low medium income countries like Bangladesh and Sri lanka and even the tools developed are most for those counties so as to make Autism Screening and diagnosis easier[18][19][20][23][30][24].

Therefore, we conclude that most computer Aided tools fall into two broad categories [30], which is either automating an existing paper based screening tolls or by using Augmented reality where home videos of individuals were used for the assessment. Secondly there is need to develop tools that will not only make diagnosis as a child having autism but also to be able to identify the level of Autism present. Thirdly, most researches were conducted using few data , these shows that there is need for developing applications for data collection as seen in [28]and [24]. And lastly, there is also need for researchers to develop a screening or diagnostic tool for some of our major languages here in Nigeria too as to make screening much easier and faster.

REFERENCES

[1] B. Tonge and A. Brereton, “AUTISM : ASSESSMENT AND DIAGNOSIS,” , www.med.monash.edu.au/spppm/research/devpsych/actnow, pp. 1–3, 2011.

[2] M. Marlow, C. Servili, and M. Tomlinson, “A review of screening tools for the identification of autism spectrum disorders and developmental delay in infants and young children: recommendations for use in low- and middle-income countries,” *Autism Reshearch.*, vol. 12, no. 2, pp. 176–199, 2019.

[3] S. L. Hyman, S. E. Levy, S. M. Myers, O. N. Children, and W. Disabilities, “Identification , Evaluation , and Management of Children With Autism Spectrum Disorder,” American Academy of Pediatrics, vol. 145, no. 1, 2020.

[4] K. Makhubele, “A Knowledge Based Exper System for Medical Advice provision”, University of Cape Town, Department of Computer Science, 2012.

[5] B. S. Abu-nasser, “Medical Expert Systems Survey” , HAL Id : hal-01610722,” vol. 1, no. 7, pp. 218–224, 2017.

[6] M. Curran, “Can a computer expert system aid the process of clinical decision-making in podiatry?”, Thesis, University of Northampton, 2005.

[7] A. K. Meena and S. Kumar, “Review : Use of Expert System in Medical Science”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 10, pp. 371–373, 2015.

[8] A. S. Adamu, S. E. Abdullahi, and R. K. Aminu, “A survey on software applications use in therapy for autistic children,” *2019 15th Inernational. Conference Electronics Computer Computation, ICECCO 2019*, pp. 1–4, 2019.

[9] M. S. Jaliaawala and R. A. Khan, “Can autism be catered with artificial intelligence-assisted intervention technology? A comprehensive survey,” *Artificial Intelligence Review*, 2019.

[10] S. Fletcher-Watson, “A Targeted Review of Computer-Assisted Learning for People with Autism Spectrum Disorder: Towards a Consistent Methodology,” *Review Journal Autism Developmental*

Disorders, vol. 1, no. 2, pp. 87–100, 2014.
[11] N. Aresti-Bartolome and B. Garcia-Zapirain, "Technologies as support tools for persons with autistic spectrum disorder: A systematic review," *International Journal of Environmental Reshearch and Public Health*, vol. 11, no. 8, pp. 7767–7802, 2014.
[12] F. Thabtah and D. Peebles, "Early Autism Screening: A Comprehensive Review," *Int. J. Environ. Res. Public Health*, vol. 16, no. 18, 2019.
[13] F. A. Lesi, J. D. Adeyemi, O. F. Aina, Y. O. Oshodi, O. Yewande, C. S Umeh, A. T. Olagunju and O. Wellington., "Autism in Nigeria: A call for action," *Journal of clinical Sciences*, vol. 11, no. 2, p. 33, 2014.
[14] E. E. Eseigbe, F. T. Nuhu, T. L. Sheikh, P. Eseigbe, K. A. Sanni, and V. O. Olisah, "Knowledge of Childhood Autism and Challenges of Management among Medical Doctors in Kaduna State, Northwest Nigeria," *Autism Research and Treatment*, vol. 2015, Article ID 892301, pp. 1–6, 2015.
[15] M. M. Ahmad,h. Ahmed, J. Baba, J. F. Legbo, A. M. Nauzo, M.Omar and A. A. Tahir, "Autism Spectrum Disorder in North-Western Nigeria," *International Neuropsychiatric Disease Journal*, vol. 12, no. 2, pp. 1–5, 2019.
[16] M. Bakare and K. Munir, "Autism spectrum disorders (ASD) in Africa: a perspective," *African journal of Psychiatry*, vol. 14, no. 3, 2011.
[17] J. Singla Asst, D. Grover, and A. Bhandari Asst, "Medical Expert Systems for Diagnosis of Various Diseases," *International Journal of Computer Applications*, vol. 93, no. 7, pp. 975–8887, 2014.
[18] S. Sajjad, H. Qamar, K. Tariq, and S. Bano, "Development of a diagnostic expert system for autism disorder-PCADEX," *Proc. 2011 International Conference Artificial Intelligence, ICAI 2011*, vol. 2, no. May, pp. 934–938, 2011.
[19] M. Mahmoudi and S. Akbari-zardkhaneh, "Developing Autism Screening Expert System (ASES) " AWERProcedia Information Technology & Computer Science, January 2013.
[20] S. Alharbi, M. Hossain, and A. Ahmed, "A Belief Rule Based Expert System to Assess Autism under Uncertainty," *Proceedings of the world Congress on Engineering and Computer Science 2015*, vol. 41, no. 3, pp. 21–23, 2015.
[21] N. Nazneen, A. Rozga, G. D. Abowd, C. J. Smith, R. Oberleitner, R. I.Arriaga and J. S. Suri, "Chapter 16 Behavior Imaging®," *Autism Imaging and Devices*, pp. 345–354, 2016.
[22] K. Cho, F. Lin, C. Song, X. Xu, M. Hartley-McAndrew, K. Doody and W. Xu, "Gaze-Wasserstein: A quantitative screening approach to autism spectrum disorders," *2016 IEEE Wirel. Heal. WH 2016*, pp. 14–21, 2016.
[23] S. Bardhan, G. Mridha, E. Ahmed, M. Ullah, H. Ahmed, S. Akhter, M. Rabbani and K. Mamun, "Autism Barta - A smart device based automated autism screening tool for Bangladesh," *2016 5th International Conference Informatics, Electronics and Vision, ICIEV 2016*, pp. 602–607, 2016.
[24] M. Satu, M. Azad, M. Haque, S. Imtiaz, T. Akter, L. Barua, M. Rashid, T. Soron and K. Al Mamun., "Prottoy: A Smart Phone Based Mobile Application to Detect Autism of Children in Bangladesh," , 4th International Conference on Electrical Information and Communication Technology, pp. 1–6, 2020.
[25] S. Mujeeb, M. Hafeez, and T. Arshad, "Aquabot: A Diagnostic Chatbot for Achluophobia and Autism," *International Journal of Advance Computer Science snd applications.*, vol. 8, no. 9, pp. 209–216, 2017.
[26] Q. Tariq, J. Daniels, J. Schwartz, P. Washington, H. Kalantarian, and D. Wall, "Mobile detection of autism through machine learning on home video: A development and prospective validation study," *PLoS Medicine*, vol. 15, no. 11, pp. 1–20, 2018.
[27] C. S. Kanimozhiselvi, D. Jayaprakash and K. Kalaivani, "Grading Autism Children Using Machine Learning Techniques," *International Journal of Applied Engineering Research*, vol. 14, no. 5, pp. 1186–1188, 2019.
[28] F. Thabtah, "An accessible and efficient autism screening method for behavioural data and predictive analyses," *Health Informatics Journal*, vol. 25, no. 4, pp. 1739–1755, 2019.
[29] M. Wedyanl, "Augmented Reality and Novel Virtual Sample Generation Algorithm Based Autism Diagnosis System ", University of Technology Sydney, Faculty of Engineering and Information Technology, Thesis, April, 2020.
[30] B. Wingfield, S. Miller, P. Yogarajah, D. Kerr, B. Gardiner, S. Seneviratne, P. Samarasinghe and S. Coleman, "A predictive model for paediatric autism screening," *Health Informatics Journal*, 2020.

An Enhanced Active Power Control Technique for Interference Mitigation in 5G Uplink Macro-Femto Cellular Network

Katfun Philemon Dawar
Telecommunication Engineering,
Federal University of Technology,
Minna, Nigeria.
dawar.pg918557@st.futminna.edu.ng

Usman Abraham Usman
Telecommunication Engineering,
Federal University of Technology,
Minna, Nigeria.
usman.abraham@futminna.edu.ng

Bala Alhaji Salihu
Telecommunication Engineering,
Federal University of Technology,
Minna, Nigeria.
salbala@futminna.edu.ng

Abstract— Macro-femto heterogeneous network (HetNet) comes with tremendous inter and intra cell interference problem. This paper considered fifth generation (5G) non-stand-alone (NSA) archtecture. We proposed an enhanced active power control technique (EAPC) to mitigate interference in uplink macro-femto HetNet. The MATLAB simulation result obtained in terms of average power consumption of macrocell user equipment (MUE) and femtocell user equipment (HUE) using EAPC technique stood at 6.7 dBm and 7.5 dBm respectively, as against that of active power control (APC), fixed power control (FPC) and power control 1 (PC1); which stood at 10.9 dBm, 23.0 dBm, 14.8 dBm for MUE and 11.1 dBm, 23.0 dBm, 14.8 dBm for HUE respectively. It indicates that HUE and MUE using EAPC technique had low average power consumption when benchmark. 5G NSA macrocell base station (en-gNB), 60% cumulative distributive function (CDF) of throughput based on EAPC, APC, PC1 and FPC techniques had 36.2 Mbps, 15.0 Mbps, 24.0 Mbps and 12.5 Mbps throughput respectively. And that of femtocell base station (Hen-gNB) according to EAPC, APC, PC1 and FPC was 25.0 Mbps, 23.0 Mbps, 10.0 Mbps and 18.6 Mbps throughout respectively. This implies that EAPC has better Hen-gNB and en-gNB throughput when benchmark with other related techniques. Hence, the proposed EAPC technique improves 5G network performance in terms of better throughput and conserving limited user equipment (UE) energy.

Keywords—Heterogeneous Network, Femtocell Network; Inter-cell Interference; Throughput; and Average Power Consumption

I. INTRODUCTION

The population and the yearning of subscribers for voice and data services is increasing exponentially, with most of them located in offices and homes. The situation is more worrisome with the shift from the normal way of life to the new normal occasioned by corona virus disease. The new normal brought about more people inclusiveness in digitized business, telemedicine, virtual meetings, seminars and conferences, among other; which further increase the demand for qualitative cellular network service. The indoor mobile user's traffics comprise of 30% voice traffic and 70% data traffic as in [1], [2], and [3]. Ericsson mobility predicted that by 2021 there will be 9 billion mobile broadband subscriptions, 20% increase in smartphone data traffic and 25% video traffic increase as in [4]. This increase in network demand calls for a more robust and efficient network.

The cost of mounting several outdoor base stations by network operators to meet up with subscriber's needs for high throughput and large network cell coverage is a challenge in homogeneous macrocell network. This necessitate the use of low power base stations as an overlaid on existing macrocells to form a heterogeneous network (HetNet), to achieve wider coverage, higher efficiency and enhanced throughput in cellular network as in [5], and [6]. 5G ultra dense network (UDN) was designed to increase throughput and spectrum efficiency of the network to accommodate more subscribers and reduced power consumption as in [7]. This can be achieve by depopulating the densely populated macrocell network using small cell (Femto) nodes and further reducing interference in the HetNet.

Femtocell being a plug and play base station is usually installed by subscribers without taking into cognizance its cell coverage radius or other nearby cells, resulting into cell overlap which increases inter-cell interference (ICI). This interference issue is considered as the major technical challenge associated with femtocell deployment on an existing macrocell layer as in [8], [9], and [10].

II. LITERATURE REVIEW

A. Related Power Control Techniques

Power is a critical resource in mobile networks, hence the need for its control. When power is mismanaged, it result into wastage, interference, high latency and drop calls. Transmitting with just enough power to maintain the required quality of service ensures minimal interference.

A.1. Power Control 1Technique

Dynamic power control technique (PC1) for mitigating interference, adjusted the transmit power of user equipment's (UEs) based on measurements from the surrounding as seen in [11]. The power control adjustment is centered on the difference (γ), between measured signal-to-interference-plus-noise ratio ($SINR_{measured}$) and target SINR ($SINR_{target}$) as expressed mathematically in (1) $\gamma = SINR_{measured} - SINR_{target}$ (1)

When the $SINR_{measured}$ is less than $SINR_{target}$, the present transmit power of user equipment (UE) will increase in the next transmission by constant power value of 2 dB, but when $SINR_{measured}$ is greater than $SINR_{target}$, the present transmit power of the UE will be decrease by same constant power value of 2 dB in the next transmission. And If the $SINR_{measured}$ is equals to $SINR_{target}$, the present UE transmit power will be maintained in the next transmission. Mathematically, PC1 transmit power adjustment is expressed in (2).

$$P_{tx} = \begin{cases} \min\left[P_{tx}(t_j) + \Delta, P_{max}\right]; & \gamma < 0 \\ P_{tx}(t_j); & \gamma = 0 \\ \max\left[P_{tx}(t_j) - \Delta, P_{min}\right]; & \gamma > 0 \end{cases} \quad (2)$$

where P_{tx} is the next transmit power, $P_{tx}(t_j)$ is the present transmit power, Δ is the constant power value, P_{min} is the minimum transmit power, and P_{max} is the maximum transmit power.

A.2. Active Power Control Technique

An active power control (APC) technique for interference management, adjusted the transmit power of aggressor (AG) based on interference message (IM) as captured in [6]. The victim (VT) computes the interference indication function (IDF) and determine whether to send an IM or not. When the computed IDF is greater than the set threshold interference, the VT sends an IM including the AG information to its transmitter, which then uses the backhaul and forward the IM to the AG indicating interference in the network, otherwise it does not send an IM. Equation (3) presents the mathematical equation for computing IDF, and (4) express when an IM is or is not sent.

$$I_i = P_t^i \psi_i (R_i)^{-\beta} \quad (3)$$

$$x_i = \begin{cases} 0, & I_i \leq I_{Threshold} \\ 1 & otherwise \end{cases} \quad (4)$$

where P_t^i is the transmit power, ψ represents log – normal shadowing, R is the distance between the transmitter and receiver, β is the pathloss component for the indoor transmission and I_i is the IDF. In (4), $I_{Threshold}$ is the set interference threshold. x_i stands for IM, when x_i = 0, it implies there is no interference and IM is not sent, and when x_i = 1, it implies there is interference and IM is sent.

The APC technique basically has two power adjustment stages: the first stage, set three transmit power (P_x, P_y, P_z) and two time levels (TL_1, TL_2). They set P_x as the maximum transmit powers, followed by P_y and lastly P_z as minimum transmit powers. When an IM is received, the APC power adjustment activates, and the transmit power of the AG is reduced from say P_x to P_y by constant down power value (Δ_{down}). If the same AG receives another IM within the first time level (TL_1), it would not further reduce its AG power to P_z level until TL_1 expires. Similarly, when the AG has no IM and TL_1 expires, then the second time level (TL_2) starts and the transmission power level increases from P_y to P_x by constant up power value (Δ_{up}). Δ_{down} and Δ_{up} are fixed power value of -2 dB and 2 dB respectively. The transmit power adjustment is mathematically expressed in (5) – (9).

$P_t = P_x$ No IM (5)

$P_t = P_y = P_x - \Delta_{down}$ IM and TL_1 starts (6)

$P_t = P_z = P_y - \Delta_{down}$ New IM and TL_1 starts (7)

$P_t = P_y = P_z + \Delta_{up}$ No IM and TL_2 start (8)

$P_t = P_x = P_y + \Delta_{up}$ No I and TL_2 running (9)

The second stage of active power control technique shapes the first stage APC transmit power based on the minimum required quality of service (QoS) of signal received. The

mathematical computation of QoS Indication Function (QIF) is expressed in (10)

$$QIF = \frac{P_{uref}\tau_{HUE}}{minRSRP_j} \quad (10)$$

where τ_{HUE} is the minimum required SINR for user equipment, P_{uref} is the uplink reference signal transmit power and $minRSRP_j$ is the minimum reference signal received power. The second and final stage of APC transmit power adjustment is given mathematically in (11).

$$P_{APc} = \max(P_{min}\, min(QIF * P_t, P_{max})) \quad (11)$$

where P_{min} and P_{max} are minimum and maximum transmit power respectively.

B. Attenuation Factor Model

This propagation model was described by Siedel, which considered the effects of building type and obstacles as in [12]. The attenuation factor model equation is given in (12) and pathloss exponent of different environments is captured in Table 1.

$$[P_L(d)]dB = [P_L(d_o)]dB + 10nlog_{10}(\frac{d}{d_o}) + faf \quad (12)$$

where $P_L(d)$ is log-distance pathloss from transmitter to receiver, $P_L(d_o)$ is free space pathloss, n is pathloss exponent, $d_0$stand for reference distance, d is the distance between transmitter and receiver, and faf is floor attenuation factor.

Table 1. Pathloss exponent of different environments

S/N	Environment	Path loss exponent *n*
1.	Free space	2
2.	Urban area cellular radio	2.7 - 3.5
3.	Shadowed urban cellular radio	3 – 5
4.	In building line-of-sight	1.6 - 1.8
5.	Obstructed in building	4 – 6
6.	Obstructed in factories	2 – 3

(Source: [12])

C. Signal to Interference Plus Noise Ratio (SINR)

en-gNB SINR and Hen-gNB SINR is calculated using (15) and (16) as presented in [11].

$$SINR_{en-gNB} = \frac{P_{MUE}PL_{MUE-en-gNB}}{\sum_M P_M^k PL_M + \sum_F P_F^k PL_F + P_n} \quad (15)$$

$$SINR_{Hen-gNB} = \frac{P_{HUE}PL_{HUE-Hen-gNB}}{\sum_M P_M^k PL_M + \sum_F P_F^k PL_F + P_n} \quad (16)$$

where P_{MUE} and P_{HUE} are the transmit power by macro user equipment (MUE) and home user equipment (HUE) respectively. $PL_{MUE-en-gNB}$ and $PL_{HUE-Hen-gNB}$ are propagation pathloss within; MUE and en-gNB, and HUE and Hen-gNB respectively. $\sum_M P_M^k PL_M$ is the sum product of interfering MUE transmit power and its propagation pathloss. $\sum_F P_F^k PL_F$ is the sum product of interfering HUE transmit power and its propagation pathloss. P_n is the thermal noise density.

D. Network Throughput

The throughput of the network is computed using Shannon-Hartley equation for throughput, given in (17)

$$c = Blog_2(1 + SINR_{Base\ station}) \quad (17)$$

where c is network throughput, B is system bandwidth, and $SINR_{Base\ station}$ is SINR of base station.

Average throughput of Hen-gNB, en-gNB and total throughput of the entire femto– macro network is obtained using equations (18), (19) and (20) respectively, as in [13].

$$c_{Hen-gNB}^{Avg} = \frac{\sum_{i=1}^{n} C_{Hen-gNB}}{N_{Hen-gNB}} \quad (18)$$

$$c_{en-gNB}^{Avg} = \frac{\sum_{i=1}^{n} C_{en-gNB}}{N_{en-gNB}} \quad (19)$$

$$c_{overall} = \frac{(N_{en-gNB} \times c_{en-gNB}^{Avg}) + (N_{Hen-gNB} \times c_{Hen-gNB}^{Avg})}{(N_{en-gNB} + N_{Hen-gNB})} \quad (20)$$

where $\sum_{i=1}^{n} C_{en-gNB}$ stand for sum of all en-gNB throughput, $\sum_{i=1}^{n} C_{Hen-gNB}$ for sum of all Hen-gNB throughput, while N_{en-gNB} and $N_{Hen-gNB}$ stands for number of en-gNB and Hen-gNB respectively in the HetNet.

III. SYSTEM DESCRIPTION AND MODEL

The system architecture in this paper captures an inter-cell interference (ICI) scenario between and within the primary and secondary system. The HetNet has one macrocell (primary system) and two overlaid femtocells (secondary system). Worst case scenario of interference in macro-femto HetNet occasioned by femtocell closed access mode, co-tier and cross-tier interference, and co-channel deployment is considered in this research. Fig. 1 present the system architecture considered in this work

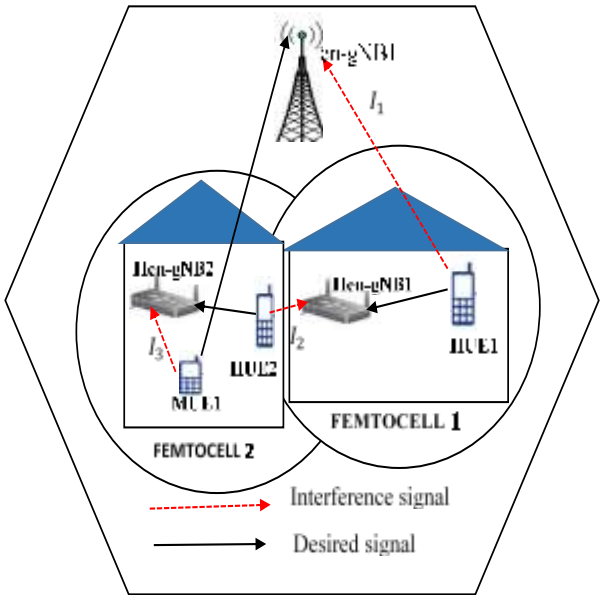


Fig. 1. System Architecture

The NSA 5G macrocell base station, called logical Node B is denoted as en-gNB and NSA 5G femtocell base station is denoted as Hen-gNB in accordance to NSA 5G system architecture presented in 3GPP standard release 15 [14]. Considering closed access mode configuration, MUE1 is not registered on Hen-gNB2 and cannot access its services; even though located close. The uplink signal from MUE1 is received as uplink cross-tier interference by Hen-gNB2. HUE1 uplink transmission is received by en-gNB as uplink cross-tier interference. Hen-gNB1 receives uplink transmission signal from HUE2 as uplink co-tier interference. In the proposed system architecture, I_1 represents uplink cross-tier interference, where en-gNB is the VT and HUE1 is the AG. I_2 is an uplink co-tier interference, where HUE2 is the AG and Hen-gNB1 is the VT. I_3 is an uplink cross-tier interference where MUE1 is the AG and Hen-gNB2 is the VT.

3.1 Pathloss Model

The proposed enhanced active power control (EAPC) technique uses pathloss model in (13) and (14) for uplink transmission from MUEs and HUEs respectively. The pathloss model ($PL_{UEs-base\ station}$) in (14) is an extension of attenuation factor model, where an obstructed building pathloss exponent of 6 and faf through one floor of 16.2 dB is used [12]. While the propagation pathloss model from MUE to base station (indoor and outdoor) in (13) is according to 3GPP LTE-Advanced pathloss model for urban deployments as in [15].

$$PL_{MUE-base\ station}(dB) = \begin{cases} 15.3 + 37.log(R1) + l_p & (Indoor) \\ 15.3 + 37.log(R1) & (outdoor) \end{cases} \quad (13)$$

$$PL_{UEs-base\ station}(dB) = -log\left(c/f * 4\pi * d_0\right)^2 + 60log\left(d/d_0\right) + 16.2 \quad (14)$$

In (13) $PL_{MUE-base\ station}$ is pathloss from MUE to base station, $R1$ is distance between MUE and base station, and l_p is penetration loss. In (14) $PL_{UEs-base\ station}$ is the pathloss from UE to base station, c is speed of light, f is transmit frequency in MHz, d_0 is a reference distance, and d is the distance between transmitter and receiver.

IV. PROPOSED ENHANCED ACTIVE POWER CONTROL TECHNIQUE

The EAPC technique is described using a flowchart presented in Fig. 2

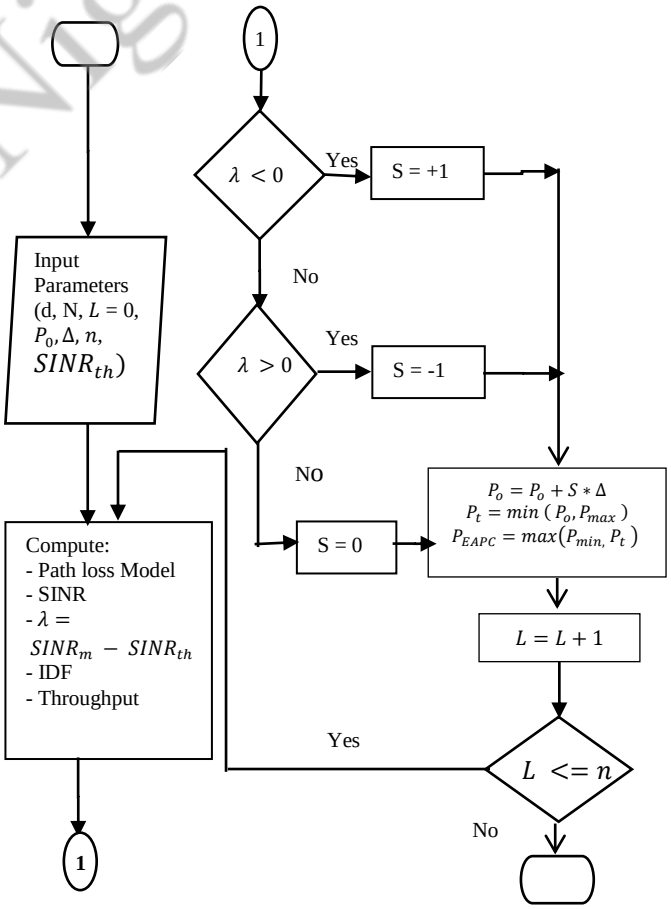


Fig. 2. EAPC flowchart

where input parameters d, N, L, $P_0, \Delta, n, SINR_{th}$ stands for initial distance between transmitter and receiver, thermal

noise density, initial loop number, initial transmit power, constant power value, final loop number, and threshold SINR respectively. $SINR_m$ stands for measured $SINR$, λ is the difference between $SINR_m$ and $SINR_{th}$ ($\lambda = SINR_m - SINR_{th}$), S for adjustment parameter, P_{max} for maximum transmit power of UEs, and P_{min} for minimum transmit power of UEs. P_{EAPC} is the enhanced active power control transmit power use for next transmission for set time duration (Tf_1) of 200 ms after which the system start all over again to determine the next transmit power. Target SINR of 10 [6] was used.

The uplink transmission power of MUE and HUEs is measured alongside their respective propagation pathloss. The transmit power of the MUEs, HUE and their computed propagation losses is used to calculate SINRs. If λ is greater than zero the present UE transmit power will be reduce by constant power value for the next transmission; when it is less than zero, the present UE transmit power will be increase by same constant power value for the next transmission and when it is equal to zero, the present UE transmit power will be maintain for the next transmission.

V. NOVELTY OF WORK

EAPC used a different femtocell pathloss model that captures more real life scenarios and reduce losses in the system. It used a constant power value of 0.5 dB in adjusting UEs transmit power for minimal power consumption; as against 2 dB used by APC and PC1. EAPC when compared to APC technique has a less complex means of determining when to adjust UEs transmit power; and it adjust the transmit power UE serving the VT, whereas APC adjust the particular transmit power of AG.

VI. Simulation Parameters, Results and Discussion

The simulation and result was obtained with the help of research system architecture and parameters sourced from ([6]; [11]; and [16]) and presented in Table 2.

Table 2. Uplink Simulation Parameters

No.	Parameter	Value
1.	Maximum transmit power of HUE and MUE	23 dBm
2.	Minimum transmit power of HUE and MUE	0 dBm
3.	Initial transmit power of HUE and MUE	5 dBm
4.	System bandwidth	10 MHz
6.	Carrier frequency	2.57 GHz
7.	Thermal noise	-174 dBm

The performance of the proposed technique is compared with three other related techniques, in terms of network throughput and average power consumption. Fig. 3 shows the average power used by MUE in communicating to en-gNB, considering ten transmissions at different time instances.

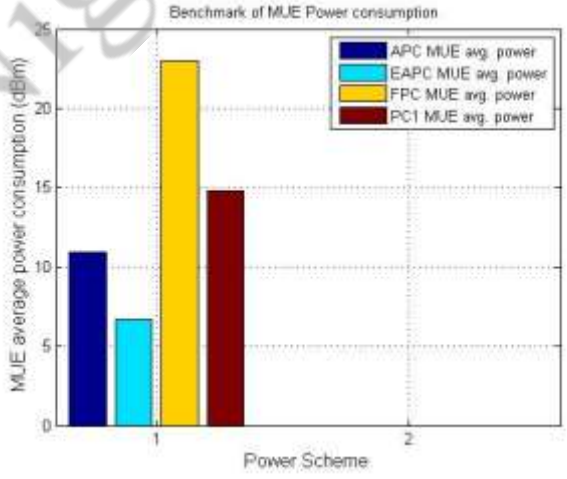


Fig. 3. Benchmark of MUE Average Power Consumption

The MUE average power consumption using APC, EAPC, FPC and PC1 power control techniques stood at 10.9 dBm, 6.7 dBm, 23.0 dBm and 14.8 dBm respectively. This indicates that EAPC technique has the lowest average power consumption followed by APC, then PC1, and lastly FPC.

Fig. 4 presents an average power consumption of HUE techniques, when transmitting to UEs.

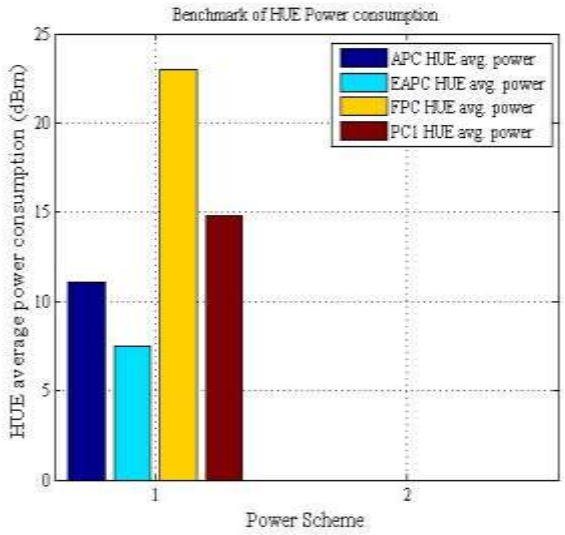


Fig. 4. Benchmark of HUE Average Consumption Power

The average consumption of HUE using APC, EAPC, FPC and PC1 power control techniques was 11.1 dBm, 7.5 dBm, 23.0 dBm and 14.8 dBm respectively. Again, EAPC has the lowest power consumption and FPC has the highest average power consumption.

Fig. 5 presentss uplink cdf of Heng-NB throughput

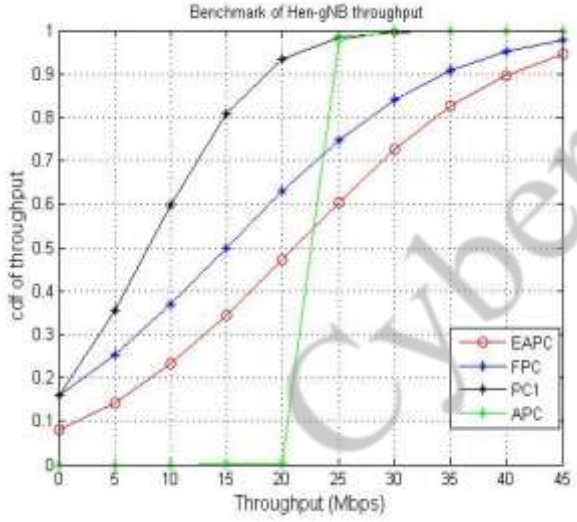


Fig. 5. Throughput of Hen-gNB

From the Hen-gNB throughput result obtained, the proposed EAPC technique at 0.6 or 60% cdf of throughput had 25.0 Mbps, while APC, PC1 and FPC had throughputs of 23.0 Mbps, 10.0 Mbps, and 18.6 Mbps respectively.

Fig.6 presents the result of uplink cdf of MUE throughput.

Fig. 6. Benchmark of en-gNB throughput

The en-gNB throughput result pointed out that the proposed EAPC at 0.6 or 60% cdf of throughput had 36.2 Mbps throughput; while FPC, PC1 and APC had 12.5 Mbps, 24.0 Mbps, and 15.0 Mbps throughput respectively.

VII. CONCLUSION

This research considered uplink transmission of macro–femto HetNet. The network simulation in MATLAB environment was guided by the research system architecture and simulation parameters, where worst case scenarios of co-channel and femtocell closed access mode deployment were employed. The proposed technique was analyzed and its performance benchmarked, as presented in figure 2 – 5. The result indicated that EAPC has the least MUE average power consumption of 6.7 dBm, and also least HUE average power consumption of 7.5 dBm.

EAPC at 60% cdf has the highest en-gNB throughput of 36.2 Mbps and highest Hen-gNB throughput of 25.0 Mbps. This implies that EAPC technique gives higher en-gNB and Hen-gNB throughput; and conserves UEs limited power in macro-femto HetNet.

VIII. REFERENCES

[1] T. Priya, and H. Seema, "Cognitive Femtocell Network Various Challenges and Security Issues," in *International Conference on Computing Methodologies and Communication* (ICCMC), 2017, pp 1-5.

[2] C. Onu,, B.A. Salihu, and J. Abolarinwa, "Enhanced Fractional Frequency Reuse in Lte-A Heterogeneous OFDMA Network," ATBU, *Journal of Science, Technology and Education (JOSTE*), vol. 6, issue 2, pp 18 – 27, Jun 2018.

[3] I. Aneeqa, A.H. Syed, and N. Dushantha, "A Multiple Region Reverse Frequency Allocation Technique for Uplink Throughput Enhancement in 5G HetNets," in *IEEE Annual Consumer Communications and Networking Conference (CCNC),* 2017, pp 905 – 909.

[4] S.A. Khan, M. Asshad, and A. Kavak, "A Power Control Algorithm and Software Tool for Femtocells in LTE-A Network," *Sakarya University Journal of Science*, vol. 22, issue 4, pp 1124-1129, Aug 2018.

[5] A. Adejo, J. Hussein, and S. Boussakta, "Interference Modelling for Soft Frequency Reuse in Irregular Heterogeneous Cellular Networks," in *International Conference on Ubiquitous and Future Networks (ICUFN),* 2017, pp 381 -386.

[6] T. U. Hassan, and F. Gao, "An Active Power Control Technique for Downlink Interference Management in a Two-Tier Macro–Femto Network," *Journal of Sensors*, Vol. 19, issue 9, pp 2015 – 2022, Jan 2019.

[7] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 18, issue 3, pp 1617 – 1655, Feb 2016.

[8] M. Al-omari, A.R. Ramli, A. Sali, and R. S. Azmir, "A Femtocell Cross-Tier Interference Mitigation Technique in OFDMA-LTE System: A Cuckoo Search based Approach,*" Indian Journal of Science and Technology*, vol. 9, issue 2, pp 1-12, Jan 2016.

[9] R. Farah, R. Asif, and A, Khaizuran, "Advanced Inter-cell Interference Management Technologies in 5G Wireless Heterogeneous Networks (HetNets)," in *IEEE Student Conference on Research and Development (SCOReD),* vol. 15 issue 3, 2016, pp 2170 – 2182.

[10] G. Mohammad, V. Gobi, G. Elias, M. M. Soheil, "Throughput Improvement in 5G Networks Using Femtocell, in Wireless Personal Communications," 2019, vol. 105, issue 2, pp 123 – 2134.

[11] M. Susanto, R. Hutabarat, Y. Yuniati, and S. Alam, "Interference Management using power control for uplink transmission in femtocell-macrocell cellular communication network," in International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering, 2017, vol. 15 issue 2, pp 245 - 250.

[12] T.S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. New Jersey: Prentice Hall PTR, 1996.

[13] O. Adeyemo, M. Dlodlo, and H. Ohize, "Mitigating Cross-Tier Cross-Boundary Interference in Fractional Frequency Reuse Technique for Multi-Tier Networks," *AFRICON (IEEE),* vol. 10, issue 2, pp 1 - 6, Sep 2015.

[14] 3rd Generation Partnership Project (3GPP) TR 21.915 V15.00 (September, 2019). *Technical Specification Group Services and System Aspects;* Release 15 Description; Summary of Rel-15 Work Items

[15] 3rd Generation Partnership Project (3GPP) TR 36.942 version 11.0.0 LTE Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Frequency (RF) System Scenarios.

[16] 3rd Generation Partnership Project (3GPP) TS 38.104 version 15.3.0 Release 15. 5G; NR; Base Station (BS) radio transmission and reception

Face Recognition with Particle Swarm Optimization (PSO) and Support Vector Machine (SVM)

Abubakar Ibrahim MUHAMMAD
Electronics & Comm. Engr. Department
Rimt University Punjab India
ibngarko@yahoo.com

R.P. SINGH
Dept of Research, Innovation & Incubation
Rimt University Punjab India
rpmgg31@gmail.com

Yusuf IBRAHIM
Computer Engineering Department
Ahmadu Bello University, Zaria
yusuf2007ee@gmail.com

***Abstract*— Every day challenges are increasingly progressing in the modern world of today. Finding the identity of an individual becomes compulsory in our societies. Therefore a means for identifying and detecting one face becomes necessary and even compulsory. Facial recognition problem is among the top vital issues that today's attention has been focused, the need to identify faces in almost every sectors like in military, education, commence and etc. become the work of engineers or scientist to see all effort are put together in order to obtained better accuracy of theses facial recognition models . Algorithms deployed in the field of facial recognition research area, do not give better or optimal performances. Then the use of means like optimization becomes necessary even within the selected or desired classification method. In this research, Local Binary Pattern (LBP) was used for feature extraction while Support Vector Machines (SVM) was used as a classifier. However, it is important to find good values of the SVM hyper parameters C and γ in order to obtain good results. Particle Swarm Optimization (PSO) is proposed to optimize and choose the best SVM hyper parameters. Results obtained using the LBP-PSO-SVM pipeline gave a [C, γ], a mean-squared-error of 0.028571 and an overall best accuracy of 98.33%. Framework carried out in this research worked better than the use of SVM alone, having less complexity with less time of implementation**

Keywords —face recognition, particle swarm optimization, Support Vector Machine

I. INTRODUCTION

Face recognition application being the most concerned research area of interest in today's world advance technology. Because of the vital role it plays in almost every sectors like security, education, business and so on, verifying and detecting the correct object either in an image or video steam become necessarily important to solve problems. Almost all the type of Algorithms deployed or used in the process of classification problem in face recognition research area, does not give 100% accuracy. Therefore it is because of these hindrances all research areas developed in this sectors need a more attention to make a better ways for enhancing the technology of facial recognition.

The face is the primary focus of attention in our today's modern societies and for social intercourse as well, the face plays a major part in sending message such as emotion and identity. We can see and recognize millions of faces throughout our lifetime and identify familiar faces at a instant even after years of separation. These scenarios are relatively robust despite significant changes in the visual stimulus caused by aging, expression or distractions, such as beards, glasses or changes in hair or face appearances'. Face recognition systems is part of facial image processing applications. The importance of these systems as a research area has increased recently. Facial recognition being the most concerned area of research in the modern technology and the way to enhances security within every society having good authenticity and reliability to our normal system's activities

Facial recognition systems are usually applied and preferred by people and security personnel in urban cities. These systems can be used for theft, crime prevention and navigations, identity verification, and other similar security activities. [1]. Face recognition is one of the most applications of image analysis. However it's a true issue to make an automated system which equals human capacity to detecting faces. Human being are quite good than systems in identifying known faces, but we are not very good when we must deal with millions of datasets when dealing a unknown faces. The computers, with an almost endless storage capacity and computational speed, should overcome these problem.

Facial recognition been the most paramount, significances to the development of modern technology and the role it plays in the various sectors such as security, education and commercial body, there involved a lot of hindrances while addressing the issues. These hindrances might have different approach depending on the

type of the issue encountered. As an area of research which great engineers deployed varieties of methods or algorithm to solve whatever the problem might be, they also need to know the best way in order to have a better performances with having a little amount of time. Face recognition involves different stages which output a better performances or good outcomes starting from face detection stage, pre-processing of the image, feature extraction, classification and face recognition.

Engineering start to developed interest in face recognition in the year 1960's or somewhere about that. The first researches on this subject area was Woodrow W. Bledsoe. In 1960, Bledsoe, along other researches, started Panoramic Research in Palo Alto, California. The majority of the research work done by this company involved are all related contracts from the U.S. Department of Defense and various intelligence agencies [2]. In the previous years, face recognition has done well by attracting much attention of researchers and these research has rapidly expanded by not only scientist but also neuroscientists in the medical and clinical health science, because of its many potential applications in computer vision, machine learning communication, image processing, artificial intelligence, and robotics

Face identification is an important part of face recognition as the first stage of automatic face recognition. However, face recognition is not straightforward scenario because it has lots of variations of image appearances, such as pose variation (front, non-front), occlusion, image orientation, illuminating condition and facial expression [3].

II. MOTIVATION

Development and activities of every society within the globe need to be monitored, interactions, behaviours and transactions of individual in the societies demand total attention, because of the complex nature of our environment, this shows a rapid a improvements and progress occurring daily. Therefore means of verifications and identification of person is necessary or even becomes mandatory.

Within the last few years, verification and identification happens in only two ways. One of way can be carried by a magnetic card. The second way is a type of password. These two ways of verification are not secure because both can be given away, or taken away by someone, or lost. However , many people can find means to forge these identities. But a technique that makes navigation surveillance and monitoring systems works like a pair of eyes has been established. With computer vision, face recognition has become increasingly relevant in today's society. Seeing the recent development in face recognition can be as result to the increase in demand to have more trusted and reliable security in data communication, commercial area, educational sectors. Most of the Major areas of commercial area of interest include biometrics, law enforcement and surveillance, smart cards, and access control [4]. Now, the need to maintain standard in security Information is of paramount, a company or an organization wants to enhances their existing security challenges. People need to have an organization with optimal security functionality which gives complete security solution to their services need. There usually exist the occurrences' of event from time to time of crimes of credit card fraud, computer break-in by yahoo boys , or security goes into the company, in shops, in government sectors. Most of these crimes the criminals that are happening now adays, the hackers take advantage of that hacking the information from the organization or have access control system of such organization. The systems do not permits oneself to have access by who we are, but by what you get at hands, such as passwords, PIN numbers and etc. by authenticate users. These happened without the permission of owner's, knowledges,

III. FACE RECOGNITION SYSTEM

Because the vital fact on the knowledge of machine learning, all the algorithms developed by researchers are subset of machine learning in the data science sector. A Machine Learning (ML) system is different from that of computer program which too many scientist in other discipline found it difficult to understand or comprehending

Fig. 1. Conventional Programming Method

The Machine Learning based computer system takes in the input data and the result (which is the output or predicted or target output) which are feed to the learning system model, and produces the Result as program which can be used for others subsequent tacks. While that of computer program, a program is written and both the program and the input data are fed to the computer system for specific task and result is obtained.

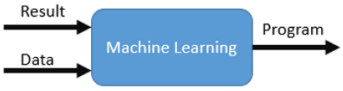


Fig. 2 Machine Learning Approach

IV. ORL DATABASE

The evolutional trends in datasets in the modern technologies for facial recognition and emotion can be useful for determining the future of our next generation. An important part of the usual enhancements made in the field of facial recognition, facial expression and emotion has been the collection of facial datasets or database for benchmarking purposes. Since the year 1990, there has been a drive in developing new models for automatic or algorithms in the field of facial recognition as a result of the significant advancement in computer technology [5]. Presently, there are different kind of databases used for facial recognition purposes which vary in expressions, vary in size, pose lighting conditions. A number of images subjects the AT & T dataset formerly known as ORL Database contain images of different faces, contains a set of face images taken between the year 1992 to April 1994 at the lab at AT & T Laboratory of Cambridge University.

Fig. 3. Example of ORL database

For this research work, the entire database was firstly shuffled in order to have fair distribution across the 40 classes. The shuffled data was then split in to train and test using 70-30 split. i.e. 280 was used for training and the remaining 120 was used for testing.

V. CLASSIFICATION

A. PARTICLE SWARM OPTIMIZATION (PSO)

Not quite long, a lot of researcher's effort has been put in place towards enhancing human to computer system interaction so that computers can have the intelligence to perceiving the emotional state of the human user and react accordingly, just like a human would do. There are different technological or varieties of organization sectors that do exist and render 100% of these services. Artificial Intelligence with robots system engineering could be developed to provide support and comfort to a bed to ridden and highly disabled individuals who are confined to a room in their houses. This is of paramount important given the present modern life style where the population of children is reducing, the middle-aged are getting busier with work schedules and where the senior people and the disabled are increasingly being left to fend for themselves [6].

An algorithm that has been very good, efficient and effective in solving a lot of issues that involve simplifying and finding optimal solution of the issue, optimizing or searching for the optimal value using the Particle Swarm Optimization (PSO) algorithm. Particle swarm optimization (PSO) is a population based stochastic optimization technique developed by Dr. Eberhart and Dr. Kennedy in 1995, inspired by social behavior of birds flocking or fish schooling [7], who's initial postulation intended for the simulation of social behavior of birds or insect as they fly in a group searching for what they eat. Particle Swarm Optimization either in its original form or with some modifications was soon found to be applicable in solving a variety for problems solving and better performances. A classical application includes finding of some problems issues which are classical in nature, electrical systems problems, neural networks, and etc. It has been applied to clustering problems such as image processing, data analysis and genetic algorithm.

B. SUPPORT VECTORS MACHINES (SVM)

Support Vector machine is the most successfully and best classification algorithm in machine learning, it's a nice method because there is simple principle of derivation for and there is also an optimization package that one can be used in order to get a solution and the solution has an intuitive interpretation.

i. Linear Separable

Linear separability is an important topic in the field of artificial intelligence specifically that of machine learning area of research. When two more separable data sets are passed into a linear model against noise and most likely will not over fit, this gives an optimal accuracy and robust than that of inseparable data. Perceptron in neural networks gives such part behavior without no constrain and difficulty in their process. The figure below gives clear example of linear separable data.

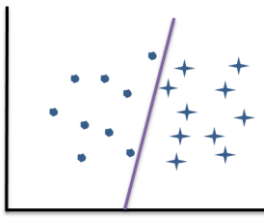


Figure 4**:** linear separable data Sample

The rationale behind the ideal of SVM start from where the limitation of perceptron (linear separable algorithm) begins. Most of real physical scenario cases are not linearly in nature but the issue of understanding the linearly separable data gives more room to engineer and scientists the courage to further their research in the field of nonlinear separable data.

Facial recognition and authentication are the important measures in almost every security organization or sectors. For the past two years or more, a different facial recognition approaches were deployed and developed. The performances of these different algorithms models are compared based on the important parameter and facial recognition rate; so called classification rate. If the classification rate reduces, then the misclassification rate will increase and vice versa. The facial recognition is done based on the minimum distance measure between the training dataset of the set feature vectors and testing dataset of the feature vectors.

Support Vector Machine (SVM) was first postulated in year 1992, introduced by Boser, Guyon, and Vapnik in COLT-92. Support vector machines (SVMs) is a supervised learning algorithm method used for different application like regression, classification and etc. Support Vector Machine comes from the category of linear classifications models. In another definition, Support Vector Machine (SVM) is among the top best binary classification algorithms tools that uses machine learning to maximize predictive accuracy while automatically avoiding over-fit to the data. Support Vector machines can be said to be as a systems which use hypothesis space of a linear functions in a high dimensional feature vectors space, training with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning machine theory. It is also being used for different applications, such as pattern recognition, hand writing analysis, facial recognition analysis and so on.

ii. Margin Maximization

Margin maximization is an interesting subject matter when talking about Support Vector Machine. Maximization is term which refer to expanding or widening a size or a particular area. In the perspective aspect and understanding to margin maximization in the support vectors machine scenario. It's one of the foundation building block of the SVM process. As one can see and from figure shown below, this gives an intuitive idea of the margin maximization scenario. There are five possible lines that separate the sample data into two different classes, the green color, purple, black, blue and red color line. Looking at all the five colors, the blue line which gives the highest maximum separation distance between the two classes.

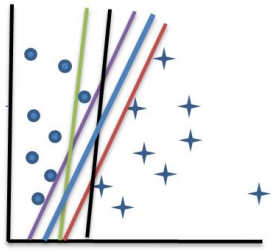


Figure 5: Linear Separable Data with Different Classifiers

Before dwelling into the concepts of Margin maximization, let us know why the need for the margin maximization. Suppose we have some linear separable sample data as shown below, and there is a need for classifying the data. We might not know the best classifier among them, whether its purple color classifier, blue color classifier, green color classifier, red color or black color classifier . The issue of choosing the best classifier comes into consideration having the largest equal distances from the nearest sample data.

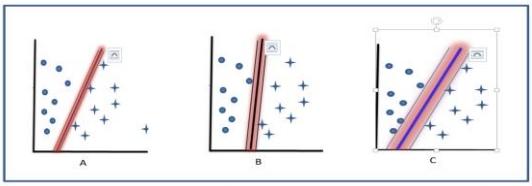


Figure 6: Margin with Different thickness

The blue color hyper plane being the fattest among the three from the above diagram gives the highest optimal and possible margin one can obtained

Support vectors machine is a supervised learning models that solve the problem of classification analyze data and recognize patterns, used for classification and regression analysis. Given a set of training input dataset, each marked for belonging to one of two classes, a SVM algorithm builds a model that assigns new data into one classes or other. SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New data are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on. In addition to performing linear classification, Support vector machines can efficiently perform a non-linear classification

using what is known the kernel trick, implicitly mapping their inputs into high-dimensional feature vectors spaces. The non-probabilistic nature of Support vector machines s is its own key strength. These nature of the SVMs is in contrary to the probabilistic classifiers like that of the Naïve Bayes, Regression and etc. Support Vectors Machine divides data into a decision boundary known as plane and determined with the only a small amount of sample data of feature vectors space. The sample data subset which supports the decision boundary are appropriate and known as support vectors. The remaining feature vectors of the dataset do not have any influence in determining the position of the decision boundary in the feature vector space. In contrast with SVMs, probabilistic classifiers develop a model that best describe the data by considering all of the data versus just a small subset. Subsequently, probabilistic classifiers likely require more computing resources[10].

- The equation of point $i(\boldsymbol{\mathcal{X}_n})$ which gives the distance from the point to plane is

$$\boldsymbol{\mathcal{W}^T\mathcal{X}_n + b = 0}$$

$$\boldsymbol{|\mathcal{W}^T\mathcal{X}_n + b| = 0}$$

- The weight vector $\boldsymbol{\mathcal{W}}$ in the above equation is $\perp$ to the plane in the $\boldsymbol{\mathcal{X}}$ space
- Let consider the two points on the plane with $\boldsymbol{X^I}$and
- Having the equation $\boldsymbol{\mathcal{W}^T X^I + b = 0}$ and $\boldsymbol{\mathcal{W}^T X^{II} + b = 0}$
- Combining the two equation $\boldsymbol{\mathcal{W}^T X^{II} = 0}$ and $\boldsymbol{\mathcal{W}^T X^I = 0}$

$$\boldsymbol{\mathcal{W}^T(X^{II} - X^I) = 0}$$

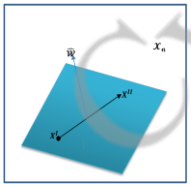


Figure 7: Support Vector

- The distance between and the plane $\boldsymbol{\mathcal{X}_n}$
- Take any point $\boldsymbol{\mathcal{X}}$ on the plane
- Projection of $\boldsymbol{\mathcal{X}_n - \mathcal{X}}$ on $\boldsymbol{\mathcal{W}}$

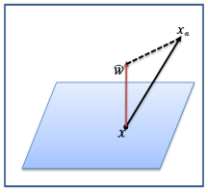


Figure 8: Unit Vector

$$\widehat{\boldsymbol{\mathcal{W}}} = \frac{\boldsymbol{\mathcal{W}}}{||\boldsymbol{\mathcal{W}}||} \textbf{ = Distance = } |\boldsymbol{\mathcal{W}^T(\mathcal{X}_n - \mathcal{X})}|$$

$$\textbf{Distance} = \frac{1}{||\boldsymbol{\mathcal{W}}||}\{|\boldsymbol{\mathcal{W}^T\mathcal{X}_n - \mathcal{W}^T\mathcal{X}}|\}$$

$$\frac{1}{||\boldsymbol{\mathcal{W}}||}\{|\boldsymbol{\mathcal{W}^T\mathcal{X}_n + b - \mathcal{W}^T\mathcal{X} - b}|\} = \frac{1}{||\boldsymbol{\mathcal{W}}||}$$

$$\text{Maximize } \frac{\mathbf{1}}{||\boldsymbol{\mathcal{W}}||}\boldsymbol{Min.}\,|\boldsymbol{\mathcal{W}^T\mathcal{X}_n + b}| = \mathbf{1}$$

$$\text{Minimize } \frac{\mathbf{1}}{\mathbf{2}}\boldsymbol{\mathcal{W}\mathcal{W}^T} \quad \text{Subject to } \boldsymbol{n = 1,2,\dots,\mathcal{N}}$$

But Notice $\boldsymbol{|\mathcal{W}^T\mathcal{X}_n + b|} = \boldsymbol{\mathcal{Y}_n(\mathcal{W}^T\mathcal{X}_n + b)}$

$$\text{Subject to } \boldsymbol{\mathcal{Y}_n(\mathcal{W}^T\mathcal{X}_n + b) \geq 1} \quad \boldsymbol{for\ \ n = 1,2,\dots,N}$$

$$\boldsymbol{\mathcal{W} \in \mathbb{R}^d, b \in \mathbb{R}}$$

Now because of the constrained optimization, it's not helpful and also there exist of an inequality constrained. Therefore to obtain an unconstrained optimization problem, we make use of *Lagrange multiplier* for this conversion (from constrained to unconstrained optimization). This will in turn gives the best separating plane having the best possible margin.

2.2.4.3 Lagrange Formulation

For the regularization of the in sample error term,

Min. $\mathbf{E}_{\text{in}}(\boldsymbol{\mathcal{W}}) = \frac{1}{N}(\mathbf{Zw - y})^{\mathbf{T}}(\mathbf{Zw - y})$ *Subject to*; $\boldsymbol{\mathcal{W}^T\mathcal{W} \leq C}$

$\nabla \boldsymbol{E}_{\text{in}}$ Is normal to the constrain

$\boldsymbol{X^{II}}$

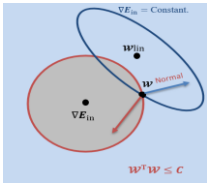


Figure 9: Quadratic Programing

	Optimization	Constrain
Regularization	$\boldsymbol{E_{in}}$	$\boldsymbol{\mathcal{W}^T\mathcal{W}}$
SVM	$\boldsymbol{\mathcal{W}^T\mathcal{W}}$	$\boldsymbol{E_{in}}$

For the Lagrange formulation problem, it converts the constrained optimization problem to unconstrained one by introducing a *Lagrange multiplier* $\boldsymbol{\alpha}$

Minimizing the objective function $\frac{1}{2}\boldsymbol{\mathcal{W}\mathcal{W}^T}$under the constrained/Subject to $\boldsymbol{\mathcal{Y}_n(\mathcal{W}^T\mathcal{X}_n + b) \geq 1}$

$$\text{minimize } \boldsymbol{\mathcal{L}(\omega, b, \alpha)} = \frac{\mathbf{1}}{\mathbf{2}}\boldsymbol{\mathcal{W}\mathcal{W}^T} - \sum_{\boldsymbol{n=1}}^{\boldsymbol{N}} \boldsymbol{\alpha_n(\mathcal{Y}_n(\mathcal{W}^T\mathcal{X}_n + b) - 1)}$$

W.r.t $\boldsymbol{\omega}$ and $\boldsymbol{b}$. & maximize W.r.t each $\boldsymbol{\alpha_n \geq 0}$

$$\boldsymbol{\nabla_\omega \mathcal{L} = \mathcal{W} - \sum_{n=1}^{N} \alpha_n(\mathcal{Y}_n(\mathcal{X}_n)) = 0}$$

$$\frac{\partial \mathcal{L}}{\partial b} = \boldsymbol{\sum_{n=1}^{N} \alpha_n \mathcal{Y}_n = 0}\ \boldsymbol{\mathcal{W} = \sum_{n=1}^{N} \alpha_n \mathcal{Y}_n \mathcal{X}_n}\ \textbf{And}\ \boldsymbol{b = \sum_{n=1}^{N} \alpha_n \mathcal{Y}_n}$$

But showing from the Lagrange formula, we can substitute for

$$\mathcal{L}(\omega, b, \alpha) = \frac{1}{2} WW^T - \sum_{n=1}^{N} \alpha_n (y_n (W^T x_n + b) - 1)$$

Then there we obtained the expression/formula for α_n

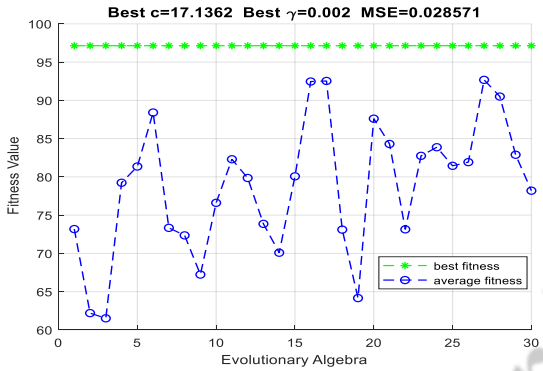
$$\mathcal{L}(\alpha) = \sum_{n=1}^{N} \alpha_n - \frac{1}{2} \sum_{n=1}^{N} \sum_{n=1}^{N} \alpha_n \alpha_m y_n y_m x_n x_m$$

VI. RESULTS AND DISCUSSION

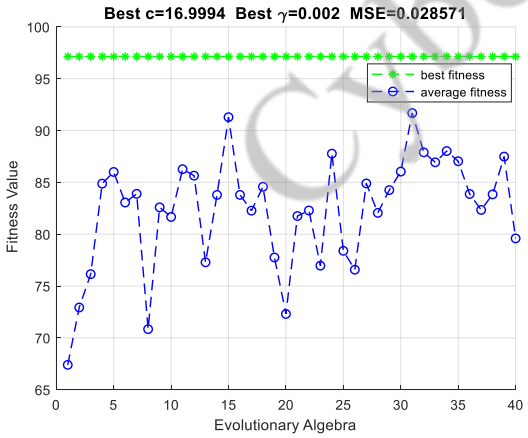
In this section, the results obtained after implemeting each item of the methodology is presented and discussed.

4.1 Results for Finding the Values of the Hyperparameters

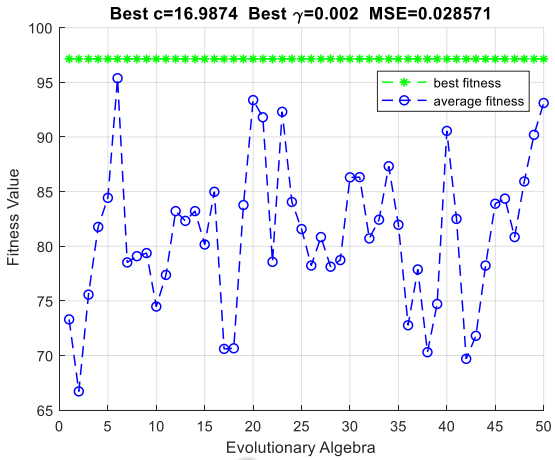
The PSO fitness curve for searching the best SVM hyperparameters (C and γ) are as shown in Figures 4.1-4.3 for different number of generation.



Figures 10: PSO fitness curve for 30 geneartion number



Figures 11: PSO fitness curve for 40 geneartion number



Figures 12: PSO fitness curve for 50 geneartion number

As can be seen from these results, only the value of hyperparameter C tends to change slightly as the number of generations are increased while the hyperparameter γ and the mean squared error remains unchanged. We however observed that the classification accuracy tends to be improved as the generation number is raised. The summary of the result obtained is presented in Table 4

Table 1: Summary of the results obtained

Approach	Maximum Generation	Optimized C	Optimized γ	MSE	Classification Accuracy
LBP-PSO-RBF-SVM	30	17.1362	0.002	0.028571	0.9583
LBP-PSO-RBF-SVM	40	16.19994	0.002	0.028571	0.9750
LBP-PSO-RBF-SVM	50	16. 9874	0.002	0.028571	0.9833

The details of how the model classifies each of the forty (40) facial images is presented in the form of confusion matrices of figures 13-15. The figures give a summary of the counts of the correct and incorrect predictions broken down by each class.

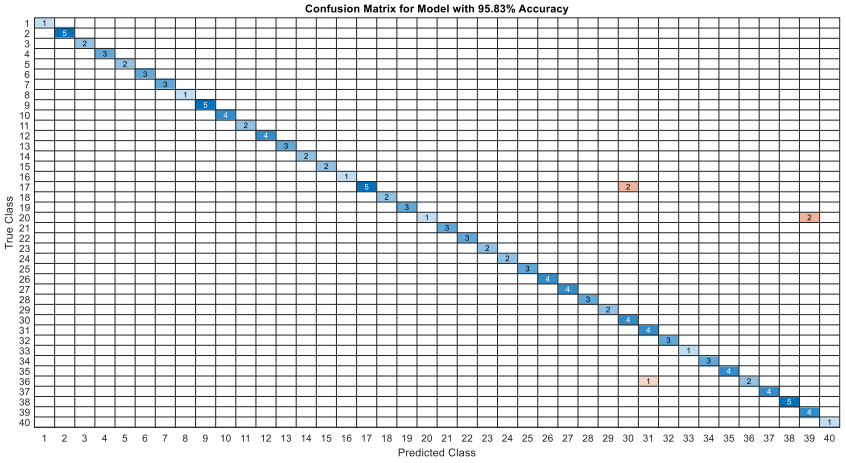


Figure 13: Confusion Matrix for Model with 95.8% Accuracy

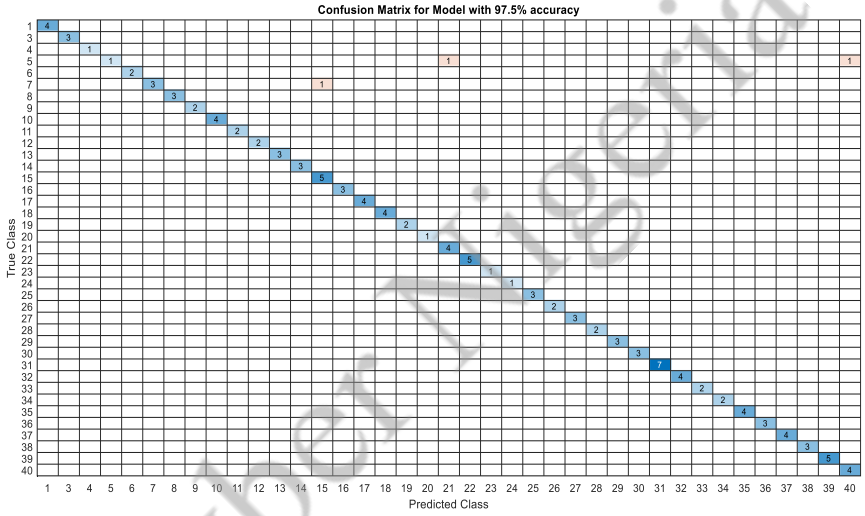


Figure 14: Confusion Matrix for Model with 97.5% Accuracy

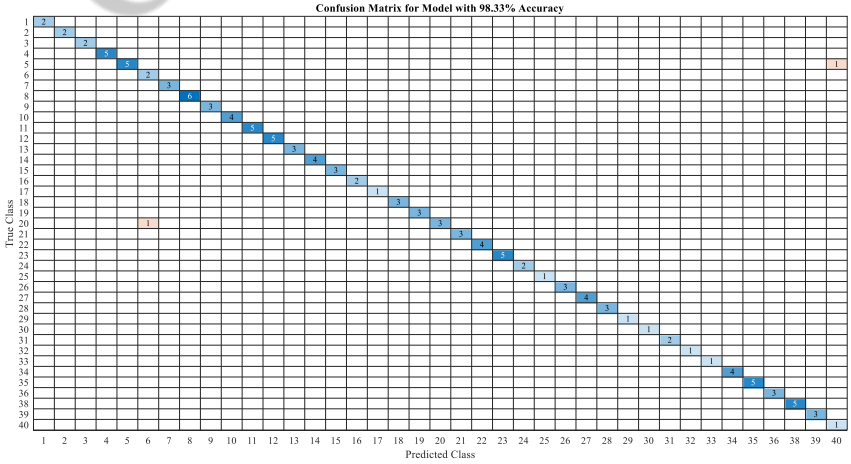


Figure 15: Confusion Matrix for Model with 98.33% Accuracy

As can be seen from figures 13-15, the confusion matrices gave the distribution of the True and predicted classes. It can be observed that the three models have 5,3 and 2 misclassified values respectively.

From the figures 4.1-4.3, it can be seen that there are 5, 3 and 2 misclassified classes respectively.

VII. CONCLUSION

Face recognition application is still a concerned research area of interest since it plays a vital role in a number of applications. It is used in verifying and detecting the correct face in either an image or a video stream. In order to obtain good recognition models, optimization of some hyperparameters becomes necessary even within the selected or desired classification method. In this research, Local Binary Pattern (LBP) was used for feature extraction while Support Vector Machines (SVM) with a Radial Basis Function (RBF) kernel was used as a classifier. Particle Swarm Optimization (PSO) was used to optimize and choose the best RBF-SVM hyper parameters [C, γ] and the results obtained were competitive.

The development of a face recognition algorithm where features were extracted from ORL images using Local Binary Patterns and classified using kernel based support vector machine has been developed. The SVM hyperparameters were optimized using Particle Swarm Optimization. Results obtained yielded promising results in terms of Mean Squared Error and average classification accuracy.

REFERENCES

1. Z. A. Fadahl, T. A. Al-Saadi, M. K. Al-Hasnawi and N. J. Al-Khafaji(2014), ' Facial recognition Based on Back Propagation Technique', International Journal of advances in computer Network and its Security(IJCNS), Vol 4, PP (11).
2. M. Ballantyne, R. S. Boyer, and L. H. Woody bledsoe (1996), 'His life and legacy'. AI Magazine, Vol. 17(1) PP (7–20).
3. Siddharth Bhavsar, Niraj Achari, and Bhavin Pandya, (2013), 'Face Detection based on Video' International Journal of Advances in Computer Science and its Applications (IJCSIA) Vol. 3, PP (86-88).
4. M. A. Kashem, M. N. Akhter, S. Ahmed, and M. M. Alam,(2011), 'Face Recognition System Based on Principal Component Analysis (PCA) with Back Propagation Neural Networks (BPNN),' International Journal of Scientific & Engineering Research, vol. 2.
5. Sohini Roychowdhury and Michelle Emmons, 'A Survey Of The Trends In Facial And Expression Recognition Databases And Methods', 1Department of Electrical Engineering, University of Washington, Bothell, (https://arxiv.org/ftp/arxiv/papers/1511/1511.02407.pdf).
6. Bashir Mohammed Ghandi, R. Nagarajan and Hazry Desa,(2009) 'Particle Swarm Optimization Algorithm for Facial Emotion Detection', IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), PP.(595-599).
7. http://www.swarmintelligence.org/tutorials.php#:~:text=Particle%20swarm%20optimization%20%28PSO%29%20is%20a%20population%20based,evolutionary%20computation%20techniques%20such%20as%20Genetic%20Algorithms%20%28GA%29.

Base Station Availablity and Telecommunication Network Quality of Service – A Review

Emmanuel Ohihoin
Department of Telecommunication Engineering
Federal University of Technology
Minna, Nigeria
ohihoin.pg919146@st.futminna.edu.ng

Henry Ohize
Department of Electrical and Electronic Engineering
Federal University of Technology
Minna, Nigeria
henryohize@futminna.edu.ng

Michael David
Department of Telecommunication Engineering
Federal University of Technology
Minna, Nigeria
mikeforheaven@futminna.edu.ng

Caroline Alenoghena
Department of Telecommunication Engineering
Federal University of Technology
Minna, Nigeria
carol@futminna.edu.ng

***Abstract*—Network Quality of Service (QoS) is hinged on Base Transceiver Station (BTS) Availability. With the preparation of roll out of Next-generation 5G network, there is bound to be a massive influx of network infrastructure and higher demand for network availability. 5G intends to achieve all-time connectivity for diverse devices and this implies that the devices must remain connected not minding the state of the channel. This paper reviews the significance of a predictive tool for base station availability for Mobile Network Operators (MNO) for better service delivery. This forecast will enhance the smart planning of operations by Managed Service Providers (MSP) in a bid of improving Base Station availability by the reduction of the Mean Time to Repair (MTTR) as well as the increment of Mean Time Between Failure (MTBF) (MTBF can be improved by redundancy) to overcome envisaged network downtimes. It is a common practice for MNOs to engage the services of MSP as they have the capability of efficiently handling technical complexities more than the clients would (client here refers to the MNO). The MSP and the MNO enter into a contractual relationship and a service level agreement (SLA) is issued. This service level agreement is an important document in the contractual agreement binding the client (MNO) and the MS provider (MSP) and it defines the key performance indicators (KPI) that the MSP must meet up with. The parameters include a detailed description of required services, network restoration, network uptime, availability, systems repair, data transfer rate and expected performance measure.**

Keywords— Base Transceiver Station, Availability, Quality of Service, Mobile Network Operator, Managed Service Provider, Service Level Agreement.

I. INTRODUCTION

The massive influx of wireless mobile cellular technologies has made communication and other related applications more available than what it was in a few decades before now. With the emerging 5G, mobile applications will experience a tremendous surge, whereas, the bandwidth requirement of the cellular network becomes very high. To cater for such a great need in the cellular network infrastructure, several base stations have been designed, deployed to appropriate geographical locations to meet the expectations of the service coverage areas and improved quality of service [1], [2]. The base stations are then linked to the carrier network via the backhaul infrastructure using microwave links or fiber-optic lines. Though, this infers that the network service downtime will affect all the dependent base stations. It becomes very essential to consider the need to maintain an acceptable availability for both transmission route and base station so that service availability is sustained. A mobile cellular network is described as a communication infrastructure comprising network elements (NEs) that allow mobile stations or user equipment (UEs) access network services through radio channels [3]. Key performance indicators (KPI) for Quality of service (QoS) such as Call Setup Success Rate (CSSR), Drop Call Rate (DCR), Traffic Channel Congestion Rate (TCH-CR), Hand Over Success Rate(HOSR) are greatly enhanced with optimum base station availability [4]–[16]. In the remaining part of this paper, we will be looking at related work, basic concepts and terminology in the research domain, Managed Service (MS) and Service Level Agreement (SLA) effects on BTS Availability; models and network predictive tools presently in use, future direction and the conclusion.

II. RELATED WORK

Research work on base station availability have centered on optimal resources utilization; power-saving and improved radio network planning and maintenance. In [17], the availability of cloud Mobile Switching Server and Telecommunication Application Server were considered with the redundancy principle. Prior to the deployment of telecommunication networks on cloud, it is very important to have an idea on the level of network availability in comparison with that of the legacy equipment, hence the necessity of the availability prediction. This helps in proper planning of the project implementation and assurance of service quality. The simulated result indicated availability values equivalent to that of the legacy telecommunication equipment is achievable. However, the outcome of the simulation needs to be authenticated by the use of real field dataset. In [18], the paper discusses the evolution of Telecommunication Cloud, availability, basic dimensioning, design concepts and some challenges of practical implementation of the technology. [20] presented a

framework for predictive model which used active and historical dataset as well as data from internet of things (IoT) devices and sensors. This work has the meritit of enabling the proactive planning for maintenance of the Radio Access Network (RAN) thereby increasing the telecommunication network availability and also reducing operational cost. Prediction of power supply failure was done by [21] by using a statistical analysis and the assessment of failure risk with the aid of fuzzy graphs and artificial intelligence. The work showed that future rectifier power failure can be avoided by predictive maintenance on the capacitors which can change in capacity as a result of ageing and electrical stress.

The papers [22], [23] both did a similar study on network availability. The authors in [22] considered that one of the main benefits of a network function virtualization (NFV) infrastructure is its high availability; the paper focuses on the analysis of the Virtualized Infrastructure Manager (VIM), a core element that is implemented through the OpenStack platform and is aimed at managing the whole NFV architecture. The system availability was evaluated by performing both a steady-state and transient analysis of Stochastic Reward Networks (SRNs) to obtain the best system configuration with the "five nines" (99.999%) availability requirement. Authors in [23] assessed how the distribution of the Software-Defined Networking (SDN) controllers contributes to the total availability of SDN. The quantity of homing and location of SDN controllers were altered. he results of the research showed how network operators can use the approach to determine the optimal cost implied by the connectivity of the SDN control platform by maintaining high values of availability. This approach may improve network flexibility and programmability, but it is likely going to introduce some challenges. In the work of [24], only a fraction of eNodeB site is powered by back up batteries during a temporary utility power cut off. The method used a modified sleep mode idea in cellular networks to control the working of the eNodeB sites in the case of electricity grid power outage. Simulations were carried out on the basis of network link with the use of radio network planning software known as ICS Designer. A significant availability was achieved during the backup period, but the research did not provide an algorithm in how to select the usable eNodeB sites. In the work of [1], a predictive model was formulated and they proposed an approach that boosts cellular network availability by event-driven base station battery profiling that identify and extract the features causing the degradation of back-up battery groups. The work indicated an 18.09% boost in the cellular network availability.

There is no doubt that base station availability is a critical factor in delivering quality services; a clear understanding of the requirement for availability and appropriate tools to achieve optimal service is thus paramount.

III. CONCEPTS AND TERMINOLOGY

Some common concepts and terminologies used in the reviewed papers are discussed here to be in the right frame to appreciate the subject matter of base station availability and telecommunication network QoS.

A. Definition of Availability

Availability has been defined by the International Telecommunication Union (ITU)) as the capability of a functional unit to be in a state to accomplish a vital purpose in a given circumstance at a given instant of time or over a given time interval, assuming that the required external resources if required are provided [25]. In short, availability is a fractional value of the amount of time the network is rendering services divided by the amount of time it is expected to deliver the services [26][11]. For a communication link like the synchronous digital hierarchy (SDH), availability as specified by ITU-T Standard G.826 is computed from the unavailable seconds (UAS). Refer to figure 1 below.

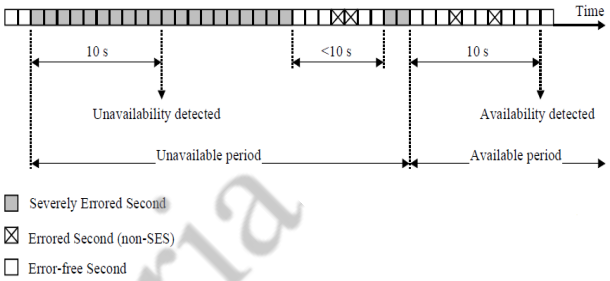


Fig. 1. Showing the Determination of UAS
Source: The ITU-T Standard G.826 Document.

Availability, A:

$$A = \frac{(Measured\ Time - UAS) * 100}{Measured\ Time} \quad (1)$$

Analytically, A is defined in [11], [17], [24]–[29] as:

$$A = \frac{MTBF}{MTBF + MTTR} \quad (2)$$

Where the Mean Time Between Failure (MBTF) is a vendor warranty for the availability of the Telecommunication mobile network operator. It is the average time between two failures for repairable items.

Mean Time to Repair (MTTR) is the average period for repair and testing. This is the guarantee of the Managed Service Provider (MSP) for assurance of the availability of the telecommunication MNO. The major task of the MSP is to continually ensure that MTTR is kept at the barest minimum.

Un-availability (U)

$$U = 1 - A \quad (3)$$

Downtime for the period, T denoted as D_T is given by:

$$D_T = (1 - A) * T \quad (4)$$

B. Failure Rate, MTBF, MTTR,MTTF and FIT

Failure Rate (λ) of a unit (assembled from many components) is the number of failures that may occur during a given period. [17], [32]. It is constant over the life

expectancy. The constant failure rate period falls between the initial 'infant mortality" and the final wear-out period as shown in figure 2 below.

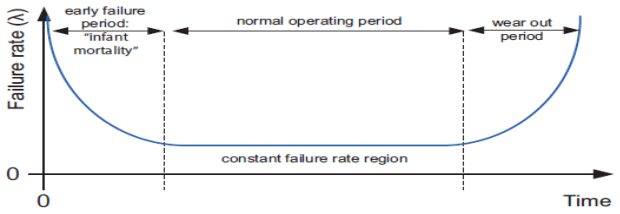


Fig. 2. Failure Rate Curve

Source: [17]

The Failures in Time (FIT) rate of a device is the ratio of the number of failures that can be expected, to a billion (10^9) device-hours of operation [17].

$$FIT = \frac{Number\ of\ failures}{10^9 hour} \quad (5)$$

$$MTBF_{hour} = \frac{1}{\lambda} \quad (6)$$

Mean-Time-To-Failure (MTTF) is the meantime expected until the first failure of a piece of equipment for a non-repairable item. MTTF is a statistical value and is meant to be the mean over a long period and a large number of units.

C. The BTS and the Mobile Cellular Network

The BTS processes speech encoding, multiplexing (TDMA), encryption, and modulation/demodulation of the radio signals. Its physical connection is achieved via the radio waves. A BTS is monitored by a base station controller (BSC) through the base station control function (BCF) [33]. A mobile cellular network is described as a communication infrastructure comprising network elements (NEs) that allow mobile stations or user equipment (UEs) access network services through radio channels [3]. Figure 3 below illustrates the mobile network and the BTS.

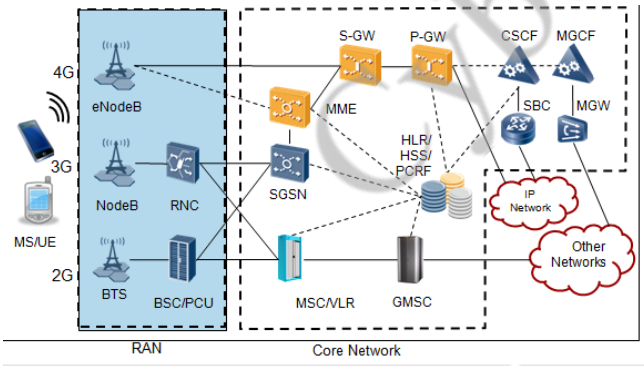


Fig. 3. Telecommunication Network

Source, [31]

D. Quality of Service (QoS)

The European Telecommunications Standards Institute (ETSI) defines QoS from the network perspective as *the capability to segment traffic or differentiate between traffic types for the network to handle certain traffic differently from others*", [23] and in the ISO definition, quality is defined as "*the totality of characteristics of a unit that bear on its ability to gratify stated and implied requirements* (ISO 8402*).*

From reviewed papers, the most predominant Key Performance Indicators (KPIs) on which GSM are assessed for QoS are:

Call Setup Success Rate (CSSR). CSSR is the ratio of unblocked call attempts to the total number of call attempts.

$$CSSR = (1 - Blocking\ Probability) * 100\% \quad (7)$$

Call Drop Rate (CDR). DCR is the ratio of dropped calls to the total number of call attempts.

$$DCR = (1 - Call\ Completion\ Rate) * 100\% \quad (8)$$

Handover Success Rate (HOSR). HOSR is the ratio of the accomplished handovers to the total number of attempted handovers.

Traffic Channel Congestion Rate (TCHCR) ia s measure of how busy a cell is in setting up a call. The higher the TCHCR, the more difficult it is to access the channel.

Table 1 below shows the acceptable standard values of the KPIs according to the Nigerian Communication Commission.

TABLE I. KEY PERFORMANCE INDICATOR FOR QUALITY OF SERVICE

Parameter	Target Value
CSSR	≥98%
DCR	≤1%
SDCCH	≤0.2%
TCCH	≤2%

Source: The Nigerian Communication Commission (ncc.gov.ng)

E. Availability Requirement by ITU

Availability requirements are usually presented in terms of nines. For many telecommunications network equipment and BTS, there is a strict standard of five or six nines.

TABLE II. AVAILABILITY AND CORRESPONDING DOWNTIME

Availability (%)	Downtime Per Year
99.9999	32s
99.999	5min 15s
99.99	52min 36s
99.9	8h 46min
99	3 days 15h 40min

Source: Calculated Using Equation (4)

IV. MANAGED SERVICE AND SERVICE LEVEL AGREEMENT ON BTS AVAILABILITY

Managed Service renders services to MNO to improve BTS and other network availability [34]–[37]. The major task of MS is the reduction of MTTR term in equation 2. Reducing this value entails a lot of conscious effort to timely restore the network after outages and also the proactive planning of preventive maintenance (PM) work on network element (NE) [20]. SLA helps in controlling and enforcing compliance to contractual terms between the MNO and MSP to maintain a low MTTR which invariably improves availability as portrayed in [26], [30], [38], [39].

V. MODELS AND NETWORK PREDICTIVE TOOLS PRESENTLY IN USE

Predictive model uses data and statistics to predict or forecast future outcome based on learning from previous data. Some of the works used the artificial neural networks (ANN), the auto regressive integrated moving average

(ARIMA) and Bayesian Network (BN) model. BN exploits the capability to combine non-linear systems, their transparent probabilistic basis, and low computational cost as in the papers [29], [31], [37], [39]–[41]. Predictive BNs are generalizations of a system that have skill at forecasting outside of the training field. The predictive and descriptive expediency of a BN depends on its complexity and the amount of data available to train it, but there is often a trade-off; higher descriptive skill comes at the expense of condensed predictive skill.

A. Artificial Neural Network

Authors in [42]–[46] used ANN in their work. An artificial neural network is a computer simulation of a system that imitates the human brain. It contains several interconnected processing elements referred to as neurons that perform some mathematical operations. The weighted linkage of neurons is information stored in the neuron. According to [47], ANN has the advantage of a flexible non-linear capability. The model is adaptively designed based on the structures of a dataset, and there is no requirement to specify a specific method of a model. In scenarios where there is no theoretical guidance to suggest a suitable procedure that ANN would be a suitable model. A benefit of ANN over most other classes of the non-linear model is that ANNs are universally superb in giving approximations with a high level of accuracy [42], [43]. This is as a result of the parallel handing out of the information of the dataset.

ANNs have some components that are used in the process of building the model.

The Basic Components of ANNs are:

- Input.
- Interconnections or weights.
- Output.
- Neurons or nodes have internal state known as an activation signal. Neurons are connected to other neurons through interconnection link, this link is associated with a weight that has information about the input signal. The input signal combines with the activation signal of the neuron after obeying an activation rule to produce an output. Fig. 4 below is a general ANN model.

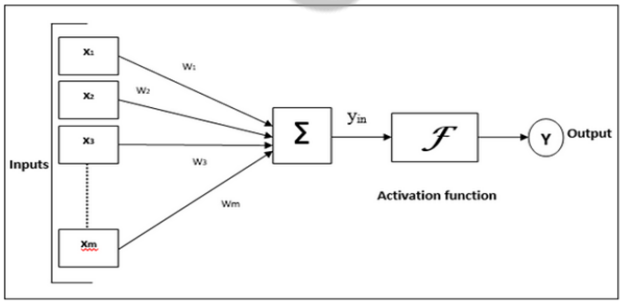


Fig. 4. General Model of Artificial Neural Network

Source:https://www.tutorialspoint.com/artificial_neural_network/artificial_neural_network_supervised_learning.htm

B. Auto Regressive Integrated Moving Average

The Auto Regressive Integrated Moving Average (ARIMA) written as Autoregressive (AR) (p) Integrated (I) (d) Moving Average (MA) (q) is a hybrid of models that exploits the functions of the Regressive, the differencing factor (Integrating) and the Moving Average in the models. The **p, d and q** are their respective orders. For the Autoregressive (AR) model, the output variable is linearly dependent on the previous values and a set of stochastic terms. The AR model having an order (p) is generally written as AR (p) and is mathematically defined as:

$$A_t = \sum_{i=1}^{P} \phi_i A_{t-i} + \varepsilon_t \quad (9)$$

Where $\phi_i,\ldots, \phi_p$ are the model's parameters and ε_t is the random error. Similarly, the output variable (A_t) for the MA depends linearly on the present value and past values of stochastic terms.

For MA of order (q) written as MA(q), (A_t) is defined as:

$$A_t = \mu + \sum_{i=1}^{q} \theta_i \varepsilon_{t-i} + \varepsilon_t \quad (10)$$

Where μ is the mean of the series, $\theta_i,\ldots, \theta_q$ are the parameters for the MA model, ε_t and ε_{t-i} are the white noise errors.

The ARIMA (p, d, q) model where p, d and q are the respective orders for the AR, integrating (differencing) and the MA models which are the parameters to be determined and used for the model is indicated in equation (11) below.

$$\left(1 - \sum_{i=1}^{p} \phi_i L^i\right)(1-L)^d A_t = \left(1 + \sum_{i=1}^{q} \theta_i L^i\right)\varepsilon_t \quad (11)$$

According to [48], [49], L is a backshift or lag operator which operates on an element in a time series to give the previous element.

C. Apache Hadoop

Apache Hadoop is an open-source software platform used in [1], [20]. It is used for writing and running applications that require the processing of a huge amount of data for predictive analytics [50]. It has an efficient framework that utilizes a distributed parallel processing on heterogeneous data for forecasting. It can store and process very big dataset ranging in size from gigabytes to petabytes of data. Hadoop has some good features that have made it very useful in predictive analytics.

- Flexibility: It can store data easily even without prior processing, whether structured or un-structured such as audio, text or video. It is more flexible than SQL-based systems.
- Computational power: The distributed computing model enables the computation of enormous amount of data using many nodes. The more the number of nodes, the more the processing power.
- Scalability: The system can be increased by merely, connecting more nodes to the system.
- Tolerance to fault: Hadoop stores multiple copies of all data automatically and the failure in one of the nodes does not affect the data processing since the task is sent to other functioning nodes for processing.
- Low cost: It is an open-source framework.

D. Windchill

Windchill was used in [17]. It is a tool used for predicting reliability, availability and other reliability-related metrics [51]. It has the features that estimate MBTF, MTTR, failure rate and other user-defined metrics. Windchill is very instrumental in product life management. It provides a comprehensive easy-to-use tool for the estimation of system reliability and MTBF. It allows the early identification of the major contributors to system failure and measures environmental impact on the system.

E. Bayesian Network

Bayesian Networks (BN) are a category of Probabilistic Graphical Model that is used to design models from a dataset and/or several experts' opinion in the particular domain of the expert **[**37**], [**39**], [**40**]**. BNs can also find application in an extensive range of tasks with prediction, time series prediction, anomaly detection, diagnostics, automated insight, reasoning, and decision-making process.

BN has a direct acyclic graph (DAG) that represents the structure, as well as a set of conditional probability tables (CPT). The observed variables are the nodes in the structure, while the edges are called ′probabilistic independence′. The relationship between the variables in the graph is measured by the CPT. Bayes' theorem is used for computing the probability distribution for the nodes. For two events (X) and (Y), Bayes' theorem states that:

$$P(X|Y) = P(Y|X) * \frac{P(X)}{P(Y)} \qquad (11)$$

VI. FUTURE CHALLENGES AND DIRECTION

Future work will entail the development of an intelligent real-time base station availability tool for efficient monitoring and service level delivery. A predictive Model for BTS Availability that will make use of artificial intelligence to adapt to technological advancement and risk mitigation for availability especially with the challenges that will accompany the next-generation technology, the fifth generation 5G.

VII. CONCLUSION

QoS has become very crucial in this era of stiff competition among the various MNOs. Subscribers of the mobile telecommunication network have become very aware of their right to get the best value from the MNOs. We cannot expect an improved QoS if the network availability of the access point – BTS is not guaranteed. Of what benefit will it be, if, after a well-prepared network, one cannot access it? In this paper, we looked at the need to predict the BTS Availability in a bid to proactively improve the BTS Availability and the QoS. To do this, the MSP is furnished with SLA to enforce adherence to the agreement on timely resolution of outages and this, in turn, brings about a reduction in MTTR and this consequently improves BTS Availability.

ACKNOWLEDGMENT

The authors of this paper sincerely appreciate our colleagues, who prefer to be anonymous, for their independent review and comments. We also express our honest gratitude to Dr. Adeiza Onumanyi for his useful advice during the course of this write-up.

REFERENCES

[1] X. Fan, F. Wang, and J. Liu, "Boosting Service Availability for Base Stations of Cellular Networks by Event-driven Battery Profiling, in *Performance Evaluation Revie"*, 2016, vol. 44, no. 2, pp. 88–93, doi: 10.1145/3003977.3004002.

[2] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A Comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016, doi: 10.1109/COMST.2016.2532458.

[3] Q. S. Mahdi, I. I. Hamarash, and J. Hassan, "Survivability Analysis of GSM Network Systems," *Eurasian J. Sci. Eng.*, vol. 3, no. 3, 2018, doi: 10.23918/eajse.v3i3p113.

[4] S. I. Popoola, A. A. Atayero, N. Faruk, and J. A. Badejo, "Data in Brief Data on the Key Performance Indicators for Quality of Service of GSM Networks in Nigeria," vol. 16, pp. 914–928, 2018.

[5] A. I. Kehinde, S. Lawan, F. O. Adunola, and A. I. Isaac, "GSM Quality of Service Performance in Abuja," vol. 7, no. 3, pp. 29–40, 2017, doi: 10.5121/ijcsea.2017.7403.

[6] C. K. Agubor, N. C. Chukwuchekwa, E. E. Atimati, U. C. Iwuchukwu, and G. C. Ononiwu, "Network Performance and Quality of Service Evaluation of GSM," vol. 3, no. 9, pp. 256–263, 2016.

[7] Nishith E and Tripathi D., (1998) "Handoff in cellular systems" IEEE Personal Communication Magazine", pp. 26–37, 2010.

[8] B. Y. Lawal, K. . Ukhurebor, M. . Adekoya, and E. Aigbe, "Quality of Service and Performance Analysis of A GSM Network In Eagle Square, Abuja and Its Environs, Nigeria," *Int. J. Sci. Eng. Res.*, vol. 7, no. 8, pp. 1992–1999, 2016, [Online]. Available: http://www.ijser.org.

[9] A. O. Adelakun, B. Y. Lawal, M. A. Adekoya, and K. E. Ukhurebo, "Chaotic assessment of the key performance indicators for a GSM Network congestion in an election period in Nigeria," vol. 9, no. 1, pp. 28–33, 2019.

[10] O. F. Oseni, S. I. Popoola, H. Enumah, and A. Gordian, "Radio Frequency Optimization of Mobile Networks in Abeokuta , Nigeria for Improved Quality of Service," pp. 174–180, 2014.

[11] A. Olaitan and A. Kehinde, "Assessment of the Reliability of Global Services Mobile Communication Networks on Quality of Services (QoS): A Comparative Study of Four Major Giants," vol. 5, no. 6, pp. 552–562, 2020.

[12] O. N. P. D. Candidate, "Evaluation and Analysis of Key Performance Indicators Which Affect QoS of Mobile Call Traffic," no. 9, pp. 14–30, 2019.

[13] H. Abdulkareem, A. Momodou, S. Tekanyi, A. Y. Kassim, and Z. M. Zakariyya, "Analysis of a GSM Network Quality Of Service Using Call Drop Rate Analysis of a GSM Network Quality of Service Using Call Drop Rate and Call Setup Success Rate as Performance Indicators," no. March, 2020.

[14] N. T. Surajudeen-bakinde, K. A. Adeniji, S. O. Oyeyele, O. Zakariyya, S. A. Olayanju, and A. M. Usman, "Assessment of Quality of Service of GSM Networks in Ilorin Metropolis, Nigeria," vol. 3, no. 1, pp. 147–155, 2020.

[15] R. N. Ali, "Handoff and Drop Call Probability: A Case Study of Nigeria's Global System for Mobile Communications (GSM) Ssector," *Sch. J. Eng. Technol.*, vol. 3, no. 2A, pp. 166–169, 2015.

[16] J. J. Popoola, S. Africa, I. O. Megbowon, and V.S.A. Adeloye, "Journal of Information Technology Impact," vol. 9, no. 2, pp. 91–106, 2009.

[17] A. Hilt, G. Járó, and I. Bakos, "Availability Prediction of Telecommunication Application Servers Deployed on Cloud," *Period. Polytech. Electr. Eng. Comput. Sci.*, vol. 60, no. 1, pp. 72–81, 2016, doi: 10.3311/PPee.9051.

[18] A. Hilt, "Evolution towards Telco-Cloud : Reflections on Dimensioning , Availability and Operability," pp. 1–8, 2019.

[19] A. Hilt, N. M. Networks, Z. Talyigas, and N. Networks, "Comparison of Availability Figures of Distributed Systems Using Multiple Redundancy Methods," no. June, 2016.

[20] T. Mahmood and K. Munir, "Enabling Predictive and Preventive Maintenance using IoT and Big Data in the Telecom Sector," pp. 1–8, 2014.

[21] S. G. Roberti and O. Mihai, "Monitoring the Parameters of the Electronics Devices to Assure the Predictive Maintenance of

Equipment," pp. 832–835, 2017.
[22] M. Di Mauro, M. Longo, F. Postiglione, R. Restaino, and M. Tambasco, "Availability evaluation of the virtualized infrastructure manager in network function virtualization environments," in *Risk, Reliability and Safety: Innovating Theory and Practice - Proceedings of the 26th European Safety and Reliability Conference, ESREL 2016*, 2017, no. January 2020, p. 423, doi: 10.1201/9781315374987-393.
[23] G. Nencioni, B. E. Helvik, A. J. Gonzalez, P. E. Heegaard, and A. Kamisinski, "Impact of SDN Controllers Deployment on Network Availability," 2017, [Online]. Available: http://arxiv.org/abs/1703.05595.
[24] J. Säe and J. Lempiäinen, "Maintaining Mobile Network Coverage Availability in Disturbance Scenarios," *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/4816325.
[25] T. Service and S. Operation, "ITU-T," 2008.
[26] M. Thulin, "Measuring Availability in Telecommunications Networks," p. 50, 2004, [Online]. Available: https://people.kth.se/~e98_thu/thesis/Availability_Thesis_final.pdf.
[27] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger, "General availability model for multilayer transport networks," *Proc. - 2005 DRCN 5th Int. Work. Des. Reliab. Commun. Networks - "Reliable Networks Reliab. Serv.*, vol. 2005, pp. 85–92, 2005, doi: 10.1109/DRCN.2005.1563848.
[28] A. M. Principle, "Chapter 4 of Network Performance and Quality of Service : Basic Calculation of the Network ' s Availability and Reliability," *Ina. Pap.*, pp. 1–13, 2018, doi: 10.17605/OSF.IO/Z5MWQ.
[29] W. Ahmed, O. Hasan, U. Pervez, and J. Qadir, "Reliability modeling and analysis of communication networks," *J. Netw. Comput. Appl.*, vol. 78, pp. 191–215, 2017, doi: 10.1016/j.jnca.2016.11.008.
[30] V. Netes, "End-to-end availability of cloud services," in *Conference of Open Innovation Association, FRUCT*, 2018, vol. 2018-May, pp. 198–203, doi: 10.23919/FRUCT.2018.8468272.
[31] W. Ahmed, O. Hasan, U. Pervez, and J. Qadir, "Reliability modeling and analysis of communication networks," *J. Netw. Comput. Appl.*, vol. 78, pp. 191–215, 2017, doi: 10.1016/j.jnca.2016.11.008.
[32] "Explanation of Terms."
[33] W. Q. Qing, "Introduction to Wireless Network Technology-Huawei Technologies Limited Training Manual." 2017.
[34] C. Esonwune, "Telecommunications Managed Services Model in sub-Saharan Africa – The Pros and Cons :," pp. 1–50, 2010.
[35] I. Hassan, "Of Managed Service Adoption By," vol. 35, no. 1, pp. 157–178, 2019.
[36] N. Tang *et al.*, "No Title□□□□□□," يبيبب, vol. ث قفثق, no. ثق ثفثفثق, p. 2018, ثفثفثفثق.
[37] S. Ibrahimovic and N. Bajgoric, "Modeling Information System Availability by using Bayesian Belief Network Approach," *Interdiscip. Descr. Complex Syst.*, vol. 14, no. 2, pp. 125–138, 2016, doi: 10.7906/indecs.14.2.2.
[38] K. Taga, B. Virag, A. Faggiano, and R. Pell, "Managed services for telecom operators," *Arthur D Little*, 2015, [Online]. Available: https://www.adlittle.com/sites/default/files/viewpoints/ADL_ManagedServicesforTelecomOperators.pdf.
[39] U. Franke, P. Johnson, J. König, and L. Marcks von Würtemberg, "Availability of enterprise it systems: An expert-based bayesian framework," *Softw. Qual. J.*, vol. 20, no. 2, pp. 369–394, 2012, doi: 10.1007/s11219-011-9141-z.
[40] T. Beuzen, K. D. Splinter, L. A. Marshall, I. L. Turner, M. D. Harley, and M. L. Palmsten, "Bayesian Networks in coastal engineering: Distinguishing descriptive and predictive applications," *Coast. Eng.*, vol. 135, no. July 2017, pp. 16–30, 2018, doi: 10.1016/j.coastaleng.2018.01.005.
[41] M. R. Usman, M. A. Usman, and S. Y. Shin, "Channel blocking analysis and availability prediction in cognitive radio networks," in *2017 International Conference on Computing, Networking and Communications, ICNC 2017*, 2017, pp. 963–968, doi: 10.1109/ICCNC.2017.7876264.
[42] J. S. Almeida, "Predictive non-linear modeling of complex data by artificial neural networks," pp. 72–76, 2001.
[43] A. H. Gandomi and D. A. Roke, "Advances in Engineering Software Assessment of artificial neural network and genetic programming as predictive tools," vol. 88, pp. 63–72, 2015, doi: 10.1016/j.advengsoft.2015.05.007.
[44] N. T. Markov, C. Lamy, D. C. Van Essen, K. Knoblauch, and D. Lyon, "A Predictive Network Model of Cerebral Cortical Connectivity Based on a Distance Rule," 2012, doi: 10.1016/j.neuron.2013.07.036.
[45] S. Kayyali, "Resource Management and Quality of Service Provisioning in 5G Cellular Networks," 2019.
[46] I. Rizomyliotis, A. Poulis, G. Apostolos, K. Konstantoulaki, and I. Kostopoulos, "Applying FCM to predict the behaviour of loyal customers in the mobile telecommunications industry," *J. Strateg. Mark.*, vol. 28, no. 1, pp. 1–15, 2020, doi: 10.1080/0965254X.2018.1479720.
[47] G. P. Zhang, "Time series forecasting using a hybrid ARIMA and neural network model," vol. 50, pp. 159–175, 2003.
[48] N. A. Bakar and S. Rosbi, "Autoregressive Integrated Moving Average (ARIMA) Model for Forecasting Cryptocurrency Exchange Rate in High Volatility Environment: A New Insight of Bitcoin Transaction," *Int. J. Adv. Eng. Res. Sci.*, vol. 4, no. 11, pp. 130–137, 2017, doi: 10.22161/ijaers.4.11.20.
[49] H. Özs, "Monitoring unstable slopes in an open pit lignite mine using ARIMA," vol. 120, no. March, pp. 173–180, 2020.
[50] J. Nandimath, "Big Data Analysis Using Apache Hadoop," pp. 700–703, 2013.
[51] K. Benefits, C. Key, and R. Metrics, "Windchill ® Prediction," pp. 1–3.
[52] Tutorials Point Homepage, http://www.tutorialspoint.com.com/, last accessed 2020/09/15.

Students Academic Performance Prediction Based on Square Root Data Transformation and Ensemble Technique

Wokili Abdullahi
Department of Computer Science
Federal University of Technology, Minna
Minna, Nigeria
abdullahwokil@yahoo.com

Morufu Olalere
Department of Cyber Security Science
Federal University of Technology, Minna
Minna, Nigeria
lerejide@futminna.edu.ng

***Abstract*— Data mining research is evolving rapidly in the educational sector because of the vast amount of student information used to detect and explore useful patterns applicable to student learning behaviour. Predicting students' progress is an essential task in any educational institution. To assess student performance, educational institutions may use educational data mining to improve their teaching practices and learning processes. All these modifications lead to enhancing the success of students and overall academic results. In data mining, classification is a popular technique that has been widely tested out to find student outcomes. An approach based on data transformation and the Ensemble method to predict student success is suggested in this report. The efficacy of the student's predictive model is measured using several classifiers: Error-Correcting Output Code (ECOC), K-Nearest Neighbour (KNN), Ensemble, Naïve Bayesian (NB), and Decision Tree (DT). The results obtained by training the different classifiers with square root transformed features improved the classification accuracy from 83% to 86%, thus improving the performance prediction model's overall performance. For the X-API dataset, this suggested technique also created a better prediction accuracy than related works that used the same dataset.**

Keywords*—*Student Performance Prediction, Data Transformation, Educational Data mining, Ensemble, classification

I. INTRODUCTION

In Computer Science, one of the active fields is data mining. Data mining deals with the process of extracting valuable information from raw data [1]. Data mining is crucial due to the rising amount of data and the immediate need to translate these data into practical information. With data mining, a search engine could be used to examine vast volumes of information and instantly report meaningful findings without requiring human participation [2]. The educational sector is a significant area in which data mining is gaining increasing interest. Data mining is referred to as Educational Data Mining (EDM) in the education field. EDM emphasizes that useful knowledge is obtained from educational information systems such as the course management systems, registration systems, online learning management systems, and application systems. This mined knowledge can help students at each stage of their studies, like primary to tertiary education [3]. Many user groups are interested in EDM, and these users use the data that EDM has found according to their vision and intent [4]. For example, educational data's hidden pattern can help educators develop teaching techniques, understand learners, strengthen the learning experience, and use them to boost their learning activities [5]. This secret perception will also help the administration make the necessary decisions to achieve high-quality results [6]. Educational information is obtained from multiple sources, such as educational institution databases, e-learning services and traditional surveys [3]. Predicting the academic success of students is a significant application of EDM. In the educational environment, the analysis and estimation of student performance is an integral aspect. This prediction task foresees the importance of an unknown variable that distinguishes students with outcomes such as pass or failure, grades and marks [7].

Numerous data mining techniques can be used for EDM, including Ensemble, Artificial Neural Networks (ANN), discriminate analysis, decision tree, rule induction, support vector machine, Naïve Bayes, and K-nearest neighbour [8]. A predictive classification model's quality is determined by its ability to identify unknown patterns correctly. The X-API dataset is an educational data set that several researchers have used to predict student academic performance. However, previous works by Francis and Babu [9], Amrieh et al. [5], Tuaha et al. [3] and Amrieh et al. [10] have provided accuracies of less than 83% for the prediction of the X-API dataset. Five classification algorithms were used in this research: K-Nearest Neighbour (KNN), Decision Tree (DT), Error-Correcting Output Codes (ECOC), Naïve Bayes (NB) and Ensemble.

The proposed approach's main objective is to develop the ensemble classification model based on transformed square root features that classify students' performance as low-level, middle-level, and high-level. The significant contribution of this paper consists of:

1. Presentation of a method for student performance prediction.
2. Comparative experimentation of different classifiers trained with transformed and untransformed features.

The arrangement of these studies is as follows: section two presents the relevant works, section three presents the methods used, section four presents the findings and discussion, and finally, conclusions were drawn in section five, and suggestions for future works were presented in section six.

II. RELATED WORK

Students' viability of progress is essential to predict student performance. The significance of predicting student performance has led researchers to become more and more interested in this field. Therefore, various researches have been published to predict students' performance.

A classification model for the prediction of student performance was built by Salal, Abdullaev and Kumar [11] using a dataset of 649 examples with 33 attributes obtained from 2 Portuguese high schools: Gabriel Pereira and Mousinho da Silveira High School. The dataset includes features, such as academic, demographic and social attributes of students. The classification target class ranged from 0 to 20, rendering the classification process extremely difficult as there were only 649 examples to be trained and assessed. Based on the initial class ranges, the target class was reduced to 6 categories due to this complexity. In WEKA software, the correlation assessment, gain ratio, and information gain were used as evaluation techniques, and these new target groups were used to pick attributes. After obtaining the outcome of the attribute selection algorithms' outcome, ten different attributes were selected, which were checked to influence the prediction outcome significantly. Eight classifiers, namely the Naïve Bayes, Random Tree, REP Tree, Decision Tree, Simple Logistics, One R, and Zero R, were fed with these selected classification attributes. One R was identified to have performed better with an accuracy of 76.7334% compared to the other seven classifiers with lower accuracy value. A comparative overview of a relatively large number of classifiers was provided by the study, offering an in-depth understanding of an extensive range of techniques. In this paper, each of the methods' performance was evaluated based only on accuracy without considering other performance metrics, which could say a lot about the suitability of a technique. The classification accuracy achieved was also low, unlike similar works that used the same dataset.

Iyanda et al. [12] conducted a comparison between two Neural Networks (NN) (generalized regression NN and multilayer perceptron) to determine the best model for student academic performance prediction based on only the educational feature of the student. The dataset used was collected from the Department of Computer Science and Engineering of the Awolowo Nigeria University of Obafemi. The data collected constitutes the academic record of learners (raw scores for each course taken) as the input variable, and the associated GPA as the output parameter. Using mean square error, receiver operating features, and accuracy, the two NN models' performance was evaluated. The generalized regression NN proved to perform better with an accuracy of 95% than the multilayer perceptron. However, without considering how demographic, social, and behavioural attributes could affect a student's output, this research used only student academic attributes for prediction.

Olalekan, Egwuche, and Olatunji [13] adapted Bayes' theorem and ANN to construct a predictive model for students' graduation probability at a tertiary institution. Four variables were used for prediction: Unified Tertiary Matriculation Test, Number of Sessions at the high school level, Grade Points at the high school level and Entry Mode. The data used was collected from the Computer Science School, Federal Polytechnic, Ile-Oluji, in Ondo State, Nigeria. The data were composed of 44 examples with five attributes. The study concludes that the ANN has a 79.31% higher performance accuracy than the 77.14% obtained by the Bayes classification model. The ANN precision improved as the hidden layers increased. As compared to other previous works, the overall accuracy in this study was low because of the small size of data used. Expanding the data size would help enhance the accuracy of the classification of the model.

Magbag and Raga [14] focused on building a model to predict first-year students' academic success in tertiary education. This research aimed to allow early intervention to help students stay on course and reduce non-continuance. The data utilized in this paper were obtained from three higher education institutions in Central Luzon, primarily in the cities of Angeles, San Fernando and Olongapo. The study subjects included first-year students from 8 academic departments from 2018-2019; Arts and Sciences, Engineering and Architecture, Computer Studies, Criminology, Education, Hospitality and Tourism, Business and Accountancy, Nursing and Allied Medical Sciences. The dataset was composed of 4,762 examples. The dataset was pre-processed, and missing values were deleted, leaving 3,466 available samples. Using Correlation-based Feature Selection, Gain Ratio and Information Gain for feature rating, feature selection was carried out. Using these selected features, the NN and logistic regression models were trained and evaluated. In comparison with similar works, the scale of the dataset used rendered the scheme more robust. However, the accuracy of 76% achieved in this analysis is low.

A new prediction algorithm to determine students' progress in academia using a hybrid (classification and clustering) Francis and Babu [9] proposed a data mining technique. The analysis used information from X-API education obtained from the kaggle repository consisting of 16 attributes with 480 instances. The dataset characteristics are demographic, academic, behavioural, and additional attributes (parent school satisfaction, student absentee days and parent response survey). Using classifiers such as SVM, Naïve Bayes, Decision tree, and NN, feature selection experiments were performed.

The selection of attributes was based on the accuracy provided by each classifier after the demographic, academic, behavioural and extra attributes were trained separately. Compared to using behavioural characteristics alone, additional features alone, educational features alone or demographic features alone the academic + behavioural + extra features provided a higher classification accuracy. These selected features were used as input for K-mean clustering and the majority vote approach. When applied to the dataset's academic, behavioural, and additional features, the proposed hybrid approach achieved an accuracy of 75.47%. However, related works using the X-API education dataset achieved greater accuracy of approximately 82% compared to this study.

III. METHODOLOGY

The methods used to carry out this research work are discussed in this section. Fig. 1 demonstrates the methods and processes that have been used to achieve the purpose of this study. Each of the measures shown in Fig. 1 is discussed in the sub-sections below.

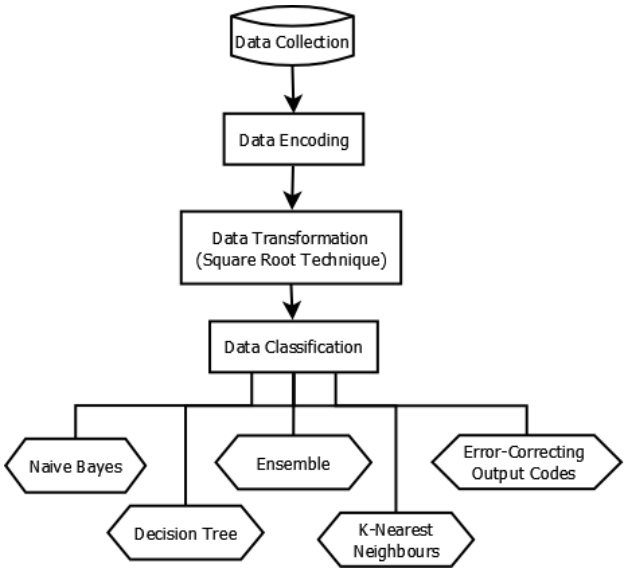


Fig. 1 Proposed System

A. *Dataset*

The data utilized in this research was gotten from Kaggle.com. The data is called X-API as it was collected from Kalboard 360 E-Learning system using eXperience API (X-API). The dataset is multivariate with 480 instances, 16 attributes and no missing values. The attributes are grouped into three major categories:

1. Demographic features, such as nationality and gender.
2. Academic background features such as grade level, educational level, and section.
3. Behavioural features such as viewing resources, raised a hand in class, school satisfaction, and parents' answering survey.

The dataset composes of 175 females and 305 males. The students came from various countries such as 172 students from Jordan, 179 students from Kuwait, 22 students from Iraq, 4 students from Morocco, 28 students from Palestine, 17 from Lebanon, 11 from Saudi Arabia, 12 from Tunis 9 students from Egypt, 7 from Syria, 6 from USA, Iran and Libya, and one student from Venezuela. The dataset was collected over two academic semesters: 245 student records were compiled in the first semester, and 235 student records were collected in the second semester. This dataset also contains a new category of features; this feature is parent parturition in the educational process. Parent participation feature has two sub-features: Parent Academic Satisfaction and Parent Answering Survey. Two hundred seventy (270) parents answered the survey, and 210 are not, 292 of the parents are satisfied with the school, and 188 are not. This dataset was used by [9], [3] [10] and [5]. The X-API dataset features and the description of these features are is presented in Table 1.

TABLE 1 FEATURES OF X-API DATASET AND THEIR CATEGORIES

S/ No	Attribute	Attribute Description	Data Type	Attribute Category
1	Gender	Student Gender (Male or Female)	Categorical	Demographic Attributes
2	Nationality	Nationality of the student	Categorical	
		(Lebanon, Kuwait, Egypt, USA, Saudi-Arabia, Jordan, Iran, Venezuela, Tunis, Syria, Morocco, Palestine, Lybia, Iraq)		
3	Place of Birth	(Lebanon, Kuwait, Egypt, USA, Saudi-Arabia, Jordan, Iran, Venezuela, Tunis, Syria, Morocco, Palestine, Lybia, Iraq)	Categorical	
4	Parent Responsible	The parent who is responsible for the student (Mom or Dad)	Categorical	
5	Educational Levels	The educational level a student belongs to (lower-level, Middle-School, High-School)	Categorical	Academic Attributes
6	Section ID	The classroom a student belongs to (A, B or C)	Categorical	
7	Course	Offered courses (Spanish, English, French, IT, Arabic, Chemistry, Maths, Biology, History, Science, Quran, Geology)	Categorical	
8	Student Semester	Student school semester (First or Second)	Categorical	
9	Student Grade	The grade category student belongs (G-01, G-02, G-03, G-04, G-05, G-06, G-07, G-08, G-09, G-10, G-11, G-12)	Categorical	
10	Student punctuality to class	Amount of days of absence of a student in the class (above-7 or under-7)	Categorical	
11	Raising of Hand	Number of times a student raised their hands (0-100)	Integer	Behavioural Attributes
12	Number of visited resources	The number of times a student visited a course content (0-100)	Integer	
13	Announcements viewed	The number of time the student checks a new announcement (0-100)	Integer	
14	Discussion Group	The number of time the student participated in discussion groups (0-100)	Integer	
15	Parents Answering Survey	If the parent answered the surveys provided	Categorical	Extra Attributes

		by the school (Yes or No)		
16	Satisfaction of Parent	If parents are satisfied with the school (Yes or No)	Categorical	
17	Class	The students are categorized into three numerical intervals based on their total grade (Low-level (0-69), Middle-level (70-89), or High-level (90-100)	Categorical	Target Class/Attribute

B. Data Encoding

There are both numeric variables and categorical variables in the dataset used. In this phase, the categorical data types of attributes were converted to numeric attributes. Data encoding was done because specific machine learning algorithms such as Naïve Bayes, vector machine support and Ensemble need numeric attribute types to work. In dealing with numeric data types, machine learning models have also proven to be efficient. The label encoding technique was employed in this research. Each label was converted to an integer value. For instance, the gender, which is in a categorical data form (Male and Female), was encoded to integer 1 and 2. Table 1 and Table 2 indicate gender encoding and target class encoding, respectively.

TABLE 2 ENCODING GENDER

Gender (categorical)	Gender (integer)
Male	1
Female	2

TABLE 3 ENCODING TARGET CLASS

Target Class (categorical)	Target Class (integer)
High-Level (90-100)	1
Middle-Level (70-89)	2
Low-Level (0-69)	3

C. Data Transformation

Transformations of the data can reduce the skewness of data and the effect of outliers in the data. Transformation approaches include centring, scaling, removal of skewness, and binning. This study used the square root transformation technique to convert a skewed distribution into a normal/less-skewed distribution. The square root of all the predictor variables was derived. Square roots that were obtained were then used to train the classifiers as inputs. In equation 1, the square root transformation formula is provided. The square root of a number A is a number B such that:

$$B^2 = A \tag{1}$$

D. Data Classification

Machine learning capability lies in its ability to generalize by correctly classifying unknown information based on models developed using the training dataset. Several machine learning classification models were used for training and classification, namely, Error-Correcting Output Codes (ECOC), Naïve Bayes (NB), Decision Tree (DT), Ensemble, and K-Nearest Neighbor. In this research work students were grouped into three numerical intervals according to their overall grade:

1. Low-Level: ranges from 0 to 69,
2. Middle-Level: ranges from 70 to 89,
3. High-Level: ranges from 90-100.

Each of the five classifiers was trained to classify students into the three classes with the square root transformed data and the data that was not altered. 80% of the data was used for training, and the remaining 20% was used to test the trained models. These five classes are presented below.

1) Error-Correcting Output Codes (ECOC)

Machine learning models are built for binary classification problems, such as Support Vector Machine (SVM) and logistic regression. As such, these binary algorithms either need to be updated or not used at all for multiclass classification problems. The ECOC technique is a tool that allows the issue of multiclass classification to be interpreted as multiple problems of binary type, enabling the direct use of native binary classification models[15]. The ECOC enables the encoding of an infinite number of binary classification problems for each class [16]. ECOC designs are independent of the classifier depending on the implementation. ECOC has error-correcting properties and has shown that the learning algorithm's bias and variance can be decreased [17].

Given a classification problem with Y_c The key aim of ECOC is to create a binary or ternary "codeword" for each class. The codewords are arranged as rows of a matrix X. *Codematrix* X is defined in equation 2.

$$X \in \{-1,0,+1\}^{Y_c \, x \, L} \tag{2}$$

Where L is the code length. From the learning point of view X specifies Y_c classes to train L dichotomizes, $a, a_2, \dots, a_L$. A classifier a_1 is trained according to the column $X\ (.\,, l)$.

2) Naive Bayes (NB)

The NB classifier is a probabilistic machine learning model based on the Bayes theorem's use with assumptions of high independence between the features. NB is used for a classification task. To predict the type of test data set, NB is fast, convenient and straightforward. In multiclass forecasting, it also suits nicely [18]. When assuming independence, a Naive Bayes classifier performs better than other models, such as logistic regression, and less data for training is needed. However, the theory of independent predictors is an important limitation of NB [19]. The Bayes theorem provides a way for P(a|b)from (a), P(b) and P(b|a) to measure the posterior likelihood. In equations 3 and 4, the posterior probability is shown in the formula. Bayes theorem provides a way of calculating posterior probability $P(a|b)$ from $P(a)$, $P(b)$ and $P(b|a)$. The posterior probability is formula is shown in equation 3 and 4.

$$P(a|b) = p(b|a) \times P(a) \Big/ p(b) \tag{3}$$

$$P(a|b) = \frac{P(b_1|a) \times P(b_2|a) \times \dots \times P(b_n|a) \times P(a)}{P(b_1,\dots,b_n)} \tag{4}$$

Where P(a|b) is the posterior likelihood of class (a, target) given predictor (b, attributes). P(a) is the prior probability of class. p(b|a) is the likelihood of a predictor given a category. $p(b)$ is the prior likelihood of a predictor.

3) Decision Tree (DT)

A DT is a simple and commonly used predictive modelling technique. DT is a type of supervised learning where, according to a particular parameter, the data is continually split [20]. The decision tree uses a tree-like model to go from observations on an item (represented in the branches) to conclusions on the target value of an item (defined in the leaves) [21]. Regression and classification problems can be solved using the DT algorithm. DT is easy to understand and view. It does not require normalization of data and preparation of data; it needs less effort. The decision to do strategic splits has a significant effect on a tree's precision [22]. Entropy, information gain and reduction invariance are techniques used in determining which attribute to the position at the root or the different levels of the tree.

Entropy is a measure of randomness in processed information. The larger the entropy, the more challenging it is to draw any conclusions from that data. A branch with an entropy of zero, for example, is chosen as the root node, and further division is required for a branch with an entropy greater than zero [22]. In equation 5, entropy for a single attribute is expressed.

$$E(S) = \sum_{i=1}^{n} -p_i log_2\, p_i \quad (5)$$

Where S is the current state, p_i is the probability of an event i of state S.

Information Gain (IG) is a statistical property that tests how well the training examples are segregated according to their target classification by a given attribute. In equation 6, information gain is expressed mathematically.

$$IG = Entropy(before) - \sum_{j=1}^{N} Entropy\,(j, after) \quad (6)$$

Where "before" is the dataset before the split, N is the number of subsets generated by the division, and (j, after) is subset j after the division.

Reduction invariance is an algorithm that is used for problems with regression. This algorithm uses the standard formula of variance to select the best split. As the criterion to divide the population, the split with lower variance is chosen. In equation 7, the standard variance formula used in this technique is represented.

$$variance = \frac{\sum(X-\mu)^2}{n} \quad (7)$$

Where $\mu$the mean of the values and X is the actual value and n is the number of values.

4) K-Nearest Neighbour (KNN)

The K-Nearest Neighbours (KNN) algorithm is a non-parametric supervised machine learning algorithm used to solve both classification and regression problems [23]. The KNN algorithm assumes the closeness of related objects. In KNN, an item is grouped by its neighbours' majority vote, with an object being assigned to the most common class of its k-nearest neighbours [24]. KNN does not need a training phase. KNN, however, suffers from the curse of dimensionality, and it is vulnerable to outliers. The Euclidean distance is a commonly used similarity measure in KNN [25]. The Euclidean distance is the linear distance between two points in Euclidean space. In equation 8, the Euclidean distance is expressed.

$$D(p,q) = \sqrt{\sum_{i=1}^{n}(q_i - p_i)^2} \quad (8)$$

Where p, q are two points in Euclidean n-space, $q_i\ and\ p_i$ are the Euclidean vectors, starting from the origin of the space and n is the n-space.

5) Ensemble Classifier

An ensemble learning model combines predictions from multiple models with a two-fold goal: the first objective is to maximize prediction accuracy compared to a single classifier[5]. The second gain is more critical generalizability due to multiple advanced classifiers. As a result, solutions, where a single prediction model would have problems, can be discovered by an ensemble. A key rationale is that an ensemble can select a set of hypotheses out of a much larger hypothesis space and combine their predictions into one [26]. Via voting or weighted voting of their forecast for the final estimates, classifiers in the ensemble learning model are merged into meta-classifiers [26].

E. Performance Metrics

In this study, five performance measures were used to evaluate the proposed method. These measures are explained below.

1. **Precision:** This is a measure that computes the number of positive predictions made that are accurate. It is determined as the proportion of positive instances correctly predicted, divided by the total number of positive cases predicted. Precision is mathematically represented in equation 9.

$$Precision = \frac{Truepositives}{Truepositives + Falsepositives} \quad (9)$$

2. **Recall:** This indicator evaluates the amount of correct positive predictions that could have been made out of all positive predictions. The formula in equation 10 represents recall.

$$Recall = \frac{Truepositives}{Truepositives + Falsenegatives} \quad (10)$$

3. **F-Score:** this is the harmonic mean of precision and recall. The formula in equation 11 represents F-Score.

$$\mathrm{F-Score} = 2 * \frac{\mathrm{precision} * \mathrm{recall}}{\mathrm{precision} + \mathrm{recall}} \quad (11)$$

4. **Accuracy:** Accuracy can be defined as the rate of correct classifications. Accuracy is calculated in equation 12.

$$\mathrm{ACC} = \frac{\text{True Positive + True negative}}{\text{True Positive + True negative + False Positive + False negative}} \quad (12)$$

5. **Receiver operating characteristic (ROC) curve:** is a graph showing the performance of a classification model at all classification thresholds. This curve plots two parameters: True Positive Rate (recall) and False Positive Rate.

IV. RESULTS AND DISCUSSION

In this work, experiments were conducted on five algorithms: Decision Tree (DT), KNN, Ensemble, ECOC and NB classifiers for features without data transformation and transformed (square root) features. Two kinds of experiments were conducted, which are:

1. Classification of student performance using data transformed features.

2. Classification of student performance based on normal features (Features without data transformation).

The outcomes of the two experiments conducted using the five classifications techniques mentioned above are shown in Table 4 and Table 5.

TABLE 4 CLASSIFICATION WITH FEATURES WITHOUT DATA TRANSFORMATION

No Feature transform										
Algorithm	***Precision (class A)***	***Precision (class B)***	***Precision (class C)***	***Recall (class A)***	***Recall (class B)***	***Recall (class C)***	***F-Score (class A)***	***F-Score (class B)***	***F-Score (class C)***	***Accuracy***
ECOC	0.7051	0.8462	0.5750	0.6667	0.8148	0.6216	0.6857	0.8302	0.5974	0.6900
Ensemble	0.7941	0.8846	0.8250	0.8182	0.9200	0.7857	0.8060	0.9020	0.8049	0.8300
KNN	0.4412	0.7692	0.7250	0.6522	0.8696	0.5370	0.5263	0.8163	0.6170	0.6400
NB	0.7642	0.8846	0.5750	0.6667	0.8519	0.6765	0.7123	0.8679	0.6216	0.7200
DT	0.6176	0.7692	0.6750	0.7000	0.7692	0.6136	0.6553	0.7692	0.6429	0.6800

In this study, student performance is classified into three classes: low-level, Middle-level and high-level. The low-level is represented as class A, middle-level is represented as class B and high-level is defined as class C. The precision, recall and f-score of the three classes for each of the five classifiers trained with data without transformation are shown in Table 4. Table 4 shows that the ensemble method produced a higher classification accuracy of 83% than the other four classifiers. Ensemble classifier also had a better precision, recall and f-score for all the three target classes than the other four classifiers. .Fig. 2 presents a ROC curve for curve comparing the DT, NB, ECOC, Ensemble and KNN classifier trained with data that were not transformed.

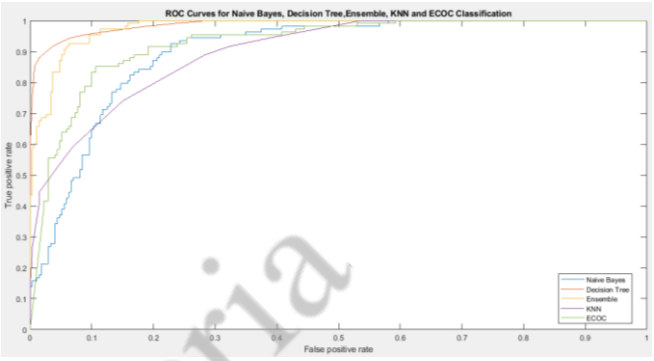


Fig. 2 ROC Curve comparing the DT, NB, ECOC, Ensemble and KNN classifier performances trained with data without transformation.

TABLE 5 CLASSIFICATION PERFORMANCE WITH TRANSFORMED FEATURES

Feature transform										
Algorithm	***Precision (class A)***	***Precision (class B)***	***Precision (class C)***	***Recall (class A)***	***Recall (class B)***	***Recall (class C)***	***F-Score (class A)***	***F-Score (class B)***	***F-Score (class C)***	***Accuracy***
ECOC	0.6970	0.9286	0.7949	0.7931	0.9286	0.7209	0.7419	0.9286	0.7561	0.8000
Ensemble	0.9091	0.9643	0.7436	0.8108	0.8710	0.9063	0.8571	0.9153	0.8169	0.8600
KNN	0.6667	0.9643	0.6923	0.7857	0.7941	0.7105	0.7213	0.8710	0.7013	0.7600
NB	0.9091	0. 9643	0.6410	0.7692	0.8438	0.8621	0.8333	0.9000	0.7353	0.8200
DT	0.8485	0.8929	0.6667	0.7368	0.8621	0.7879	0.7887	0.8772	0.7222	0.7900

From the classification result in Table 5, the ensemble method produced a higher classification accuracy of 86% compared to the other four classifiers. The Ensemble method also created a better precision, recall and f-score for all the three target classes than the other four classifiers.

Fig. 3 presents a ROC curve for curve comparing the DT, NB, ECOC, Ensemble and KNN classifier trained with a transformed feature set.

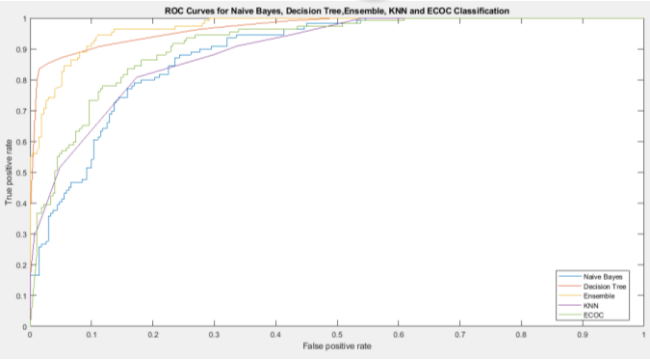


Fig. 3 ROC Curve comparing the DT, NB, ECOC, Ensemble and KNN classifier performances trained with untransformed features

Table 6 compares the accuracy of NB, DT, KNN, ECOC and Ensemble after being trained with untransformed features and transformed features. Based on the result shown in Table 6, each of the five classifiers performed better when prepared with the transformed features. Ensemble method achieved an accuracy of 86% when trained with the transformed features and achieved an accuracy of 83% when trained with untransformed features. NB achieved an accuracy of 82% when trained with the transformed features and achieved an accuracy of 72% when trained with untransformed features. ECOC, KNN and DT also achieved higher accuracy when trained with the transformed features.

TABLE 6 COMPARISON OF DT, KNN, ENSEMBLE, ECOC AND NB PERFORMANCE FOR UNTRANSFORMED FEATURES AND TRANSFORMED FEATURES

	ACCURACY	
Algorithm	***Untransformed features***	***Data Transformed Features***
ECOC	0.6900	0.8000
Ensemble	0.8300	0.8600
KNN	0.6400	0.7600
NB	0.7200	0.8200
DT	0.6800	0.7900

Fig. 4 shows a comparison of DT, KNN, Ensemble, ECOC and NB accuracy when trained with untransformed features and transformed features.

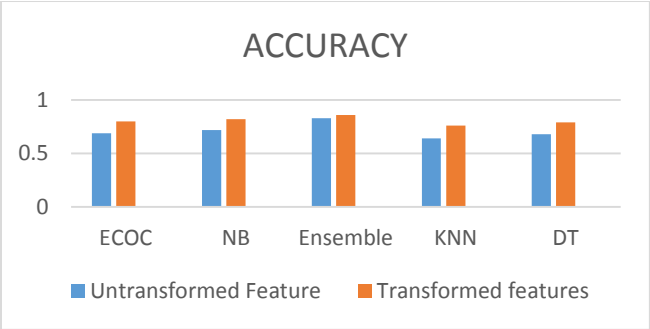


Fig. 4 Comparison of DT, KNN, Ensemble, ECOC and NB performance for untransformed features and transformed features

Table 7 and Fig. 5 compare the proposed method with related works that used the X-API dataset. From the results in Table 7, it can be seen that this study produced a better classification accuracy of 86% for the X-API dataset when compared with previous works.

TABLE 7 COMPARISON OF THE PROPOSED METHOD WITH RELATED WORKS

Algorithm	Dataset	Accuracy (%)
Ensemble (Proposed Method)	X-API	**86.0**
Artificial Neural Network [3]	X-API	78.1
Artificial Neural Network [10]	X-API	73.8
Decision Tree [5]	X-API	82.2
Clustering + Decision Tree [9]	X-API	75.5

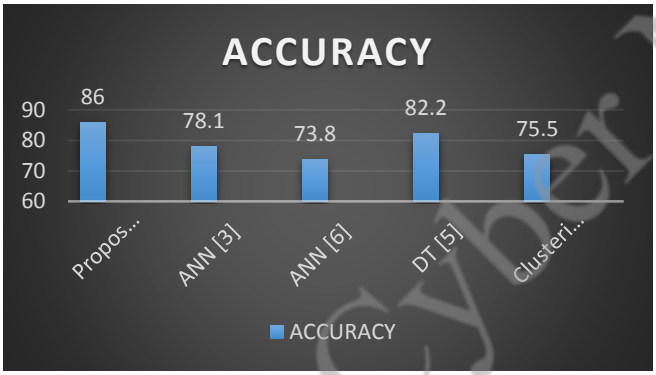


Fig. 5 Comparison of the proposed method with related works

V. CONCLUSION

This study performed a comparative result for five classifiers: KNN, DT, Ensemble, NB and ECOC in respect to student performance prediction for X-API dataset. The proposed method obtained a higher classification accuracy than previous works that used the X-API dataset. From this research, it can be established that the application of square root transformed features for training classifiers can improve the classification accuracy. Square root transformation reduces right skewness, and it also has the advantage that it can be applied to zero values. In conclusion, a system was developed which can accomplish student academic performance prediction.

VI. FUTURE WORKS

Only the square root transformation method was in this study. For future work, more transformation techniques could be applied to evaluate their effect on classification accuracy. In this study, only the X-API dataset was used. Other datasets may be considered to enhance the model robustness. Experiments may also be carried out using more data mining techniques such as genetic algorithms and discriminate analysis model.

REFERENCES

[1] S. Hussain, N. Abdulaziz Dahan, F. M. Ba-Alwi, and N. Ribata, "Educational Data Mining and Analysis of Students' Academic Performance Using WEKA," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 9, no. 2, p. 447, Feb. 2018, doi: 10.11591/ijeecs.v9.i2.pp447-459.
[2] S. Rajagopal, "Customer Data Clustering using Data Mining Technique," vol. 3, no. 4, 2011, doi: 10.5121/ijdms.2011.3401.
[3] S. Tuaha, I. F. Siddiqui, and Q. Ali Arain, "Analyzing Students' Academic Performance through Educational Data Mining," *3C Tecnol. Innov. Apl. Pyme*, pp. 402–421, May 2019, doi: 10.17993/3ctecno.2019.specialissue2.402-421.
[4] C. Romero and S. Ventura, "Educational Data Mining: A Review of the State of the Art," *IEEE Trans. Syst. Man Cybern. Part C, Appl. Rev.*, vol. 40, no. 6, pp. 601–618, Nov. 2010, doi: 10.1109/TSMCC.2010.2053532.
[5] E. A. Amrieh, T. Hamtini, and I. Aljarah, "Mining Educational Data to Predict Student's academic Performance using Ensemble Methods," *Int. J. Database Theory Appl.*, vol. 9, no. 8, pp. 119–136, Aug. 2016, doi: 10.14257/ijdta.2016.9.8.13.
[6] M. B. Shah, M. Kaistha, and Y. Gupta, "Student Performance Assessment and Prediction System using Machine Learning," in *2019 4th International Conference on Information Systems and Computer Networks*, Mathura, India, Nov. 2019, pp. 386–390, doi: 10.1109/ISCON47742.2019.9036250.
[7] M. Imran, S. Latif, D. Mehmood, and M. S. Shah, "Student Academic Performance Prediction using Supervised Learning Techniques," *Int. J. Emerg. Technol. Learn. IJET*, vol. 14, no. 14, p. 92, Jul. 2019, doi: 10.3991/ijet.v14i14.10310.
[8] L. M. Abu-Zohair, "Prediction of Student's performance by modelling small dataset size," *Int. J. Educ. Technol. High. Educ.*, vol. 16, no. 1, p. 27, Dec. 2019, doi: 10.1186/s41239-019-0160-3.
[9] B. K. Francis and S. S. Babu, "Predicting Academic Performance of Students Using a Hybrid Data Mining Approach," *J. Med. Syst.*, vol. 43, no. 6, p. 162, Jun. 2019, doi: 10.1007/s10916-019-1295-4.
[10] E. A. Amrieh, T. Hamtini, and I. Aljarah, "Pre-processing and analyzing educational data set using X-API for improving student's performance," in *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Amman, Jordan, Nov. 2015, pp. 1–5, doi: 10.1109/AEECT.2015.7360581.
[11] Y. K. Salal, S. M. Abdullaev, and M. Kumar, "Educational Data Mining: Student Performance Prediction in Academic," vol. 8, no. 4, p. 6, 2019.
[12] A. R. Iyanda, O. D. Ninan, A. O. Ajayi, and O. G. Anyabolu, "Predicting Student Academic Performance in Computer Science Courses: A Comparison of Neural Network Models," *Int. J. Mod. Educ. Comput. Sci.*, vol. 10, no. 6, pp. 1–9, Jun. 2018, doi: 10.5815/ijmecs.2018.06.01.
[13] A. M. Olalekan, O. S. Egwuche, and S. O. Olatunji, "Performance Evaluation Of Machine Learning Techniques For Prediction Of Graduating Students In Tertiary Institutions," in *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, Ayobo, Ipaja, Lagos, Nigeria, Mar. 2020, pp. 1–7, doi: 10.1109/ICMCECS47690.2020.240888.
[14] A. Magbag and R. R. Jr, "Prediction Of College Academic Performance Of Senior High School Graduates Using Classification Techniques," vol. 9, no. 04, p. 6, 2020.
[15] G. Armano, C. Chira, and N. Hatami, "Error-Correcting Output Codes for Multi-Label Text Categorization," p. 12, 2013.
[16] T. G. Dietterich and G. Bakiri, "Solving Multiclass Learning Problems via Error-Correcting Output Codes," *J. Artif. Intell. Res.*, vol. 2, pp. 263–286, Jan. 1995, doi: 10.1613/jair.105.
[17] S. Escalera, O. Pujol, P. Radeva, and P. Ivanova, "Error-Correcting Output Codes Library," *J. Mach. Learn. Res.*, vol. 11, p. 4, 2010.
[18] P. Bhargavi, M. Tech, and D. S. Jyothi, "Applying Naive Bayes Data Mining Technique for Classification of Agricultural Land Soils," p. 7, 2009.
[19] "Comparative Study of K-NN, Naive Bayes and Decision Tree Classification Techniques," *Int. J. Sci. Res. IJSR*, vol. 5, no. 1, pp. 1842–1845, Jan. 2016, doi: 10.21275/v5i1.NOV153131.
[20] N. Patel and D. Singh, "An Algorithm to Construct Decision Tree for Machine Learning based on Similarity Factor," *Int. J. Comput. Appl.*, vol. 111, no. 10, pp. 22–26, Feb. 2015, doi: 10.5120/19575-1376.

[21] K. David Kolo, S. A. Adepoju, and J. Kolo Alhassan, "A Decision Tree Approach for Predicting Students Academic Performance," *Int. J. Educ. Manag. Eng.*, vol. 5, no. 5, pp. 12–19, Oct. 2015, doi: 10.5815/ijeme.2015.05.02.
[22] A. S. Olaniyi, S. Y. Kayode, H. M. Abiola, S.-I. T. Tosin, and A. N. Babatunde, "STUDENT'S PERFORMANCE ANALYSIS USING DECISION TREE ALGORITHMS," p. 8, 2017.
[23] Z. Zhang, "Introduction to machine learning: k-nearest neighbours," *Ann. Transl. Med.*, vol. 4, no. 11, pp. 218–218, Jun. 2016, doi: 10.21037/atm.2016.03.37.
[24] A. Kataria and M. D. Singh, "A Review of Data Classification Using K-Nearest Neighbour Algorithm," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 6, pp. 354–360, 2013.
[25] X. Gu, L. Akoglu, and A. Rinaldo, "Statistical Analysis of Nearest Neighbor Methods for Anomaly Detection," in *33rd Conference on Neural Information Processing Systems*, Canada, 2019, p. 11.
[26] O. W. Adejo and T. Connolly, "Predicting student academic performance using multi-model heterogeneous ensemble approach," *J. Appl. Res. High. Educ.*, vol. 10, no. 1, pp. 61–75, Feb. 2018, doi: 10.1108/JARHE-09-2017-0113.

A SURVEY ON ANTENNA SELECTION

Basil Ozuluonye
Telecommunication Department
Federal University of Technology, Minna
ozuluonye.pg915008@st.futminna.edu.ng

Henry Ohize
Electrical Department
Federal University of Technology, Minna
henryohize@futminna.edu.ng

Achonu Adejo
Telecommunication Department
Federal University of Technology, Minna
achonu@futminna.edu.n

***Abstract* – Next generation 5G and 6G seek to achieve all-time connectivity for heterogeneous devices. This implies that the devices must stay connected irrespective of channel status. Using diversity in multi-antenna devices, communicating nodes explore different channel paths to improve link reliability. Due to prohibitive implementation costs, antenna selection has been adopted for mobile telecommunication. In the work presented here the authors consider the various approaches in antenna selection, and develop accurate taxonomy to represent current efforts. The rest of the work is organised as follows: section I is the introduction, section II the system model, section III contains discussions on the antenna selection taxonomy, section IV analysis methodology, section V open research areas and section VI concludes the work.**

Keywords – 5G, 6G, Multiple in multiple out MIMO, Suboptimal, Sum rate, JASUS

INTRODUCTION

5G and 6G wireless communication promises to further improve cellular communication performance with increased bit-rates in orders of gigabits/seconds, extremely low latency for communication networks and quality of service. One technology that has made the expected improvements possible is the multiple-in multiple-out (MIMO) system in which communicating nodes may have more than one antenna.

Having more antennas at either ends of the communication link of a MIMO system can improve both link quality and signal-to-noise ratio (SNR). However, despite the immense benefits of MIMO in 5G and beyond, the MIMO technology comes with very high implementation cost because of the sheer number of radio frequency (RF) chains required to be connected to the antennas. Well known components of the RF chain include the digital/analogue converters (DAC), intermediate frequency generator, analogue-to-digital converter (ADC), mixer, RF filter, RF amplifier, local oscillator and modulator.

In antenna selection, algorithms are developed to search a device for antennas based on specific objectives for a user or group of users. The antennas are then connected to available RF chains for transmission or reception. The search may be optimal or sub-optimal, where the former yields better objective output for users but is known to be computationally intensive, while the latter trades marginally poorer outcomes with lower computational difficulty. It has been observed that when the right subset of antennas are selected in the devices, communication can be conducted reliably as if all antennas were indeed used to transmit or receive [1][2]. Consider the forward and reverse link communication between a multi-antenna base station and users within the cell range, as represented in figure 1 below.

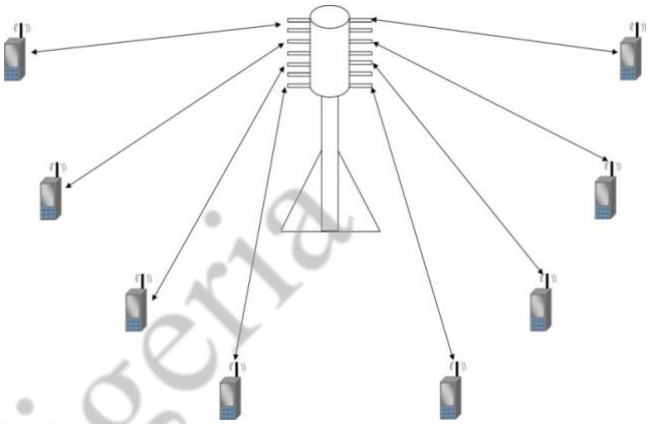


Figure 1: Uplink and downlink in massive user MIMO system

Contributions of the paper

The objective of this work is to offer insight into possible research areas in this field while providing readers a comprehensive overview of the taxonomical classification in the field of MIMO antenna selection.

SYSTEM MODEL

The relationship between the input and output in a MIMO antenna selection is expressed below: [2]

$$y_k(t) = H_k x_k(t) + n_k(t)$$

Where y_k is signal intercepted at the user equipment at time t, H is the channel gain matrix, x is the transmitted bit and n is the white Gaussian noise present. Most of the surveyed works considered Rayleigh fading wireless communication environment. Both $yk, Hk \in \mathbb{C}Nrk \times 1$

MIMO capacity can be expressed as:

$$C = \log_2(1 + \rho H)$$

Where C is the capacity, H is the channel matrix, and ρ is the signal-to-noise ratio (SNR). Since more than one antenna is capable of exploiting channel condition in a MIMO system, the achievable capacity is therefore higher. With the implementation of antenna selection, only the most suitable

antennas are selected by the switching algorithm as seen in figure 2.

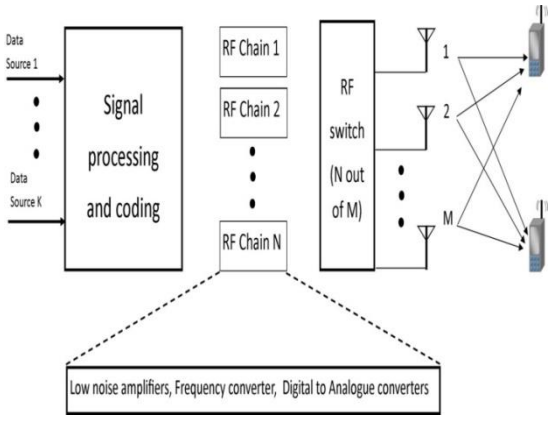


Figure 2: Multi-user MIMO in the downlink path for K number of users

DISCUSSIONS ON ANTENNA SELECTION TAXONOMY

This work attempts to intuitively categorise works done in AS, using taxonomy developed by the authors in order to properly represent the solutions provided in various antenna selection (AS) schemes. We shall consider the following:

SNR-based antenna selection techniques (ASTs),
Capacity-based ASTs,
Energy-aware ASTs,
Joint AS and User Selection (JASUS),
Statistical ASTs,
Distributed ASTs, and
Heuristic ASTs.

SNR-Based Antenna Selection Techniques

SNR based antenna selection techniques involve subset selection criteria in which the antenna elements with the highest instantaneous signal-to-noise ratio (SNR) are selected. The authors in [3] and [4] develop computationally efficient AS algorithms, called the subset-based joint AS (SJ-AS) to maximise channel SNR. In order to improve channel robustness against distortion and loss, the method in [5] uses the Frank Wolfe FW method with the minimisation of signal Weighted Mean Square Error (WMMSE) at the base station.

Classification	Description	References
SNR-based AS	AS in which SNR of received signal is objective	[3][4][5]
Capacity-based AS	AS in which achievable capacity if channel is objective	[2][6][7][8][9][10][11][12][13][14][15] [16][17][18][19][20]
Energy-aware AS	AS in which energy conservation is objective	[21][22][23][24][25][26][27][28][29]
JASUS AS	AS scheme which combines selection with user targets	[1][30][31][32]
Statistical AS	AS approach which is primarily analytical of different schemes	[33][34][35][36][37][38][39]
Distributed AS	AS approach which combines antennas from remote nodes	[40][41]
Heuristic AS	AS approach carried out by machine learning and self-correcting programs	[42],[43],[44],[45],[46],[47],[48],[49]

Table 1: Taxonomy of current research in antenna selection

Capacity-Based ASTs

Capacity based AS techniques involve selection criteria based on which elements have the highest achievable channel capacity. This classification would also include the determination of secrecy outage probability, SOP for RF networks which have unknown embedded receivers, such that the SOP could also form the basis for AS decisions. Antenna selection in the downlink is investigated in [2] by using cylindrical arrays. In [6] the author investigated capacity maximisation in a multi-antenna MIMO where the capacity is incremented by the AS.

The authors in [7] proposed an AS scheme that improves what is termed as Secrecy Outage performance (SOP) for mutli-antenna wiretap. Authors' work in [8] seeks to maximise the achievable sum-rate under a set of constraints, including the transmit power. Authors in [9] investigate AS in a mutli-antenna wiretap system for various channels, where AS is carried out with an eavesdropper receiver.

Information rate is the objective of the authors' work in [10] where a two-step algorithm was proposed, both algorithms are based on polynomial complexity 2-way link selection. In [11] the channel capacity to handle bursty and continuous data from user nodes was investigated using a generic algorithm. In [12] the authors develop an algorithm that maximises the channel capacity and energy efficiency.

The work in [13] notes that the effective transmission rate in the user terminal is reduced in the block diagonalisation (BD) and block maximum SNR (BMSN) used to realise multi-user MIMO (MU-MIMO) broadcast transmission, when the total number of receive antennas is equal to the total number of transmit antennas. In [14] the work develops an AS based on sum capacity maximisation. In order to reduce device processing time however, the processing load is distributed among various neighbouring nodes thus enhancing its performance.

In [15] the state-of-the-art square maximum-volume (SMV) AS is compared with a proposed alternative the RMV matrices which is shown to solve the limitation of the SMV approach and achieve a suboptimal performance. In [16] a fast, environment aware AS is inspired by the reverse petri nets RPNs, which is capable of reverse processing, a property of Petri Nets. The AS proposed maximises the total achievable capacity for a distributed array.

Originally developed for streaming services and vehicular communications, the work in [17] considers the joint problem of multi-cast beamforming and AS for a single multi-cast MIMO system. The CSI is used to generate spot beam patterns capable of delivering high throughput to a common set of users. In [18] a method called antenna number modulation (ANM) is developed, where the number assigned to an antenna is used to alter the bits transmitted rather than commonly known spatial modulation (SM). With a single RF chain, bits to be transmitted are encoded for particular antennas using numbers. The number known as ANM bits specifies the transmitting antenna. Work shows that MIMO ANM AS has better performance than SM MIMO. A MIMO non-orthogonal multiple access (MIMO NOMA) over Nakagami channel is considered in [19] where a TAS is proposed to maximise received signal power and channel capacity. In [20] the proposed methods initially generate a reduced group of antennas before selecting the best candidate based on achievable capacity. The methods are named capacity-based reduced-complexity exhaustive search (CRCES) which generates the candidate subset by sorting the antennas based on channel capacity, as well as

the norm based RCES in which antennas are sorted based on descending norm value of each column of the channel matrix.

Energy-Aware Antenna Selection Techniques

In Energy Aware AS techniques, the AS search performed is subject to the constraint on power allocation or energy efficiency, usually jointly with other communication objectives such as the computational difficulty. Although AS is generally seen to reduce power consumption due to the use of far fewer RF chains than number of antennas, some AS algorithms work to specifically keep energy conservation at a certain level. In [21] the work shows that fully switching RF chains causes inherent insertion losses which result in poor power delivery to the output ports.

The proposed scheme in [22] increases energy efficiency using a suboptimal transmit AS with zero former (ZF) precoding. Although the work in [23] implemented its algorithm over a relay system, it is unique in its incorporation of renewable energy over a MIMO cognitive radio network (MIMO CRN). In MIMO simultaneous wireless information and power transfer (SWIPT) the work in [24] investigates spatial switching to attain pre-determined quality of service (QOS) based on the constraint of energy efficiency (EE) in the system.

A new solution for EE is developed in [25] to solve power allocation problems in point-to-point MIMO spatial multiplexing schemes. The authors in [26] proposed an algorithm to jointly minimise the mean square error (MSE) at the receiver and reduce the transmission power consumed by the antenna elements. In [27] a two-way link setup is analysed for a multi-antenna node with low complexity processing where power is transmitted in the forward link via SWIPT, while information is exchanged in downlink (DL) and uplink (UL). In [28] AS in the receiver node in Massive MIMO-NOMA is proposed for the reverse communication link such that the number of connected devices can be significantly increased. The work proposed one optimal AS and three sub-optimal algorithms to handle various objectives including power allocation. The work in [29] adopts a so-called "green" perspective which suggests that simultaneously activating several power consuming RF units of active antennas will significantly reduce power efficiency.

Jasus Antenna Selection

There are several works which propose methods that jointly combine antenna selection with user selection. It forms an interesting area of research in antenna selection, earning recognition as an important category in the classification of types of antenna selection with regards to chosen objectives. The author in [1] carried out some work on a MIMO-NOMA system, and proposed a limit to the number of antennas for AS. The proposed method in [30] uses low resolution ADCs at the base station. This type of ADCs is known to consume low power. The work obtains optimal BS Antenna selection. In [31] an AS scheme was proposed using semi-orthogonality measure. The work in [32] presents a JASUS algorithm for multiuser massive MIMO system.

Statistical AS

Statistical AS schemes are significantly experimental, and tests the properties of AS MIMO so as to determine the behaviour of the multi antenna system for AS. A distributed AS technique is studied in [33] for a DL MIMO, with decode and forward (DF). The network is analysed jointly with AS at both selected relay node as well as base station. The work in [34] analyses the Euclidean distance (EDAS) approach in AS schemes. EDAS is shown to have better performance than other current, existing methods compared with in the work. Information secrecy is investigated in the work in [35] where a simple linear pre-coding method is used in a transmit scheme. It is seen in the results that the information leakage intercepted at the eavesdropper is minimised when the base station has more active transmit antennas. In [36] authors study performance limits of massive MIMO systems by implementing various antenna selection algorithms. Author's work in [37] studies the extent to which AS can determine secrecy performance of a MIMO wire-tap channel.

A dual-hop cooperative MIMO system which has multiple antenna relays is studied for various quadrature amplitude modulation (QAM) methods in [38]. The work in [39] seeks to mitigate the problem of hardware cost and computational complexity by using a reconfigurable array.

Distributed AS Schemes

The distributed AS schemes refer to AS in which the receive or transmit node antennas are effectively distributed across more than one physical device, such that the extra-transmitting nodes or extra-receiving nodes function as relays and cooperate with each other to carry out reliable communication. The need for this cooperative transmission or reception is due to the inexistent direct communication path from transmitter to receiver, often occurring because communication path is blocked or fully degraded. The relays may be multi-antenna nodes which will serve to jointly transmit information to the target receiver over one or more hops. In [40] transmit AS (TAS) is developed to achieve particular QOS for a given user by remodelling the TAS problem as a Knapsack problem, KP. The work in [41] proposes a cooperative MIMO scheme which is implemented over several relay nodes. This MIMO relay scheme is combined with space shift keying (SSK).

Heuristic AS

In heuristic AS scheme, the algorithm acquires training data, usually derived from the feedback data which the user equipment (UE) sends via reverse channel to the base station or transmitter. Using the training data from the feedback, the heuristic algorithms can classify the data to represent various antenna performances, and it can simplify the AS process because the data helps algorithms take AS decisions based on previous events or data. This process of taking data samples and using them to determine or train algorithmic behaviour is a machine learning process. Transmit AS using Machine Learning is modelled in [42]. Two suboptimal antenna swapping algorithms are proposed in [43] in which the algorithms replace previously selected antennas in every iteration according to specified objectives such as SNR or power. In the work in [44] adaptive AS algorithm is proposed for the multi-antenna receiver with large array. Convolutional Neural Networks model is used in [45] to select suitable sub-arrays.

The work in [46] suggests that conventional TAS often introduce redundant calculations. The proposed algorithm will avoid this problem by employing pattern recognition methods, similar to machine learning approach for TAS. In [47] a Monte Carlo (MC) heuristic JASUS method developed for multiple cell and multiple user massive MIMO downlink systems is proposed. Another MC algorithm is explored in [48] where a cyclic and self-updating method called the Monte Carlo Tree Search is deployed for AS. In [49] a more computationally efficient estimation distribution algorithm (EDA) is proposed to respond to rapidly changing channel conditions.

ANALYSIS METHODOLOGY

Most of the current works in antenna selection evaluate the proposed systems over Rayleigh flat fading channels, in other words, Rayleigh channels which are not frequency

selective. For a majority of the algorithms proposed, the Monte Carlo simulations were used to analyse system performance, a minor collection of the works used Matlab or Mathematica programs.

OPEN AREAS IN ANTENNA SELECTION

In the area of heuristic algorithms, more work needs to be done to better validate the machine learning systems and develop online algorithms which can track channels with time-varying statistics. To minimise insertion losses due to matrix switching during AS [24], more research can be done in implementing of partly connected switching architectures. MIMO wire-tap continues to present a lot of opportunity for research because of the goal of improving security of transmitted messages in the physical layer [30]. Characterising large system MIMO wire-tap in the presence of eavesdroppers forms an interesting direction. The design of MIMO wire-tap system with mutli-eavesdropper and beamforming inspires research work in this field [15]. In the area of the JASUS algorithms, the application of the joint algorithms to wideband channels is an on-going research subject. In JASUS critical objectives to be considered are the system performance indices using imperfect CSI with user synchronization.

Energy aware algorithms can continue to improve. Research is expected to further expand the application and limits of the proposed algorithm in [7] to apply to more practical cases such as multiple user MIMO systems and joint antennas selection problems.

CONCLUSIONS

To the best of our knowledge no author has worked extensively on taxonomy review in antenna selection. Researches surveyed point to the need to increase diversity gain and mitigating the computational complexities. Better algorithms will reduce associated costs and utilise higher degrees of freedom for large MIMO to increase throughput and reduce latency, all requirements for 5G cellular.

The area of antenna selection remains vital in the achieving of increased capacity for 5G and 6G communication. Due to the instantaneously varying communication channels, spatial diversity offered by antenna selection will work to maintain reliable link quality. Methods continue to evolve in antenna selection, with focus on power, capacity and implementation complexity.

REFERENCES

[1] . Keerti Tiwari, Davinder S. Sani, Sunil V. Bhooshan. “ANTENNA Selection for MIMO systems over Weibull-Gamma” fading channel Perspectives in Science 8, 475 – 478 (2016)

[2] N. Hassan, and X. Fernando, “Massive MIMO Wireless Networks: An Overview”, Ryerson University, DOI 10.3390/electronics6030063, September 2017

[3] Mohammad Lari, “Wireless Network. Effective capacity of receive antenna selection MIMO–OSTBC systems in co-channel interference”. DOI 10.1007/s11276-016-1219-x

[4] Xiongfei Zhai, Yunlong Cai, Qingjiang Shi, Minjian Zhao, Geoffrey Ye Li, Fellow, IEEE, and Benoit Champagne. “ IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS ”, VOL. 35, NO. 9, SEPTEMBER 2017 2085 Joint Transceiver Design With Antenna Selection for Large-Scale MU-MIMO mmWave Systems

[5] Jie Tang, Daniel K. C. So, Arman Shojaeifard, Kai-Kit Wong, Fellow, IEEE, and Jinming Wen, “ IEEE Transactions on Wireless Communications Joint Antenna Selection and Spatial Switching for Energy Efficient MIMO SWIPT System ” DOI 10.1109/TWC.2017.2702575

[6] S. Gaur, and M. A. Ingram, “ Transmit/Receive Antenna Selection for MIMO Systems to Improve Error Performance of Linear Receivers ” Georgia Institute of Technology, Atlanta, March 2016

[7] YUZHEN HUANG1, FAWAZ S. AL-QAHTANI2, TRUNG Q. DUONG3, JINLONG WANG1, AND CHUNXIAO CAI, “ SPECIAL SECTION ON SECURITY IN WIRELESS COMMUNICATIONS AND NETWORKING ” Received June 25, 2016, accepted July 14, 2016, date of publication July 19, 2016, date of current version August 26, 2016. Digital Object Identifier 10.1109/ACCESS.2016.2593012 Secure Transmission in Spectrum Sharing MIMO Channels With Generalized Antenna Selection Over Nakagami-mChannels

[8] Hongjiang Lei, Chao Gao, Imran Shafique Ansari, Yongcai Guo, Yulong Zou, Gaofeng Pan, and Khalid A. Qaraqe, “ IEEE Transactions on Vehicular Technology Secrecy Outage Performance of Transmit Antenna Selection for MIMO Underlay Cognitive Radio Systems over Nakagami-m Channels ” DOI 10.1109/TVT.2016.2574315,

[9] HUA TANG , XIANZHENG ZONG, AND ZAIPING. “ Global-Searching-Based Iterative Swapping Antenna Selection for Massive MIMO Systems with Imperfect Channel Estimation ” NIE Received August30,2018, accepted October 26,2018,date of publication November9,2018,date of current version November30,2018. Digital Object Identifier 10.1109/ACCESS.2018.2878732. Pp 66757-66564

[10] Zaid Abdullah, Charalampos C. Tsimenidis and Martin Johnston, “ 24th European Signal Processing Conference (EUSIPCO) Tabu Search vs. Bio-inspired Algorithms for Antenna Selection in Spatially Correlated Massive MIMO Uplink Channels ”, 2016.

[11] Bin Wang, Yongyu Chang and Yang Sun, “ IEEE Transactions on Antennas and Propagation Performance of the Large-scale Adaptive Array Antennas in the Presence of Mutual Coupling ”, DOI 10.1109/TAP.2016.2550053.

[12] Jingon Joung, “Machine Learning-based Antenna Selection in Wireless Communications” DOI 10.1109/LCOMM.2016.2594776 IEEE COMMUNICATIONS LETTERS, VOL. 0, NO. 0, MONTH 2016 1

[13] Maryam Olyaee1, Mohsen Eslami1 , Javad Haghighat1 “ An energy-efficient joint antenna and user selection algorithm for multi-user massive MIMO downlink ”. IET Communications Research Article doi: 10.1049/iet-com.2017.0905 www.ietdl.org IET Commun., 2018, Vol. 12 Iss. 3, pp. 255-260 © The Institution of Engineering and Technology 2017

[14] Hongjiang Lei, Ming Xu, Imran Shafique Ansari, Gaofeng Pan, Khalid A. Qaraqe, Senior and Mohamed-Slim Alouini, “IEEE Transactions on Green Communications and Networking. On Secure Underlay MIMO Cognitive Radio Networks with Energy Harvesting and Transmit Antenna Selection ”DOI 10.1109/TGCN.2017.2684827

[15] Feng Shu, Zhengwang Wang, Riqing Chen, Yongpeng Wu, and Jiangzhou Wang, “ IEEE Transactions on Vehicular Technology Two High-performance Schemes of Transmit Antenna Selection for Secure Spatial Modulation ” DOI 10.1109/TVT.2018.2844401,

[16] Hua Tang*, Zaiping Nie “ IEEE Signal Processing Letters RMV Antenna Selection Algorithm for Massive MIMO ” DOI 10.1109/LSP.2017.2783350

[17] Saba Asaad, Ali Bereyhi, Amir M. Rabiei, Ralf R. Müller, Rafael F. Schaefer “ Optimal Transmit Antenna Selection for Massive MIMO Wiretap Channels ” 2018

[18] Ahmet M. Elbir1 and Kumar Vijay Mishra “ Deep Learning Design for Joint Antenna Selection and Hybrid Beamforming in Massive MIMO ” 2. 978-1-7281-0692-2/19/$31.00 ©2019 IEEE pp 1585 – 1586

[19] Gang Chuai, Weidong Gao, Kaisa Zhang, Xuewen Liu and Zhiwei Si, Saidiwaerdi Maimaiti et al. “ EURASIP Journal on Wireless Communications and Networking “ “ A low-complexity algorithm for the joint antenna selection and user scheduling in multi-cell multi-user downlink massive MIMO systems ” (2019) 2019:208 https://doi.org/10.1186/s13638-019-1529-7

[20] Mahdi Eskandari, Ali Mohamad Doost Hoseini, Mohammad Sadegh Fazel, “ An energy-efficient joint antenna selection and power allocation for MIMO Systems under limited feedback.” Signal Processing journal homepage, Signal Processing 163 (2019) 66–74

[21] Hui Zhao, Youyu Tan, Gaofeng Pan, Yunfei Chen, and Nan Yang, IEEE Transactions on “ Vehicular Technology Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks ” DOI 10.1109/TVT.2016.2529704

[22] Mukti Verma1, Sachin Dogra2, Atul Mishra3, “ A New Rapid Broadcast Antenna Selection Algorithm for MIMO System ”International Journal Of Scientific & Engineering Research, Volume 7, Issue 7, July-2016 1054 ISSN 2229-5518 IJSER © 2016 http://www.ijser.org

[23] Yuan Gao, Han Vinck, and Thomas Kaiser, IEEE Transactions on “ Signal Processing Massive MIMO Antenna Selection: Switching Architectures, Capacity Bounds and Optimal Antenna Selection Algorithms “ DOI 10.1109/TSP.2017.2786220.

[24] Zhaojie Sun, Yue Xiao, Ping Yang, Shaoqian Li, and Wei Xiang, “ IEEE Transactions on Vehicular Technology IEEE 1 Transmit Antenna Selection Schemes for Spatial Modulation Systems: Search Complexity Reduction and Large-scale MIMO Applications ” DOI 10.1109/TVT.2017.2696381

[25] Yangyang Zhang, Jianhua Ge, " Joint Antenna-and-Relay Selection in MIMO Decode-and-Forward (DF) Relaying Networks Over Nakagami-m fading channels " IEEE Signal Processing Letters DOI 10.1109/LSP.2017.2671401

[26] Ferhat Yarkin, , Ibrahim Altunbas, Ertugrul Basar, "IEEE Communications Letters 1 Source Transmit Antenna Selection for Space Shift Keying with Cooperative Relays" DOI 10.1109/LCOMM.2017.2659119

[27] Yuehua Yu, He Chen, Yonghui Li, Zhiguo Ding, and Li Zhuo, " Antenna Selection in MIMO Cognitive Radio-Inspired NOMA Systems " 2658 IEEE COMMUNICATIONS LETTERS, VOL. 21, NO. 12, DECEMBER 2017

[28] Saba Asaad, Amir Masoud Rabiei, Ralf R. Müller, " IEEE Transactions on Wireless Communications Massive MIMO with Antenna Selection: Fundamental Limits and Applications " DOI 10.1109/TWC.2018.2877992

[29] Ping Yang, Jing Zhu, Yue Xiao, Zhi Chen, " Antenna selection for MIMO system based on pattern recognition "DIGITAL COMM and Networks 5 (2019) 34 – 39.DOI: doi.org/10.1016/j.dcan.2018.10.001

[30] Daniel G. Wilson-Nunn, Anas Chaaban, Aydin Sezgin, and Mohamed-Slim Alouini, " Antenna Selection for Full-Duplex MIMO Two-Way Communication Systems " IEEE Communications Letters 1. DOI 10.1109/LCOMM.2017.2681066

[31] Behrooz Makki, Anatole Ide, Tommy Svensson, Thomas Eriksson, Mohamed-Slim Alouini "A Genetic Algorithm-based Antenna Selection Approach for Large-but-Finite MIMO Networks". IEEE Transactions on Vehicular Technology, Citation for the published paper: Makki, B. ; IDE, A. ; Svensson, T. et al. (2017)

[32] Pierluigi V. Amadori, and Christos Masouros, " IEEE Transactions on Communications Large Scale Antenna Selection and Precoding for Interference Exploitation", DOI 10.1109/TCOMM.2017.2720733

[33] Shiwen He, Yongming Huang, Jiaheng Wang, Luxi Yang, and Wei Hong,"Joint Antenna Selection and Energy-Efficient Beamforming Design " IEEE Signal Processing Letters 1, DOI 10.1109/LSP.2016.2588731

[34] Adrian Garcia-Rodriguez, Christos Masouros, and Pawel Rulikowsk,, " IEEE Transactions on Communications 1 Reduced Switching Connectivity for Large Scale Antenna Selection " DOI 10.1109/TCOMM.2017.2669030.

[35] Ryan Husbands, Qasim Ahmed, and Junyuan Wang I , " Wireless Communications Symposium. Transmit Antenna Selection for Massive MIMO: A Knapsack Problem Formulation ". IEEE ICC 2017

[36] Aritra Konar, and Nicholas D. Sidiropoulos, " A Simple and Effective Approach for Transmit Antenna Selection in Multi-user Massive MIMO Leveraging Submodularity ", IEEE Transactions on Signal Processing 1, DOI 10.1109/TSP.2018.2863654

[37] Nobuyoshi KIKUMA†a),Fellow, Kentaro NISHIMORI††,and Takefumi HIRAGURI , Special Section on " Communication Quality in Wireless Networks Effect of User Antenna Selection on Block Beam forming Algorithms for Suppressing Inter-User Interference in Multiuser MIMO System " IEICETRANS.COMMUN.,VOL.E101–B,NO.7JULY2018 1523 INVITED PAPER

[38] Rui Zhao, Hongxin Lin, Yu-Cheng He, Dong-Hua Chen, Yongming Huang, and Luxi Yang, " Secrecy Performance of Transmit Antenna Selection for MIMO Relay Systems With Outdated CSI ", 546 IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 66, NO. 2, FEBRUARY 2018

[39] Chongjun Ouyang, and Hongwen Yang , "Massive MIMO Antenna Selection: Asymptotic Upper Capacity Bound and Partial CSI ". 2018

[40] Jinjin Men, Jianhua Ge, Chensi Zhang, " A Joint Relay-and-Antenna Selection Scheme in Energy Harvesting MIMO Relay Networks ", IEEE Signal Processing Letters, DOI 10.1109/LSP.2016.2538290

[41] Shiwen He, Yongming Huang, Jiaheng Wang, Luxi Yang, Wei Hong, " Joint Antenna Selection and Energy-Efficient Beam forming Design",IEEE Signal Processing Letters 1.DOI 10.1109/LSP.2016.2588731

[42] Hao Li, Julian Cheng, Zhigang Wang, Houjun Wang, " Joint Antenna Selection and Power Allocation for an Energy-efficient Massive MIMO System " IEEE Wireless Communications Letters. DOI 10.1109/LWC.2018.2869152,

[43] Mahdi Eskandari, Ali Mohamad Doost-Hoseini, Jaehoon Jung, and Inkyu Lee " Antenna Selection and Power Allocation for Energy Efficient MIMO Systems " 546 JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 20, NO. 6, DECEMBER 2018.

[44] Jung-Chieh Chen, " Joint Antenna Selection and User Scheduling for Massive Multiuser MIMO Systems With Low-Resolution ADCs. " IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY 1DOI 10.1109/TVT.2018.2884228

[45] Marcele O. K. Mendonc¸a, Paulo S. R. Diniz, Tadeu N. Ferreira, and Lisandro Lovisolo, " Antenna Selection in Massive MIMO Based on Greedy Algorithms ". IEEE Transactions on Wireless Communications JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, OCTOBER 2018 1. DOI 10.1109/TWC.2019.2959317

[46] Xiongfei Zhai, Qingjiang Shi, Yunlong Cai, and Minjian Zhao "IEEE Transactions on Communications Joint Transmit Precoding and Receive Antenna Selection for Uplink Multiuser Massive MIMO Systems " DOI 10.1109/TCOMM.2018.2854175.

[47] ISSN 0735-2727, Radioelectronics and Communications Systems, 2018, Vol. 61, No. 12, pp. 547–555. © Allerton Press, Inc., 2018. Original Russian Text © T.A. Sheikh, J. Bora, M.A. Hussain, 2018, published in Izvestiya Vysshikh Uchebnykh Zavedenii, Radioelektronika, 2018, Vol. 61, No. 12, pp. 688–698. Tasher Ali Sheikh*, Joyatri Bora**, and Md. Anwar Hussain " Sum-Rate Performance of Massive MIMO Systems in Highly Scattering Channel with Semi-Orthogonal and Random User Selection1 "

[48] Dongxuan He, Chenxi Liu,, Tony Q. S. Quek, and Hua Wang, " IEEE Wireless Communications Letters Transmit Antenna Selection in MIMO Wiretap Channels: A Machine Learning Approach " DOI 10.1109/LWC.2018.2805902

[49] Ahmet M. Elbir and Kumar Vijay Mishra, " IEEE Transactions on Wireless Communications 1 Joint Antenna Selection and Hybrid Beamformer Design using Unquantized and Quantized Deep Learning Networks " DOI 10.1109/TWC.2019.2956146

Determining Mice Sex from Chest X-rays using Deep Learning

Abiodun Ajiboye
Institute of Computer Vision and Machine Learning
Lagos
Nigeria
abiodun@cvml.org.ng

Kola Babalola
European Molecular Biology Laboratory
European Bioinformatics Institute
Wellcome Trust Genome Campus, Cambridgshire, UK
kola@ebi.ac.uk

***Abstract*—Following on from work by Babalola *et al.* [1] we show that the sex of mice can be determined from x-ray images of the chest region alone using convolutional neural networks. We further investigate the anatomical differences that may be responsible for this, as it may be useful in determining phenotype changes caused by knocking out genes - hence in understanding genotype-phenotype effects. Our results indicate that the cervical vertebrae may play an important role in the ability of our convolutional neural network to classify the sex of mice correctly using only x-rays of the chest region.**

***Index Terms*—CNN, classification, genotype, phenotype, knockout**

I. Introduction

In genetics understanding the relationship of genotype (the genetic makeup of an organism) to phenotype (the observed attributes) plays an important role in the understanding and treatment of diseases. The use of animal models in research into the eitology and treatment of disease is fundamental. About 85% of the protein coding genes in mice are identical to those of humans. Hence, it is not surprising that mouse models play a prominent role in medical research. Several groups are using mouse models to investigate the genetic underpinnings of important diseases.

The International Mouse Phenotyping Consortium (IMPC) [2] is one such group whose ultimate goal is to phenotype all protein coding genes in the mouse. This involves creating mutants in which a single gene is removed (knockouts) and investigating phenotype changes in these when compared with mice having a complete set of genes (wildtypes). The process of 'phenotyping' knockouts involves assessing up to 250 biological parameters relevant to human health and disease. An important procedure involves obtaining x-ray images of each mouse. Quantitative and qualitative features indicating abnormalities in bone structures are recorded by expert annotation to give over 50 parameters.

Revolutionary progress in machine learning (ML) and genetics coupled with advances in imaging technology are providing unprecedented opportunities in many fields including medical research. A particular branch of machine learning (Deep Learning) has gained prominence in the last few years due to improved computing power and greater availability of data. Deep learning is a rapidly evolving field and use of the latest techniques can deliver significant efficiency gains and produce new insights. We are particularly interested in using Convolutional Neural Networks (CNNs) on image data produced by the IMPC.

This work uses data made available by the International Mouse Phenotyping Consortium (IMPC) through the European Bioinformatics Institute, Cambridgeshire, UK

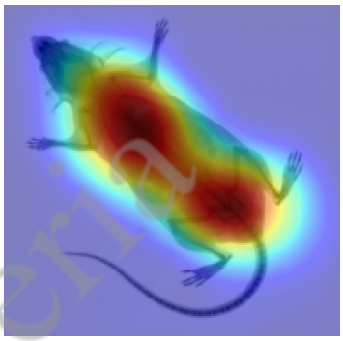


Fig. 1. Results of occlusion sensitivity from [1], showing that the regions most important in distinguishing the sex are around the pelvis and the chest.

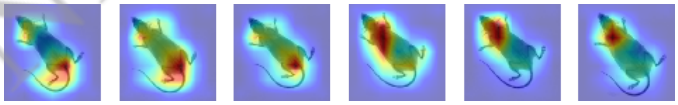


Fig. 2. From [1] - class activation maps of 3 randomly chosen wildtype females (1st three) & males (last 3) again showing the chest and the pelvic regions are important in distinguishing sex

Babalola *et al.* [1] demonstrated that convolutional neural networks (CNNs) trained on whole body dorso-ventral images of mice could be used to determine their sex. They investigated the regions of the image important for classification accuracy and determined the chest and the groin area as hotspots. The fact that the groin area is important is understandable due to the presence of the sexual organs. However, the importance of the chest region was not well understood.

Here we follow-up on their study and exclusively look at the chest region with the following aims:

1) Can the chest region alone be used to classify the sex of mice?
2) If the chest region can be used to classify sex of mice can

we determine or understand the anatomical feature(s) the model is focusing on?

II. Method

We broadly follow the approach taken by [1]. We use the same training set and network architecture that they do and we investigate the model characteristics using occlusion sensitivity [3] and their variation of the class activation maps of [4]. However, we diverge from their approach by aligning each image in the vertical direction by finding the principal moment of the binary image of the mouse foreground. We crop the aligned image in the region around the chest. This region of interest is used to train our model using a transfer learning approach based on the VGG-16 model.

A. The CNN model

We used the same dataset as [1] of 3,014 X-ray images of mice (1502 male, 1512 female) - except that we re-aligned the images and cropped the chest region as detailed above. The images were randomly split in a 60:20:20 ratio for training, validation and testing respectively. The thirteen convolutional layers of the VGG-16 model [5] pretrained on 1.4 million images from the ImageNet dataset formed the base of our model. We applied transfer learning [6] by freezing these layers and the three fully connected layers were trained using our data. The number of outputs of the final fully connected layer was changed to 2 (from 1000) for the male and female classes.

There are a number of frameworks that could have been used to build the models e.g. TensorFlow [7] or Keras [8]. We opted to use the PyTorch framework [9] thereby following the choice of [1]. The images used to build the VGG-16 model were of size 224x224 and had 3 channels (red, green and blue). Our images are single channel gray scale images of varying size. We cropped a square region around the chest area and rescaled this to 224x224 pixels. To get three channels we simply copied the image twice to give a 224x224x3 image. The intensity of each image was normalised using the mean and standard deviation from the training set of VGG-16 and dividing the by standard deviation of this training set. The parameters of the fully connected layers of the model were obtained using stochastic gradient descent and cross-entropy loss.

B. Understanding what the CNN is looking at

To visualise the features important in the network making its decision we used class activation mapping and sensitivity to occlusion. Sensitivity to occlusion was carried out on 100 images of male and female mice that had been processed without errors by the model. A 30 pixel square mask of 0 values was scanned across each image. The scan started at the origin and at each step the mask was moved one pixel to the right until it touched the right edge of the image, at which point it was shifted one pixel down and to the left edge of the image. In this way the mask was overlaid on the image from left to right and top to bottom. Each occluded version of the image was processed by the model and the outcome stored for each location of the mask. The mean of the occlusion results over all the 100 images was taken to produce a heat map highlighting areas whose occlusion resulted in incorrect classifications.

Although occlusion sensitivity is a straightforward method of investigating parts of an image that are salient in the performance of a model, it has two drawbacks. Firstly, the scanning takes time and secondly, for best results it needs to be applied to a representative set of images. Class activation maps do not suffer from these drawbacks. They work on individual images to highlight features whose activations are important when applying the model to a single image. The class activation mapping method proposed by [4] uses the global average pooling layer. However, we use the variation proposed by [1] which maps activations from the output of the final fully connected layer to the final convolution layer. Each of the $7 \times 7 \times 512$ features in this layer is individually weighted and global average pooling in the third dimension is applied to give a 7×7 image that is resampled to the dimensions of the input image. The superpostion of this on the input image gives the CAM.

TABLE I
Confusion matrix for model performance over the test set

	actual male	actual female
predicted male	289 (TP)	11 (FP)
predicted female	5 (FN)	299 (TN)

III. Results

To assess the performance of the model standard metrics of Accuracy ($\frac{TP+TN}{TP+FN+TN+FP}$), Precision ($\frac{TP}{TP+FP}$) and Recall ($\frac{TP}{TP+FN}$) were computed over the test set. The accuracy of classifying males and females was 97% and the precision and recall males were 0.96 and 0.98 respectively. For the female class they were 0.98 and 0.96 respectively. The confusion matrix associated with the results is shown in Table I

The result of performing occlusion sensitivity is displayed in Figure 3. This shows that the performance of the model decreased when regions around the forearm, neck and some local parts of the chest area were occluded.

The average class activation maps of all the males are shown in Figure 4 and those for the females in Figure 5. These look different for the different classes and show hotspots in localised regions. Of particular interest is the region around the neck that is highly weighted for the female class and less so for the male class. This region is consistent with the results obtained by [1].

IV. Discussion and conclusions

The results presented above show that the model with only the chest region performed well in classifying sex. The results are similar to those of [1] (97% here compared with their 98%), which is remarkable as the region around the pelvis housing the sexual organs was excluded in our case. However,

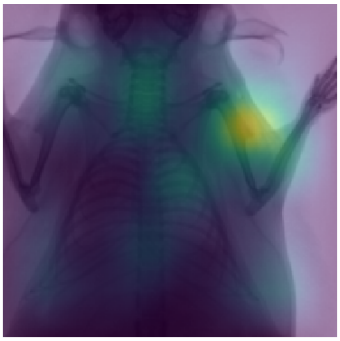


Fig. 3. Results of investigating model performance with occlusion sensitivity for the chest area, showing that the regions that may be important in distinguishing the sex around the neck, the forearm and some localised parts of the chest.

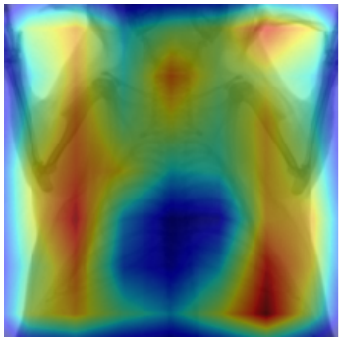


Fig. 4. The average class activation map over the 1502 male mice. This shows hotspots around the ribs and to a lesser degree in the neck region.

the investigations with the occlusion sensitivity were not as definitive as in [1]. On the other hand the class activation maps showed that the neck regions identified as important in [1] featured in this case especially in the female mice. Our study further localised this region to the vertebrae in the neck. This result helps to point towards the vertebrae in the neck as a possible candidate for sexual dimorphism (the presentation of different non-sexual organ characteristics by two sexes of the same species) and a potential phenotype marker.

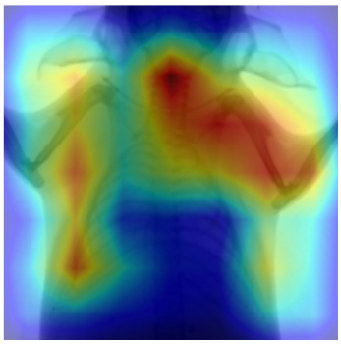


Fig. 5. The average class activation map over the 1512 female mice. This shows hotspots mainly around the neck region.

Acknowledgment

Kola Babalola is a member of the International Mouse Phenotyping Consortium supported by the United States National Institutes of Health (NIH) Grant U54 HG006370.

References

[1] K. Babalola, H. H. Mashhadi, V. Muñoz-Fuentes, J. Mason, and T. Meehan, "Investigating sex related phenotype changes in knockout mice by applying deep learning to x-ray images," in *Medical Image Understanding and Analysis*, 2020, pp. 359–369.

[2] M. Dickinson, A. Flenniken, X. Ji, and et al., "High-throughput discovery of novel developmental phenotypes," *Nature*, vol. 537, p. 508–514, 2016.

[3] M. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," *ECCV*, 2014.

[4] B. Zhou, A. Khosla, L. A., A. Oliva, and A. Torralba, "Learning deep features for discriminative localization," *CVPR*, 2016.

[5] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*, 2015. [Online]. Available: http://arxiv.org/abs/1409.1556

[6] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" in *Advances in Neural Information Processing Systems 27*, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, Eds., 2014, pp. 3320–3328. [Online]. Available: http://papers.nips.cc/paper/5347-how-transferable-are-features-in-deep-neural-networks.pdf

[7] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, M. Kudlur, J. Levenberg, R. Monga, S. Moore, D. G. Murray, B. Steiner, P. Tucker, V. Vasudevan, P. Warden, M. Wicke, Y. Yu, and X. Zheng, "Tensorflow: A system for large-scale machine learning," in *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, 2016, pp. 265–283. [Online]. Available: https://www.usenix.org/system/files/conference/osdi16/osdi16-abadi.pdf

[8] F. Chollet *et al.*, "Keras," https://github.com/fchollet/keras, 2015.

[9] A. Paszke, S. Gross, and et al., "Pytorch: An imperative style, high-performance deep learning library," in *Advances in Neural Information Processing Systems 32*, H. Wallach, H. Larochelle, A. Beygelzimer, F. d' Alche-Buc, E. Fox, and R. Garnett, Eds. Curran Associates, Inc., 2019, pp. 8024–8035. [Online]. Available: http://papers.neurips.cc/paper/9015-pytorch-an-imperative-style-high-performance-deep-learning-library.pdf

Detecting Advance Fee Fraud using NLP Bag of word Model

Muhammad Hamisu
School of Computer Science and Technology
University of Bedfordshire
Luton, Bedfordshire
muhammad.hamisu@study.beds.ac.uk
muhammadsharifai@gmail.com

Dr Ali Mansour
School of Computer Science and Technology
University of Bedfordshire
Luton, Bedfordshire
ali.mansour@beds.ac.uk

Abstract— **Advance fee fraud, a form of Internet fraud is among Cybercrime that causes financial loss to the global economy and has been linked to Internet fraud that are originating from Nigeria. This paper present a fraudulent email classifier that detect and classify email as either fraudulent or non fraudulent using the Natural language process model of Bag of Words. The classifier is design and trained to detect and classify advance fee fraud that originate from Nigeria, as the data set used for the training and testing of the classifier originate from there. The classifier was trained using various machine learning algorithms using the Bag of words generated as predictors. Choosing the best algorithms the classifier was tested and performed successfully.**

Keywords— Advance fee fraud, Bag of Words, Internet Fraud, Machine Learning, Nigeria.

I. INTRODUCTION

Internet fraud is negatively affecting the lives of people both financially and psychologically due to the losses victims of such crime are facing. Victims of Internet fraud ended up not only suffering from financial loss but getting in a state of confusion, frustration, and sometimes depression [1], [2], [3]. The United States Federal Bureau of Investigation (FBI), define Internet fraud as the use of Internet service or software with Internet access to defraud victims or to otherwise take advantage of them [4]. Various means or methods have been used by fraudsters to defraud their victims over the Internet, some of the most frequently reported Internet fraud include; Business email compromise (BEC), Email account compromise (EAC), Credit card fraud, Phishing, Romance fraud, Identity theft, Internet auction fraud, 419 fraud, Government impersonation, Advance fee fraud, Non delivery of merchandise, Ransomware, Scareware, Malware, Spoofing, Pharming, etc. [5], [6], [7].
Internet fraud is one among the many cybercrimes committed, but it is among the few that cause huge economic impact to the society as reported that in one year alone, cybercrime had cost the global economy more than $450 Billion [8].

Even as the world battles with the covid-19 pandemic, a report published by Interpol showed a global rise in Internet fraud especially during the period of lockdown as the digital economy and online business grows rapidly such was also the case with cybercrime [9]. Internet fraud has risen to a record high with increased calls for the need to find new ways and research to protect customers from falling into fraudsters [10].
Internet fraud is the most prevalent crime in England and Wales according to a House of Commons Committee report [11]. Statistics from Office for National Statistics in Great Britain showed that Internet fraud is on the rise and is among the most reported cybercrime in the UK [12].
An Australian Government report indicates that Internet Fraud is the highest Cybercrime committed with 53%, 53% and 52% of the total cybercrime in the country in year 2016, 2017 and 2018 respectively. While email is identified as the leading form of communication between fraudsters and victims in Australia [13].
Australians lost almost half a billion dollar to Internet Fraud in 2018 alone. A total of $489million was lost, up by $149million in 2017, this shows the alarming rate with which Internet fraud is growing and pointed to the urgent need to mitigate it [14]. Those figures do not truly reflect the actual cost of scam in Australia as not everyone that becomes victim of Fraud reports it to the police.
In the US, The FBI Internet Crime Complaint Centre (IC3) report showed that in the year 2019 alone over $100 million was lost to Advance fee fraud in the US [15].

Sometime cybercrime are linked or blamed to specific countries either as state sponsored or the origin where the crime take place. Nigeria suffers from reputation damage as some form of Internet fraud are been linked to the country. A number of Cybersecurity Intelligence report showed that large number of Nigerian gangs are involved in Internet fraud, as it was observed in a research that majority of a scam emails IP address come from Nigeria [16].

The Australian Competition and Consumer Commission categorically list Nigerian scam as part of a known fraud in the country, and according to statistics in two months only the sum of $46,544 was lost to that scam [17]. Another form of Internet Fraud is called 419, which is synonymous to Advance Fee Fraud. The name 419 is a reference to the section of the Nigerian Constitution that deals with the crime and is been internationally recognised as a form of fraud that originates from Nigeria [17].

The arrest and prosecution of Nigerians for various Internet fraud offence has also add to the reason why Nigeria is sometimes associated to issue of Internet fraud, especially with some popular arrest that makes global headline like that of Hushpuppi and others [18].

In this paper, we present a method for the detection and classification of Advance fee fraud, originating from Nigeria, by applying the Bag of words technique to identify some of the common words that are used by fraudsters in communicating with their victims. Fraudulent emails dataset were analysed, which were collected from Nigeria's law enforcement agency, the Economic and Financial Crimes Commission (EFCC), and the Kaggle website [19].

This paper is organised as follows: Section 2 Discusses Advance fee fraud, Section 3 discusses Natural language processing and the Bag of word model, Section 4 presents the related work, while the research method and the results are presented in section 5, and lastly section 6 concludes the paper.

II. ADVANCE FEE FRAUD

Advance fee fraud happens when a victim is promised a huge sum of money that will be made as a result of either a legal or illegal activities like transferring money of a late African dictator, or claiming that inheritance will has been left in the victim's name by an unknown relative, or some kind of lucrative business, etc. but with the demand of some advance payment to facilitate the transaction or activity. Advance fee fraud victims are mainly contacted via email which is sent to target mainly English-speaking people who have names common to that country [20], [21], [22].

Table shows the figures of losses as a result of Advance Fee Fraud from Australia, UK, and US.

The following table 1 shows the figure of losses as a result Advance Fee Fraud from Australia, UK, and US.

TABLE I. ADVANCE FEE FRAUD LOSSES FROM AUSTRALIA, UK, AND US [14, 23-27]

Country	Fraud Type	Amount lost	Reports	Year
Australia	Nigerian (Advance Fee)	$1,404,108	1,498	2016
Australia	Nigerian (Advance Fee)	$1,665,373	1,287	2017
Australia	Nigerian (Advance Fee)	$1,379,285	878	2018
Australia	Nigerian (Advance Fee)	$ 1,066,838	661	2019
Australia	Nigerian (Advance Fee)	$ 203,190	428	2020 (Nov)
UK	Advance Fee	$14,000,000	8,133	2018
US	Advance Fee	$60,484,573	15,075	2016
US	Advance Fee	$57,861,324	16,368	2017
US	Advance Fee	$ 92,271,682	16,362	2018
US	Advance Fee	$ 100,602,297	14607	2019

III. NATURAL LANGUAGE PROCESSING

Natural language processing is a branch of Artificial intelligence that deals with the relationship and interaction between computer and human natural languages. It works on how computers can understand and effectively respond to humans using human spoken languages [28]. Natural language deals with huge amounts of data especially with the emergence of new and sophisticated technology that lead to the emergence of "Big Data" such as in the case of analysis, translation and conversion. Corpus is the body of large text (Plural is Corpora). The need for natural language processes stem out of the need for computers to learn a human language to effectively communicate with humans and to also be able to acquire information from written documents [28]. The natural language processes for information seeking are divided into three:

- Text classification
- Information retrieval, and
- Information extraction

Language models are models that predict the probability distribution of language expressions [28].

Language is defined by formal programming languages (like java and python) as a set of strings; specified by a set of roles called grammar. In the English language a written text is composed of characters – letters, digits, punctuation, and space [28].

Bag of words Model

The Bag of words model consists of unique words that have been used in communication which are either written or verbal. To generate the Bag of words, the following steps are followed: Tokenization, Stop word removal, Lemmatization, and Stemming [29].

IV. RELATED RESEARCH WORK

Some researchers sought to find a solution for Advance fee fraud and other forms of Internet fraud. In this section we present some of the relevant research work that have been published relating to Advance fee fraud.

Research by [30] proposed the detection of Advance fee fraud by analysing cluster features in the fraudulent message. The researchers used Global CM algorithms to detect the fraud from Internet. The result presented Lib SVM 97.5% and Random Forest algorithms 96.82 using 1080 dataset for the research which were collected online from websites potifos and svbislaws from the year 2000 to 2005 [30].

[31] Present an Advance Fee fraud detection system using Ontology engineering. The research proposed the design and development of fraud detection system based on Application Knowledge Engineering Methodology (AKEM). It specify four steps in tracks for the successfully development of a fraud detection system as follows; System engineering, Terminology Engineering track, Knowledge Engineering, and Language Engineering. The system was developed using Java.

Pellon and Anesa present an analysis of Advance fee fraud emails and suggested the use of Linguistic approach in detecting such fraud. The research present the list of 20 words that according to co-occurrence from analysis of 507 emails dataset using AntConc a freeware text analysis tool kit [32].

[33] proposed a Linguistic analysis detection technique (Particularly pronoun use) for the detection of Advance fee fraud. The research use Diction, a computer assisted text analysis software to detect fraud. Using 30 fraudulent emails data set, an accuracy result of 80% was achieved [33].

[34] Presented a research that analyse Scam bait communication and develop a classifier. The classifier identify Advance fee fraud based on textual content using features extracted from the scam baiting communication that was analysed. The research use Logic Regression, Naïve Bayes and Support vector machine algorithms achieving the best accuracy result of 96.3% from Support Vector machine.

3248 data set were used in the research collected from Enron Data set and 419eaters.

A work published by Yangbin and Zhao looked at "Fortune from the Dead (FFD)" a type of Advance fee fraud. The researchers proposed the use of ontology base information extraction method to recognize fraud evidence from texts samples of Nigerian fraud emails using RegEx, a free and open source machine learning software programmed in Java. The result of the research showed 94% and 91% precision and recall count was achieved and 92% and 80% precision and recall count were achieved from Over invoicing fraud. The researchers used a small number of emails in their research (only 50 emails corpus dataset was used in the research). A 50 emails dataset is too small for the validation of the research. Also, the research only looked into one type of Advance fee fraud, the Fortune from the dead [35].

Another research conducted by [36] proposed the detection of fraudulent emails using Waikato Environment for knowledge analysis (WEKA) data mining software and employ TF-IDF for feature extraction. The research used Nigerian emails as part of their dataset.

V. RESEARCH WORK AND RESULT

In the research 4500 fraudulent emails were collected as dataset and used in the research. The dataset is been divided into Training set (2000) and Testing set (2500). The dataset (which is in CVS format) is input to MATLAB. Predictors features used are the Bag of Words generated using text mining. Text mining is used to get quantitative statistics on large sets of text which can be structured or unstructured. Text mining is used in many areas of ICT some of which application includes;

- Word frequency count, phrases in documents and performing data analysis.
- Classification of text based on content automatically.

Using MATLAB, the following are the bag of words generated according to word frequency count as shown in table ii.

TABLE II. SHOWING BAG OF WORDS GENERATED

S/N	Word	Count
1	Money	7952
2	Account	7004
3	Bank	5455
4	Fund	5306
5	Transaction	4640
6	Transfer	4003
7	Foreign	3949
8	Assist	3913
9	Company	3686
10	Contact	3684
11	Country	3385
12	Secure	3157
13	Email	3043
14	Million	3009
15	Please	2847
16	Invest	2640
17	Deposit	2602
18	Dollar	2569
19	Government	2514
20	Confidential	2404
21	Next	2318
22	Kin	2164
23	Online	2146
24	Contract	2043
25	Claim	2024
26	State	2017
27	Information	1947
28	Nigeria	1822
29	Fax	1774
30	Late	1714
31	Document	1680
32	Interest	1664
33	Immediately	1621
34	Need	1599
35	Share	1547
36	Africa	1535
37	Urgent	1525
38	Propose	1480
39	Amount	1449
40	Private	1401
41	Partner	1368

Using the Bag of Words generated as Predictors, six machine learning algorithms were used for the classification and the following result was achieved as presented in table iii. For the development of the Classifier, the response is set as Binary classification while the validation holdout was at 25%.

TABLE III. THE RESULTS AND PERFORMANCE OF ALL MACHINE LEARNING ALGORITHMS USED

Algorithm	Result	Prediction speed
Decision Tree	100%	**7100**
Discriminant Analysis	100%	5900
Logic Regression	100%	3600
Support Vector Machine	**88.48%**	**6566.66**
Nearest Neighbour	**69.22%**	**4333.33**
Ensemble	98.46%	578

As shown in table 3, during the experiment the best result achieved is from Decision tree with the overall performance of 100% and also has the highest overall prediction speed of 7100 observations per second.

Discriminant has the second best performance with an overall accuracy result of 100% at a prediction speed of 5900. Logic regression also produce high accuracy result with the overall result at 100% and a prediction speed of 3600 observations per second. Ensemble produce an overall result of 98.46% and an

overall prediction speed of 578 prediction per second. The overall result achieved with Support vector machine is 88.48% which is among the lowest accuracy result achieved in the research work. The overall prediction speed is 6566 observations per second. K nearest neighbour produce the lowest result in the research with an overall accuracy result of 69.22% and a prediction speed of 4333.33 observations per second.

VI. CONCLUSIONS

In this paper, we present a fraudulent email classifier using the Bag of Word model. Fraud emails were identified and successfully classified as Fraud with accuracy of 100%. The Bag of words features that were generated and used as Predictors proved successful with regards to Advance Fee fraud detection and classification. Hence, this research has successfully accomplished and achieve the state aim of successful Detection and Classification of Advance fee fraud email that originate from Nigeria through the application of Artificial Intelligence technique. The Classifier produced the best result with Decision Tree algorithms achieving 100% accuracy and 7100 observations per second prediction speed. This result achieved is the best ever achieved in trying to classify Advance fee fraud originating from Nigeria according to the best knowledge and investigation of the researchers. No any other research work has ever attempt to successfully detect and classify Fraudulent emails that are specifically coming from one particular destination or country (in this case Nigeria).

ACKNOWLEDGMENT

The authors wish to acknowledge the EFCC for providing part of the data set used in the research.

REFERENCES

[1] BBC News, "New Jersey man posed as soldier in dating site scam - Prosecutors", BBC News, January, 2019, [Online] Available at: https://www.bbc.co.uk/news/world-us-canada-49574448 [Accessed 07 September. 2019].

[2] A. Brenoff, "How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts". HuffPost., 2017. [Online] Available https://www.huffingtonpost.co.uk/entry/romance-scams-online-fbi-facebook_n_59414c67e4b0d318548666f9?guce_referrer=aHR0cHM6Ly9jb25zZW50LnlhaG9vLmNvbS8&guce_referrer_sig=AQAAAEIQc2oZZgY0aojwEad0jzGsayrW4MuO5rA01HIG8XSfcVKWHHHqDaeOe4BJLgqGYGbq1SxePdERrQ23mkRqXQUGKKmrTwOf0MJJda_CQFClfMMJlMLkkLnAIVvc1JhkDxpt0aNdXHCIPZxzzlRKpfCgR0nyrDiH0IBYzVGEx8E1&guccounter=2 [Accessed 14 Aug 2019].

[3] BBC News. (2017). "Online dating fraud victim numbers at record high", BBC News. January 2017. [Online] Available at: https://www.bbc.co.uk/news/uk-38678089 [Accessed 13 Aug. 2019].

[4] Federal Bureau of Investigation, "Internet Fraud", 2019. [Online] Available at: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/ [Accessed 13 Mar 2019].

[5] Action Fraud, "Types of fraud", 2019. [Online] Available at: http://www.actionfraud.police.uk/a-z-of-fraud [Accessed 13 Mar 2019].

[6] Central Bank of Nigeria, "2016 Annual Report of Nigeria Electronic Fraud Forum", 1st ed. [eBook] Abuja, Nigeria, Available at: https://www.cbn.gov.ng/documents/NeFFar.asp [Accessed 16 Apr. 2017].

[7] Internet Crime Complaint Centre "2018 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3) United States. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf. [Accessed 12 Feb 2020].

[8] L. Graham, "Cybercrime costs the global economy $450 billion: CEO". CNBC, 7 February 2017. [Online] Available at: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html [Accessed 12 Feb 2020].

[9] Interpol, (2020). *Unmasked: International COVID-19 Fraud Exposed*. [Online] Available at: <https://www.interpol.int/en/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed [Accessed 21 October 2020].

[10] Forbes (2020), "How e-commerce explosive growth is attracting fraud", Forbes, May 2020, [Online] Available at https://www.forbes.com/sites/louiscolumbus/2020/05/18/how-e-commerces-explosive-growth-is-attracting-fraud/?sh=28677feb6c4b#136539866c4b [Accessed 12, November, 2020].

[11] House of Commons Committee of Public Accounts, The Growing threat of online fraud. London: House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/399/399.pdf.

[12] Office for National Statistics, "Crime in England and Wales: year ending Mar 2019", [Online] Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019#increase-in-the-volume-of-fraud-offences-in-the-last-year.

[13] Australian Competition and Consumer Commission, *Australian business hit hard by email scams*. [Online] Available at: https://www.scamwatch.gov.au/news/australian-businesses-hit-hard-by-email-scam [Accessed 09 June, 2019].

[14] Australian Competition and Consumer Commission. "Scam cost Australians half a billion dollars", 2019. [Online] Available at: https://www.scamwatch.gov.au/news/scams-cost-australias-half-a-billion-dollars [Accessed 10 Jun 2019].

[15] Internet Crime Complaint Centre, "2019 Internet Crime Report". US US Department of Justice, Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA, 2019. [Online] Available at: https://pdf.ic3.gov/2019_IC3Report.pdf [Accessed 15 Nov 2020].

[16] Crowdstrike, "Crowdstrike", 2020. [Online] Available at: https://www.crowdstrike.com/wp content/brochures/reports/NigerianReport.pdf. [Accessed 12 Feb 2020].

[17] Australian Competition and Consumer Commission, "Nigerian scams", 2019. [Online] Available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams [Accessed 13 Apr 2019].

[18] BBC News. "Why Nigeria's Internet Scammers are role models", BBC News. June 2019, [Online] Available at: https://www.bbc.co.uk/news/world-africa-49759392 [Accessed 12, November, 2020].

[19] Kaggle, Fraudulent E-mail Corpus. [Online] Available at: https://www.kaggle.com/rtatman/fraudulent-email-corpus#fradulent_emails.txt [Accessed 12 Aug. 2019].

[20] Action Fraud "Advance fee fraud". [Online] Available at: http://www.actionfraud.police.uk/node/290 [Accessed 13 Mar. 2020].

[21] Federal Bureau of Investigation "Internet Fraud". [Online] Available at: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/ [Accessed 13 Mar. 2020].

[22] Internet Crime Complaint Centre (2018). Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3) United State. https://www.ic3.gov/crimeschemes.aspx#item-12.

[23] Internet Crime Complaint Centre (2016), "2016 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3) United States. https://pdf.ic3.gov/2016_IC3Report.pdf.

[24] Internet Crime Complaint Centre, "2017 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3) United States. https://pdf.ic3.gov/2017_IC3Report.pdf.

[25] Internet Crime Complaint Centre (2018), "2018 Internet Crime Report", Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3) United States. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf.

[26] Graham, L. "Cybercrime costs the global economy $450 billion: CEO". [Online] CNBC. Available at: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html [Accessed 14 Apr. 2020].

[27] Fraud the Facts 2019 https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf.

[28] Russell Jonathan, S. and Norvig, P. (2009). Artificial Intelligence: A Modern Approach. 3rd ed. New Jersey, US: Pearson, pp.860 - 872. ISBN-13: 978-0136042594.

[29] Mathworks (2020). Introducing Machine Learning pdf. https://uk.mathworks.com/help/stats/index.html?s_cid=doc_ftr.

[30] Abiodun Modupe, Oludayo, O. Olugbara and Sunday, O. Ojo (2011). Exploring Support Vector Machines and Random Forests to Detect Advanced Fee Fraud Activities on Internet. 2011 11th IEEE International Conference on Data Mining Workshops. DOI 10.1109/ICDMW.2011.81. pp 331 – 335.

[31] Kerramans Koen, Yan Tang, Rita Temmerman and Gang Zhao (2005). Towards Ontology-based E-mail Fraud Detection. 2005 IEEE Conference on Artificial Intelligence, Portugal. DOI: 0-7803-9365-1/0. Pp 106 – 111.

[32] Pellon Ismael and Patrizia Anesa, (2020). Advance-Fee Scams: A Corpus and Genre Analysis. ResearchGate, 2020. Pp 1- 14.

[33] Rofiat Allia, Rebecca Nicolaidesa, Russell Craig (2018). Detecting advance fee fraud emails using self-referential pronouns: A preliminary analysis. University of Portsmouth, UK. [Online] Available at https://researchportal.port.ac.uk/portal/files/8604176/CRAIG_2018_cright_AF_Detecting_advance_fee_fraud_emails_using_self_referential_pronouns.pdf.

[34] Edward Mathew, Claudia Peersman and Awais Rashid (2017). Scamming the Scammers: Towards Automatic Detection of Persuasion in Advance Fee Fraud. International World Wide Web Conference Committee (IW3C2), 2017. DOI: 10.1145/3041021.3053889. pp 1 -7.

[35] Gao Yangbin, and Gang Zhao. "Knowledge based information extraction: A case study of recognizing emails of Nigerian fraud". Natural language processing and Information systems, NLDB 2005, Alicate Spain, June 15-17, 2005, Proceedings.

[36] Sarwat Nizamani, Nasrullah Memon, and Mathies Glasdam, "Detection of fraudulent emails by employing advanced feature abundance". Egyptian Informatics journal, Vol. 15, pp. 169-174, 20

Automatic Diacritic Recovery with focus on the Quality of the training Corpus for Resource-scarce Languages

Ikechukwu Ignatius Ayogu
Department of Computer Science
Federal Polytechnic, Idah
Kogi State, Nigeria
ig.ayogu@gmail.com

Onoja Abu
Department of Mathematics and Statistics
Federal Polytechnic, Idah
Kogi State, Nigeria
abu.onoja@gmail.com

***Abstract*—The development and availability of high quality corpus for many African languages is still hampered by dearth of appropriate software tools and devices. To be able to rapidly create large quantities of high quality corpus of majority of African and Nigerian languages, a diacritic tool is required. The presentation of texts of natural languages without diacritic marks presents significant problems to both human and computational processing systems due to partial or total loss of the accompanying grammatical, syntactic and or semantic information. This paper investigated the effect of diacritic quality of a small-sized training corpus on the classification accuracy of some simple and commonly used machine learning algorithms for diacritic restoration tasks following the character-based approach. The classification accuracy of eight of the diacritic-bearing characters of Yorùbá language of Nigeria were investigated. The results show that the completeness and correctness of diacritics has a significant effect on the performance of the algorithms; decision tree algorithm produced the overall best accuracy response of 3.22 % to the data quality improvement. The observations from the learning behaviours of the algorithms suggests that a 100,000 words corpus is adequate to train a decision tree model for automatic diacritic restoration for Yorùbá language but insufficient to obtain a state-of-the art results for the LDA, LOGREG and SVM algorithms.**

***Index Terms*—Diacritic quality, Supervised learning, n-gram features, Yoruba language**

I. Introduction

Diacritic restoration is an important low-level text pre-processing task. The process of restoring diacritics involves the replacement of plain input text characters by their corresponding accented and or sub-dotted forms which represent the true authography of the given language. Diacritic restoration is important because it promotes better understanding and utilization of textual contents in human-to-human, human-to-machine, and machine-to-machine communication [1,2,3,4,5]. Diacritic marks impose a restriction on the lexico-semantic and prosodic behaviour of lexical items in the linguistic processes of any language that employ diacritics in its writing system. Unfortunately, the absence of diacritics does not only affect the distribution of texts [6], it also frees the words from lexical, semantic, gramatical and prosodic usage restrictions, thereby creating a variety of lexico-semantic, segmental and suprasegmental difficulties [4,7,8,9]. The presentation of texts of natural languages (electronic or printed) without diacritic marks presents significant problems to both human and computational processing systems due to partial or total loss of grammatical, syntactic and or semantic information they carry [10,11,12].

Diacritics is an integral part of the writing systems of many Nigerian languages and hence these aforementioned problems significantly abound; Yorùbá language, the focus of this paper, prominently employs accents and sub-dots with a high vowel to consonant ratio. These disambiguating diacritic marks are often left out in texts due to the difficulty involved in typing due to lack of appropriate keyboards [6], clumsy input methods where adaptable keyboard exist, indifference [13] and lack of good understanding of the orthographic conventions in the languages, especially for younger citizens that have become extreemely influenced by high-contact English language, the official language of Nigeria.

The trend in the diacritic restoration reseacrh community tends to suggest an increased interest in the more compute-intensive models for automatic diacritic restoration. This is obviously motivated by their perceived superior performance over the simpler models; examples of such is the use of SMT- and NMT-inspired approaches [14,15,16]. However, the issue of data insufficiency arguably, still remains a challenge, nothwithstanding the simplicity or complexity of the models. The problem of data insufficiency remains a problem in the resource-scarce language scenarios because it is established that high-quality outcome requires large-quantities of high-quality input data. This is a significant huddle for many African languages, hence there is an imperative to find leverage in small-sized, high-quality data for high-quality results using simpler, less data-hungry models.

Poor or low data quality is considered an important issue because, as our results show, incorrect and/or incomplete tone-marking in texts increases the ambiguity problem. The lexdiff metric [10] is observed to be affected significantly by

This research received funding from TETFund, Nigeria.

TABLE I: Yorùbá diacritic-bearing symbol variants.

Symbol	a	e	ẹ	i	o	ọ	u	m	n	s
Diacritic variant	à, á, a	è, é, e	ẹ̀, ẹ́, ẹ	ì, í, i	ò, ó, o	ọ̀, ọ́, ọ	ù, ú, u	m̀, ḿ, m̄	ǹ, ń n̄	ṣ

the degree of completeness and correctness of tone/diacritic marks. This is so because as was observed from our data, with correct, complete marking, the number and sizes of ambiguous word types reduces significantly.

This paper reports the effects of diacritic quality on the performance of character-based n-gram features for diacritic restoration using four supervised machine learning algorithms on a 100,000-word corpus. The result shows that decision tree algorithm produces the best response to the improvements in the diacritic quality of the corpus. Thus a decision tree model was then trained using the optimal parameters on an overwhelmingly larger but lower diacritic quality jw300 [17] corpus.

The object of this paper is to provide some insights into how diacritic quality affects the performance of four classic supervised learning algorithms using the character-based sliding window, n-gram based feature context approach on a research-purposed 100,000-word corpus of Yorùbá language. The paper established that the quality of the data in terms of completeness and correctness of diacritization of the training corpus complements the performance of the algorithms. This is because as the quality of the data set increased, there was a correspoding decrease in the lexdiff quantity.

II. Diacritics in Yorùbá Writing System

Yorùbá language has twenty-five symbols in its alphabet, comprising eighteen (18) consonants { *b, d, f, g, gb, h, j, k, l, m, n, p, r, s, ṣ, t, w, y* } and seven (7) vowels { *a, e, ẹ, i, o, ọ, u*}. As predominant in many languages of the world, Yorùbá vowels are the principal bearers of the diacritic marks (tonal accents and sub-dots - separately or combined in a single letter); two sylabic nasals, *m, n* also bear tone marks. The only other consonant that bear sub-dot (not accents) is the symbol *ṣ*. The presence or otherwise of the diacritics affect the phonetic realization of the words. Tonality in Yorùbá is indicated by the use of three tones - low, mid and high tones marked in texts using grave accent, macron and acute accent respectively. The mid tone is however conventionally not marked in writings except for the syllabic nasals. Table I shows these diacritic-bearing letters of Yorùbá writting system.

Tonemes are distribited freely on Yorùbá words but high tones are not permitted to appear on the first syllable when it is a vowel [18]. Tone is a mandatory component of the language and thus diacritic- or tone-bearing symbols must be reflected in true Yorùbá language text. The absence of diacritics alter the intent of the writer/writing; it makes reading and processing difficult. For instance as simple as it appears, writing *sí and ṣí* would default to *si* without diacritics and that simply confuses the intent of the message as exemplified in

(a) Adé ti lọ *sí* ilé-ìwé → Adé has left for school
(b) Adé ti *ṣí* fèrèsé náà → Adé has opened the window.

In (b) above, leaving out the sub-dot in letter *s* would swiftly alter the *act of doing* to the *act of going*, thereby changing the message. The samples in Table II exposes some of the major weakness of writing without diacritic marks in Yorùbá; it shows how the supposed symbols and their diacritic versions are simply latinized, leading to grammatical and semantic confoundment.

In the cases above, well-grounded native speaker would easily walk around the problems posed by ambiguity arising from non-use of diacritic marks by instincts or ability to speedily derive accurate judgement from the context and knowledge of the discourse. It is however not so for anyone who lack adequate linguistic competence or whose language use capacity is low. Machines also suffer from the problems associated with the absence of diacritics [12].

III. Related Work

The literature is replete with implications of missing, incomplete or partial diacritization on texts. The challenges posed include readability and comprehension problems [18] that arises from the ambiguity imposed by the indistinguishability of surface word forms. This ambiguity problems have also been linked to the difficulty experienced by natural language processing systems [10].

Diacritic restoration approaches are segregated based on the level of support tools they incorporate [18]. Some researchers have combined varying degrees of higher-level linguistic resources in an attempt to improve the efficacy of diacritic restoration while others have focused mainly on the use of raw text only. This research is aligned with the latter. The approach is well motivated for the mostly low-resourced Nigerian languages. As noted by [10], backing off from word to grapheme level opens up diacritic restoration to languages for which lexical resources are not available.

Although there are not quite many research publications on diacritic restoration research for Yorùbá and many other Nigerian languages, the awareness for research in this direction has grown substantially. This is evident in the number of research publications by Nigerian authors from 2014 till date on this subject. Noteworthy among these are [12], [18] and [19]. It is noteworthy that all these efforts were motivated by the pioneering efforts of [10], [11] and [20] which specifically formed the bais of [12] and [18]. Motivated by the deficiencies in the latin encoding for many languages of the world and the challenges arising from

TABLE II: Mapping Diacritic-bearing symbols with examples

Symbol	Sym Variants	Mapping	Samples
a	à, á, a	a	aja:aje → àjà, ajá : ajé, àjẹ̀
e	è, é, e	e	eru → èrú, ẹrú, ẹrù
ẹ	ẹ̀, ẹ́, ẹ	e	ekun:esin → ẹkún, ẹkùn, ẹ̀kún, èsìn, ẹsìn, ẹ̀sín
i	ì, í, i	i	ilu: ila: igba → ìlú, ìlù, ilá, ilà, ìlà, ìgbà, ìgbá, igba, igbà, igbá
o	ò, ó, o	o	obi:odo:ogbon → obì, òbí: odò, odó, ọ̀dọ́, ọ̀dọ̀: ọgbọ́n, ọgbọ̀n
ọ	ọ̀, ọ́, ọ	o	oko:okun → ọkọ́, ọkọ, ọ̀kọ̀: òkun, okun, okùn
u	ù, ú, u	u	su:sun → sú, sù, sú: sún, sùn, sun
m	m̀, ḿ, $\bar{m}$	m	mo:mu → mu, mú, mọ̀, mọ́
n	ǹ, ń $\bar{n}$	n	na → ná, nà
s	ṣ, s	s	sile:si → sílẹ̀, ṣílé: sí, ṣí, ṣì

missing diacritics in the available electronics texts that hinder other important activities like corpus compilation and the need to circumnvent reliance on lexical resources that were hardly available, [10] proposed machine learning approaches that rely on local grapheme context; an approach that has become quite popular today.

The character-context-based sliding window feature approach adopted in this paper is well motivated for data-scarce scenarios. Its popularity in recent research puts some earlier views of some researchers on its perfomance into question. The debate centers around its ability to cope with word-level ambiguity but research has subsequently demonstrated that the character-context-based approach is not weak. Recent studies concretely points out that it can compete favourably with the word or syllable approach and this paper would further demonstrate that word-level accuracy for the character-based approach can approach the state-of-the-art when built with complete, accurately diacritic marked data. [18] studied tone-mark insertion in Yoruba text using syllable-based features. The paper compared the syllable-unit to word and character based units for tone-mark determination in a sliding window setup using TiMBL [21] similarly to [10]. A careful study of their results shows clearly that none of the three focus units (character, syllable and word) produced a superior performance, strictly. Other works that are of specific relevance are briefly outlined next.

DePauw *et al* [10] investigated the performance of the MBL algorithm using the local grapheme context approach was evaluated for 7 African languages and 6 languages from Europe as well as China Pinyin using a task-oriented approach (word-level accuracy). Results for Yorùbá was 40.6% at word-level and 68.2 % at the grapheme level. In [12], a total of 100 data sets, derived across 13 different sliding window feature templates were used to evaluate the performance of five learning algorithms for Igbo language. The decision tree algorithm gave the accuracy of 94.49 % for FS1, unigram on each side of the target; the accuracies of the maining models were all above average. Orife [22] on the other hand experimented an MT-inspired formulation of the diacritic restoration task for Yorúbá, similar to [14, 15] and [16] and reported that the type of RNN did not make much difference in the prediction accuracy using the implementation in openNMT [23]. An examination of the results from these two research shows that the simpler approaches are still competitive.

IV. Experimental Setup

The classification accuracy for eight (8) diacritic-bearing characters consisting of the seven vowels and a consonant (*a, e, ẹ, i, o, ọ, u*, s) were investigated. The eight characters were mapped into six symbol groups, according to their base Latin forms. Each mapping group was treated as a separate classification task [24], resulting in one binary, three 3-way and two 6-way classification tasks involving a consistent many-to-one mapping of diacritized symbol respectively to the same latinized form (table III). Thus, the prediction accuracy of each of the selected algorithms was measured at the symbol group level since this reflects the basic representation of the characters in undiacritized texts.

A. Experimental Corpus

The experimental corpora were obtained from three sources: theyorubablog.com *(https://www.theyorubablog.com)*, jw.org *(www.jw.org)* and Yorùbá corpus (*yo-jw300*) from the jw300 corpus [17], a parallel corpus of over 300 languages. Texts from theyorubablog.com can be considered an open-domain text with a good balance of textual content on social, economic, political, cultural and general knowledge discourse. Texts from jw.org on the other hand is religion-oriented, predominantly featuring texts on the teachings of the Christian faith. jw.org also feature texts on scientific, economic, political and socio-cultural discourses but these are discussed with strong religious tone and from biblical perspective. Two experimental corpora were designated: *yoblog-jw-data* (created by combining three-parts of texts from theyorubablog.com with one-part jw.org) and the *yo-jw300* corpus which was chosen because of its overly large size compared to *yoblog-jw-data*, our primary experimental corpora. A study of the *yoblog-jw-data* revealed a considerable level of inconsistent, incomplete and incorrect diacritic markings and thus a high amount of ambiguous tokens. This necessitated manual, hand-correction and the resulting data designated *yoblog-jw-cor-data*. Some statistics on each of these experimental corpora is presented in table IV.

From the statistics in table IV, it is noticeable how the completeness of diacritics on the data (*yoblog-jw-cor-data*)

TABLE III: Symbol-class mapping for the classification task

Latin form (group)	a	e	i	o	u	s
Classes	à, á, a	è, é, e, ẹ̀, ẹ́, ẹ	ì, í, i	ò, ó, o, ọ̀, ọ́, ọ	ù, ú, u	ṣ, s

TABLE IV: Statistics on the experimental corpora

Corpus	Size (words)	Lexdiff	Accented ratio	% Ambig tokens	Token Types
yoblog-jw-data	107,218	1.2643	0.6831	0.9342	5,506
yoblog-jw-cor-data	106,576	1.1378	0.7987	0.6971	4,053
yo-jw300	$>$ 10,000,000	1.1148	0.8435	0.9368	40,295

reduces the degree of ambiguity in the data. The reduction of token types from 5,505 to 4,053 is a strong reflection of the magnitude of improvement resulting from the diacritic normalization.

B. Features and Data Sets

The character-based sliding window approach was adopted in this research because of its language-agnostic properties and suitability for social media applications [24]; an emerging application domain for Nigerian languages.

Samples (training/test instances) were extracted using n-gram context-based features from the experimental corpora described in Section IV-A using a symmetric sliding window mechanism [20, 10, 11, 12,24]. Specifically, the feature spaces described in table V were investigated.

For each window, samples were extracted from the corpus using the structure depicted in table V. i is the diacritic-bearing character in focus whose class is to be determined; to the left of this i^{th} character of interest, is a decreasing index used to keep track of the left context of the n-gram span. A similar interpretation is given to the right context. For each window, data points were extracted from the corpus for the experiments.

V. Experiments, Results and Discussion

A. Experiments

Experiments were carried out to evaluate the effect of partial, incomplete and incorrect diacritics on the prediction accuracy of four learning algorithms: decision tree (DTL), linear discriminant analysis (LDA), logistic regresion (LOGREG) and support vector machines (SVM), for each of the designated character feature templates starting with a bigram (w_2) on either side of the target character and up to a context of six characters (w_6) on either side of the target character. For ease of reference, we designate window n as w_n, interpreted as n characters to the left and right side of the target character. Thus, this defines a $2n+1$ attribute space for each sample in a given feature template. Due to memory limitation, the size of the experimental data set was limited to a maximum of 100,000 in each case and experimented in a 5-fold crossvalidated setup. Three experimental sessions, one for each experimental corpus (table IV), were performed across all the four selected algorithms.

B. Results and Discussion

The first experimental investigation utilized the baseline corpus, *yoblog-jw-data*. This experiment determined a baseline performance of the data prior to the improvement of the diacritic quality of the data by manual, hand-correction. In the second stage, the baseline corpus was substituted with the hand-corrected, fully diacritized version of the corpus, *yoblog-jw-cor-data*, in order to determine the likelihood and scale of performance improvement due to full compliments of diacritic marks on the experimental corpus. Overall, feature templates w_6, w_5 and w_4 showed the most interesting performance across all algorithms and data sets. For ease of reference, the results from the baseline and the fully diacritized corpus are jointly presented in tables VI, VII and VIII where the accuracy of the models for baseline corpus is shown in column b and that of the hand-corrected, fully diacritized corpus is given in column d. To gain insight into the behaviour of the learning models, learning curves were plotted of model's mean square errors (MSE) on the test set as the training set size increases. The learning curves for the best window, w_6 for each of the four algorithms are presented pair-wise in figures 1 to 4.

It is evident from table VI that DTL exhibited the highest overall response in accuracy of predictions on both the baseline and the diacritiaclly improved corpus. Its performance margin increased by an average of 3.22 % across all the symbol-groups from the baseline. Other models achieved a slight increase in prediction accuracy for the various symbol groups except in the case of group *i* for which a significant decline was recorded for LDA, LOGREG and SVM across all the sliding windows. The magnitude of performance improvement is noticed to be dependent on the diacritic variability of the symbol groups, for instance, for the s-group, the increase in the prediction accuracy in table VI is maginal; this is because the symbol s has only one alternative ṣ unlike in the case of groups *e*, *i*, or *o* for which there are many diacritic variants. A similar trend if observed in tables VII and VIII. Also, the average percentage increase in prediction accuracy is found to vary with the sliding window from 3.101 in w_4, 3.103 in w_5 to 3.220 in w_6 for DTL.

Figure 5 shows the overall accuracy of the respective models for each corpus for increasing window size. The effect of missing or incorrect diacritics is strongly indicated in the graphs; this is most especially for the decision tree algorithm. This effect is a reflection of the lower ambiguity in the diacritic normalized corpus. The cross-validated learning curves in figure 1 points to the adequacy of the data for DTL but not so for other models. This is seen in figures 2, 3 and 4. The inadequacy of the data is much more severe for SVM

TABLE V: Sliding-window feature template: $2 \leq n \leq 6$

Window	X_i												Y_i
	$decreasing\,index: \leftarrow$					$focus$	$\rightarrow: increasing\,index$						
w_2					·	·		·	·				
w_3				·	·	·		·	·	·			
w_4			·	·	·	·	$i=0$	·	·	·	·		
w_5		·	·	·	·	·		·	·	·	·	·	
w_6	·	·	·	·	·	·		·	·	·	·	·	·

TABLE VI: Symbol-group accuracy for the baseline corpus (b) and fully diacritized (d) corpora using w_6 feature template

Letter group	DTL		LDA		LOGREG		SVM	
	b	d	b	d	b	d	b	d
a	91.58	95.41	78.97	79.36	80.50	81.23	78.23	79.34
e	92.32	95.71	76.6	79.07	80.34	83.09	77.36	80.63
i	94.78	97.11	83.99	77.80	85.91	81.31	84.53	79.10
o	92.01	95.68	76.99	77.72	79.60	82.65	96.51	78.51
u	93.73	96.77	84.61	86.98	92.65	86.83	85.03	88.20
s	96.40	98.12	92.11	91.45	96.94	96.28	93.93	95.44

TABLE VII: Symbol-group accuracy for the baseline corpus (b) and fully diacritized (d) corpora using w_5 feature template

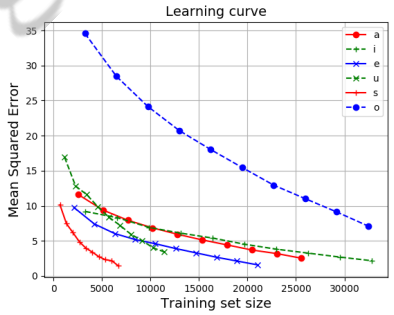
Letter group	DTL		LDA		LOGREG		SVM	
	b	d	b	d	b	d	b	d
a	91.28	95.07	78.94	79.24	80.11	80.83	72.85	76.44
e	92.19	95.58	76.46	78.84	79.70	82.36	70.09	76.38
i	95.19	96.98	83.79	77.43	85.63	80.79	84.22	78.72
o	91.98	95.37	76.95	77.66	79.02	80.57	71.07	75.65
u	93.38	96.45	84.12	86.44	86.73	88.90	78.19	84.28
s	96.13	97.97	93.30	92.48	93.44	95.49	82.74	89.43

(figure 4 (b)). Thus, the performance of the LDA, LOGREG, and SVM models can be improved by increasing the size of the data set.

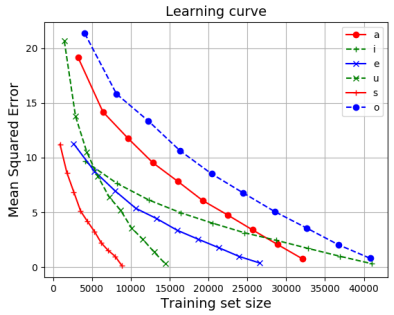
Table IX presents the performance of the decision tree algorithm on the over 10 million word yo-jw300 corpus, using w_6, the best from the two previous experiments. It is however to be noted that the yo-jw300 corpus, though large has many instances of incorrect, missing or partial diacritics. As indicated in table IX, the prediction accuracy is comparable to what was obtained from the 100,000 words experimental corpus. Figure 6 gives an indication that the limit on data has been attained.

C. Conclusion

This paper has presented results from the investigation of the effect of diacritic quality of training corpus on the performance of some simple and commonly used machine learning algorithms for diacritic restoration tasks. The results show that the completeness and correctness of diacritics has a significant effect on the performance of the algorithms but it is most important for the decision tree algorithm. The observations from the learning behaviours of the remaining algorithms suggests that a 100,000 words corpus is insufficient to obtain a state-of-the-art results for these algorithms except for the decision tree algorithm. The target of this paper was to identify a simple algorithm that achieves a state-of-the-art results on a relatively small training corpus since existing research have used larger corpus.



(a) Baseline data



(b) Fully diacritized

Fig. 1: Learning behaviour of DTL with increasing training size and at $w6$

ACKNOWLEDGEMENT

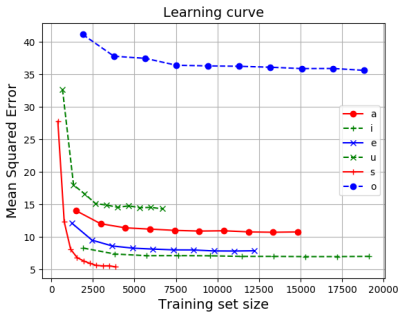
The research presented in this paper is funded by the Tertiary Education Trust Fund (TETFund), Nigeria and through

TABLE VIII: Symbol-group accuracy for the baseline corpus (b) and fully diacritized (d) corpora using w_4 feature template

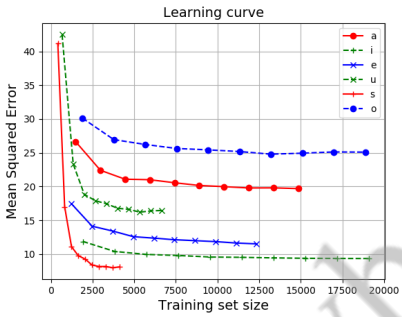
Letter group	DTL		LDA		LOGREG		SVM	
	b	*d*	*b*	*d*	*b*	*d*	*b*	*d*
a	90.29	94.12	78.33	78.76	79.66	80.25	75.38	76.12
e	91.53	94.80	74.76	77.32	79.00	81.29	73.07	75.63
i	94.73	96.41	82.93	76.55	84.49	79.15	81.75	74.45
o	91.31	94.57	76.93	77.47	78.57	80.02	74.84	75.90
u	92.91	95.98	82.50	85.17	85.05	87.51	80.30	83.33
s	95.66	97.71	92.59	91.85	93.88	94.67	89.40	88.74

TABLE IX: Symbol-group accuracy for DTL on yo-jw300 corpus using w_6

Symbol-group	a	e	i	o	u	s
Accuracy	99.573	99.876	99.786	99.673	99.897	99.973

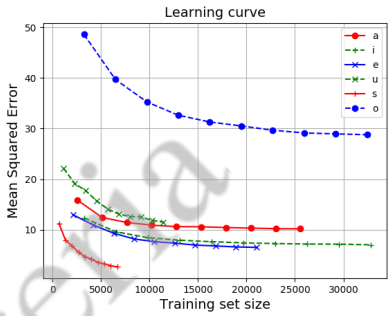


(a) Baseline data

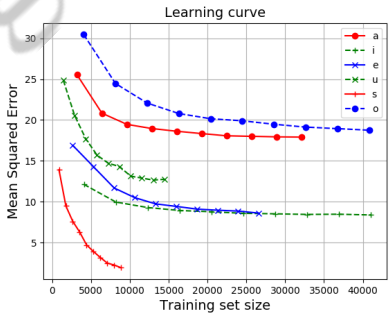


(b) Fully diacritized

Fig. 2: Learning behaviour of LDA with increasing training size and at $w6$



(a) Baseline data



(b) Fully diacritized

Fig. 3: Learning behaviour of LOGREG with increasing training size and at $w6$

the support of The Federal Polytechnic, Idah Kogi State, Nigeria.

REFERENCES

[1] A. Chennoufi & A. Mazroui, Morphological, syntactic and diacritics rules for automatic diacritization of arabic sentences, Journal of King Saud University-Computer and Information Sciences 29 (2017) 156–163.

[2] F. Debili & H. Achour, Voyellation automatique de larabe, in: In Computational Approaches to Semitic Languages, 1998, pp. 42–49.

[3] M. Elshafei, H. Al-Muhtaseb & M. Al-Ghamdi, Machine generation of arabic diacritical marks, MLMTA (2006) 128–133.

[4] E. W. Hermena, D. Drieghe, S. Hellmuth & S. P. Liversedge, Processing of arabic diacritical marks: Phonological-syntactic disambiguation of homographic verbs and visual crowding effects, Journal of Experimental Psychology: Human Perception and Performance 41 (2015) 494–507.

[5] T. V. Asubiaro, Effects of diacritics on web search engines performance for retrieval of yoruba documents, Journal of Library and Information Studies 12 (2014) 1–19.

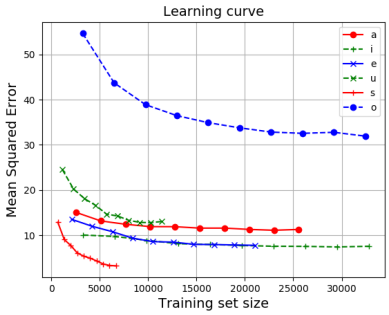
[6] T. Asubiaro, Statistical patterns of diacritized and undiacritized yorb texts, International Journal of Computational Linguistics Research 6(2015) 77–84.

[7] B. T. Hung, Vietnamese diacritics restoration using deep learning approach, in: In 2018 10th IEEE International Conference on Knowledge and Systems Engineering, 2018, pp. 347–351.

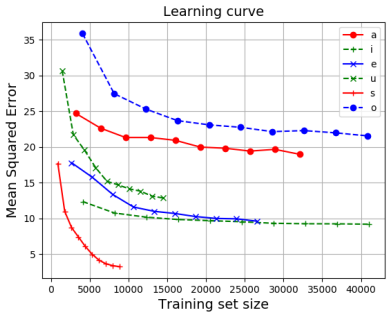
[8] C. Ungurean, D. Burileanu, V. Popescu, C. Negrescu & A. Dervis, Automatic diacritic restoration for a tts-based e-mail reader application, UPB Scientific Bulletin, Series C 70 (2008) 3–12.

[9] O. J. Akporokah, Issues, problems and solutions in english and igbo suprasegmental features: A constrastive analysis, Journal of Resourcefulness and Distinction 14 (2017) 1–7.

[10] G. De Pauw, P. W. Wagacha & G. M. De Schryver, Automatic diacritic restoration for resource-scarce languages, in: In International Conference on Text, Speech and Dialogue, Berlin, 2007, pp.170–179.

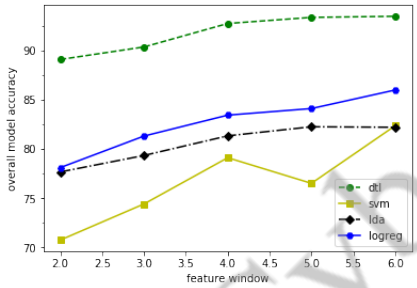


(a) Baseline data

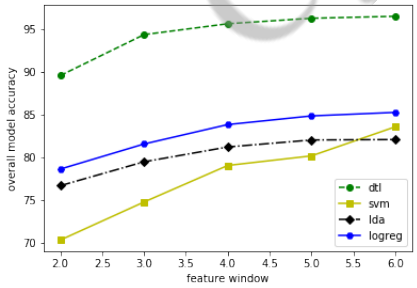


(b) Fully diacritized

Fig. 4: Learning behaviour of SVM with increasing training size and at $w6$



(a) Baseline corpus



(b) Normalized corpus

Fig. 5: Overall model accuracy for different window sizes and corpora

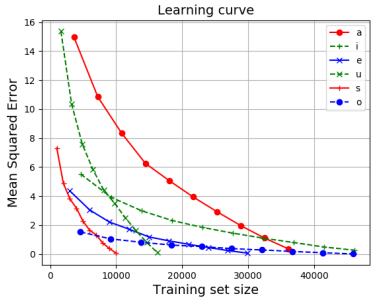


Fig. 6: Learning behavior of DTL on the jw300 data

[11] K. P. Scannell, Statistical unicodification of african languages, Language resources and evaluation 45(3) (2011) 375–386.

[12] I. Ezeani & M. R. Hepple, I. Onyenwe, Lexical disambiguation of igbo using diacritic restoration, in: In Proceedings of the 1st Workshop on Sense, Concept and Entity Representations and their Applications, ACL, 2017, pp. 53–60.

[13] A. Lánínhún & O. Olakojo, The use of diacritised letters in yorb text messaging among mobile phone users in Ọ̀yọ́ East local government area of nigeria, Yorb: Journal of the Yorb Studies Association of Nigeria 8 (2017) 1–38.

[14] T. H. Pham, X. K. Pham & P. Le-Hong, On the use of machine translation-based approaches for vietnamese diacritic restoration, arXiv preprint arXiv:1709.07104 (2007).

[15] T. Schlippe, T. Nguyen & S. Vogel, Diacritization as a machine translation problem and as a sequence labeling problem, in: In Proceedings of the Eighth Conference of the Association for Machine Translation in the Americas, 2008, pp. 270–278.

[16] T. N. D. Do, D. B. Nguyen, D. K. Mac & D. D. Tran, Machine translation approach for vietnamese diacritic restoration, in: In 2013 IEEE International Conference on Asian Language Processing, 2013, pp. 103–106.

[17] Z. Agi & I. Vuli, Jw300: A wide-coverageparallel corpus for low-resource languages, in: In Proceed-ings of the 57th Annual Meeting of the Association for Computational Linguistics, Italy, 2019, pp. 3204–3210.

[18] F. O. Asahiah, O. A. Odejobi & E. R. Adagunodo, Restoring tone-marks in standard Yorb electronic text: improved model, Computer Science 18 (2017) 301–315.

[19] T. Adegbola, L. U. Odilinye, Quantifying the effect of corpus size on the quality of automatic diacritization of yorb texts, in: In Proceedings of 3rd International Workshop on Spoken Languages Technologies for Under-resourced Languages, Cape Town, South Africa, 2012, pp. 48–53.

[20] R. F. Mihalcea, Diacritics restoration: Learning from letters versus learning from words, in: In International Conference on Intelligent Text Processing and Computational Linguistics, Heidelberg, 2002, pp. 339–348.

[21] W. Daelemans, J. Zavrel, K. Van Der Sloot & A. Van den Bosch, Timbl: Tilburg memory-based learner, Tilburg University (2004).

[22] I. Orife, Attentive sequence-to-sequence learning for diacritic restoration of yorb language text, in: In Proceedings of Interspeech, 2018, pp. 2848–2852.

[23] G. Klein, Y. Kim, Y. Deng, J. Senellart & A. M. Rush, Opennmt: Open-source toolkit for neural machine translation, 2017, pp. 67–72.

[24] J. Ács & J. Halmi, Hunaccent: Small footprint diacritic restoration for social media, in: In Normalisation and Analysis of Social Media Texts (NormSoMe) Workshop Programme, 2016, p. 1

Design of a customer-centric surveillance system for ATM banking transactions using remote certification technique

Olugbemiga Solomon POPOỌLA
Department of Computer Science
Ọsun State College of Education
Ila-Ọrangun, Nigeria
popsol7@yahoo.com

Adebayọ Olusọla ADETUNMBI
Department of Computer Science
Federal University of Technology
Akurẹ, Nigeria
aoadetunmbi@futa.edu.ng

Chukwuemeka Christian UGWU
Department of Computer Science
Federal University of Technology
Akurẹ, Nigeria
ugwuemmy407@yahoo.com

Ibraheem Temitọpẹ JIMOH
Computer Resource Centre
Federal University of Technology
Akurẹ, Nigeria
ibraheemjimoh@gmail.com

Kayọde Boniface ALESE
Department of Cybersecurity
Federal University of Technology
Akurẹ, Nigeria
bkalese@futa.edu.ng

***Abstract*—Automated Teller Machine (ATM) is a major tool for electronic banking (e-Banking). It enables the availability of banking services anytime and anywhere. Presently, most ATMs communicate only with the banking system networks for security monitoring and enforcements. This design presents a customer-aware surveillance system for all attempted ATM banking activities. Employing a graphical modeling tool (Unified Modeling Language), the design integrates an additional input, through an inbuilt IP Camera that stealthily captures the ATM user facial image; which is automatically transmitted to the mobile device of the bank account owner, through some dedicated artificial intelligent agents, for remote certification; which either authorizes the transaction appropriately, or signals a security-violation alert to the banking security system. Thus, online and real-time monitoring of ATM banking transactions is enabled; reporting suspected unusual attempts to account owner and bank security unit. Hence, customer-level visibility of ATM banking security, through remote certification of a proxy ATM user, is made possible.**

Keywords—automated teller machine transactions security, electronic surveillance, artificial intelligent agent, objects oriented design, unified modeling language

I. INTRODUCTION

Secure banking transactions through Automated Teller Machine (ATM) require the physical presence of the account owner at the ATM post. This is because all known ATM security systems request for some form of inputs from the account owner; and the visibility of transaction security-status is limited to the banking systems [10–17]. Moreover, most countermeasures for attacks via ATM are post-attack in nature, because unsuccessful transactions are not reported on real-time basis; that is, no customer-bound alert on attempted, aborted, or failed transactions.

However, reports of successful transactions, in form of SMS/Email alerts, are sent to the customer. But, reversing a completed stealthy operation, whose possible traces could be hidden, with no automated tracking or retreating system to undo the transaction, might be doubtful. The possibility of blocking an account with suspected successful transactions is absolute – that is, account would be blocked to both the attackers and the owner; and the unblocking of such account is usually not fully electronic. Hence, the existing possible countermeasures for suspected ATM transactions are tedious, unfriendly, not immediate, nor customer-visible.

As development advances on the positive side of computing evolutions, so is the versatility of the code-breakers. Every invention in the computing technology gives birth to its own security issues. Security challenges are now more complex because wireless connectivity has become inevitable, for most business organizations, in order to take full advantages of information technology (IT) [1]. Security risk, threat and vulnerability associated with the deployment of automated system are becoming alarming. Many of these security issues are being taken care of; by hardening and fortifying the internal and external perimeter of the system, by building restrictions into the usage mechanisms, or by completely blocking unauthorized usage [2]. Unlike internal threats, external threats are easily recognized; thus, appropriate remediation may not be costly. Internal security becomes more complex and cumbersome when proxy usage of a system is inadvertently permitted.

ATM, like many other banking tool, allows proxy users. For instance, trusted subordinates could assist their busy-boss to withdraw cash through ATM, using the boss ATM card and personal identification number (PIN). This possibility gives anybody in the custody of such security tool and information the opportunity to use them illegally; the acquisition mode of such sensitive tool and/or information notwithstanding. Such burglary attempts are internal to the account owner; and the possible unimpeded proxy usage of ATM constitutes a potent attack vulnerability. Meanwhile, common security of ATM transactions relies mostly on the integrity of the secure crypto processor [3]. Encryption of personal information is being used to prevent fraud of sensitive data while in transit between the ATM and the financial network.

Suppose an intimate acquaintance of the account owner fraudulently attempt to use the ATM card without prior consent; or decided to abuse some earlier privileged consents; or was tempted to withdraw above an authorized amount; or stealthily want to have knowledge of the account balance. Suppose the ATM card of a bank account is lost or misplaced together with some helpful security particulars; or the security particulars are successfully hacked. These, and such many other, scenarios are the motivations for a computing design, capable of keeping account owner and

account custodian aware of all activities and events at the ATM post [4].

II. Appraised Reviews of Related Works

Including human iris as a key security element of the database [10], the basic ATM authentication method was replaced with iris recognition. Extracted iris features stored in ATM smart card are compared against the acquired data from the camera and the database. This would definitely restrict the ATM user to the bank account owner only.

Implementing typing pattern recognition as an additional layer of security to the card and personal identification number (PIN) authentication process of ATM [11], keystrokes were extracted as the user types the PIN. Extracted habitual pattern is compared against that of the database. Behavior recognition is subject to training, during which bugs could be introduced. More importantly, behaviors depend on the degree of functionality of parts of human body, which could change with changing psycho-physiological states. Again, the user must be the owner.

As a second-level security, when fingerprint verification is successful, a verification code is sent to the global system for mobile communication (GSM) device of the account owner, without which access is permitted; even if the password is cracked or stolen [12]. This, also, necessitates the physical presence of the account owner at the ATM.

With account database containing fingerprint attached with a corresponding identification number, bank account could be accessed, without an ATM card, by using Advanced Encryption Standard (AES) algorithm. The keypad and fingerprint scanner serve as an input to ATM [13]. Encryptions are capable of blocking any form of security-data interception by third parties. In this case, however, the ATM user must be the account owner.

A multilayer security mechanism was presented [14], which utilized a multimodal biometrics authentication: Deoxyribonucleic acid (DNA) and fingerprint. Impression of finger (captured real-time) and DNA barcode (stored on ATM card) are taken as inputs into the ATM, where features extracted are verified with the stored account database. This compels the presence of the account owner at the ATM.

Presenting a secure bio-cryptographic authentication system for card-less ATM using enhanced fingerprint biometrics trait and encrypted personal identification number (PIN) [15], Log-Gabor filtering algorithm was adopted, on fingerprint biometrics and truncated SHA512/256 crypto-graphic hash algorithm to secure PIN, as second-level of authentication. Here, the fingerprint was captured real-time; and would always require the account owner's attention.

PIN verification and fingerprint recognition [16] was combined for identification. When fingerprint is verified, a four digit one-time-password (OTP) is generated and sent, through the GSM technology, to the mobile number of the account owner. For a possible enrolment of account owner fingerprint, the physical appearance is still mandatory.

Conceptual model of an Automated Fingerprint Identification Machine (AFIM) was presented [17]. In the AFIM model, even if a user PIN is hacked, the model with the exact reference fingerprint allows only a valid finger image for the password enrolment. Even this high level ATM design requires that customers must register fingerprint personally at the ATM.

Whoever is in possession of valid security information of a bank account possesses unhindered accesses to that account, hackers/thieves inclusive. The means through which the enabling access right/privilege is obtained is not a concern in this work, because such access could be permitted intentionally by the account owner. Whether the consent is deliberate or otherwise, ATM proxy usage is certainly possible; and judging from the reviewed related works, no known security mechanism is available in such sphere.

In all the reviewed related works, the requirement of the physical appearance of the bank account owner at the ATM, to validly enable any transaction, is mandatory. In their mechanisms, although the object of proxy was successfully blocked, that blocking the proxy user would invariably block the proxy method is doubtful. Again, outright blockage may be counter-valuable; especially, when proxy usage is considered best option regarding ensuing circumstantial exigencies, such as some unforeseen events of psycho-physiological related contingencies. Thus, taking care of these identified drawbacks is worthwhile, because planning for failure is fundamental to security design principle.

In real-life practice, absolute blockage of ATM proxy user is observed to be inherent in the contemporary ATM security measures. Meanwhile, versatility (flexibility) is always a key requirement of human systems; and artificial intelligence should adapt to the changing human nature. However, relative blockage of ATM proxy usage (relative to the transactions certification by the bank account owner) is a possibility; whose exploration is considered worthwhile.

III. The ATM Security Design Requirements

The main components of ATM that affect the interaction between ATM and its users are: Key Switch (to start up or shut down the ATM), Card Reader (to read the magnetic stripe of users' ATM cards), Screen (to display messages to users), Key Pad (to enter information into the ATM), Cash Dispenser (to dispense cash for users), Deposit Slot (to deposit cash or checks from users), Printer (to print receipts), and Communication Network Infrastructure (to communicate with the bank upon any transaction or activity) [5].

In addition to the primary components, inbuilt IP Camera is needed to be incorporated into the ATM to capture the user facial image. Internet-friendly mobile communication device, which is accessible on 24/7 bases, is required for the bank account owner to handle the remote certification. Dedicated intelligent agents for intelligent monitoring of initiated transactions and real-time feedbacks (alerts) to appropriate banking security points. Robust Internet and GSM networks are needed to enable multimedia messaging services (MMS) for certification and authorization processes.

Handling security at specification and design levels, identifying areas to deploy security mechanisms to catch security exceptions when they occur, is a challenging task in software engineering. The process may seem counter-intuitive. This is because conventional requirements stipulate that the system must do something, while security requirements are frequently focused on ensuring something must not be done. Moreover, security is focused not solely on what is supposed to happen, but also what may go wrong.

The Use Case model's end-to-end view of the system shows the impact of choosing to deploy or not deploy security mechanisms at different points in the system. Use Case model places requirements in a certain context. Context is critical in security. Contextually, how the Use Cases are related to the assets that the security mechanisms must protect, and the overall flows, dependencies and assumptions that the system makes, could be shown. Use Case models provide a format to conduct architectural trade-off analysis of security mechanisms at different points in the system [9].

IV. The ATM Security Design Approach

In Object Oriented Design (OOD), a software system is designed as a set of interacting objects that manage their own private state and offer services to other objects. Objects are created by instantiating an object class that defines the attributes and operations associated with the object. Several objects of the same class may co-exist in the same program. Object classes are abstractions of real-world or system entities that encapsulate state information, and that define a number of operations (services or methods) that create, access, or modify the state. Objects are independent entities that may readily be changed because state and representation information is held within the object. Changes to the representation may be made without reference to other system objects. System functionality is expressed in terms of operations or services associated with each object. Objects interact by calling on the operations defined by other objects. Interaction is shown by arrows linking the objects. There are no shared data areas. Objects communicate by calling on services offered by other objects rather than sharing variables. A program component cannot be affected by modifications to shared information. Changes are therefore easier to implement. Objects may be distributed and may execute either sequentially or in parallel.

OOD is a paradigm that is replacing function-oriented designs. OOD combines both data and methods into cohesive units (classes). Universal Modeling Language (UML) is a notation that is often used to model Object Oriented (OO) systems. It provides various diagrams for modeling OO system's structure, dynamic behavior, states and architecture. Creating an OOD is an iterative process based on applying the knowledge stored in a system's Use Cases. UML is used by various OOD methodologies to capture decisions about the structure of a system under design [6].

UML describes a system from a number of views, which represent properties of the system, from various perspectives and, relative to various purposes. Views are presented in models, which define a number of model elements, their properties and the relationships between them. The information contained in a model is communicated in graphical form, using various types of diagram [7]. The UML standard specifies diagram types for documenting the system models. Each diagram type models a distinct characteristic of a system's structure. For instance, Use Case Diagrams model the interactions between a system and its external entities (actors) in terms of use cases; Class Diagrams model the classes, or building blocks, used in a system. UML employs Use Case modeling, which identifies the use cases of the system, each representing a different capability that the system provides to its clients. Each Use Case describes a typical scenario for which the user uses the system. Use Cases are used to generate a shared understanding of the problem to be solved, the key relationships and actors in a system [8]. For each Use Case scenario, a well-defined task is identified; that is, a unique system entity with distinct identity. Each of these is structured to indicate a vivid procedure of how the outcome of the scenario is accomplished; and this is represented in a set of diagrams usually referred to as Activity Diagrams. The activities in these activity diagrams are also organized in an orderly sequence, to indicate when and for how long a procedure is actually carried out, in a set of diagrams usually referred to as Sequence Diagrams.

V. Conceptual Frameworks of the ATM Security

The components of the ATM security system include the ATM Banking System (ATMBS), the ATM Display Screen (ATMDS), the ATM Card Reader (ATMCR), the ATM Key Pad (ATMKP), the ATM Cash Dispenser (ATMCD), the ATM Cash Stocks System (ATMCSS), the ATM Card (ATMC), the ATM User (ATMU), the Bank Database System (BDBS), the Bank Security Surveillance System (BSSS), the Bank Accounts Basic Information (BABI), the Bank Account Biometric Data (BABD), an IP Camera (IPC), a Bank Account Owner Mobile Device (BAOMD), a Dedicated Verification Intelligent Agent (DVIA), a Dedicated Authorization Intelligent Agent (DAIA), and a Dedicated Anti-Burglary Intelligent Agent (DABIA). Fig. 1 below shows these components.

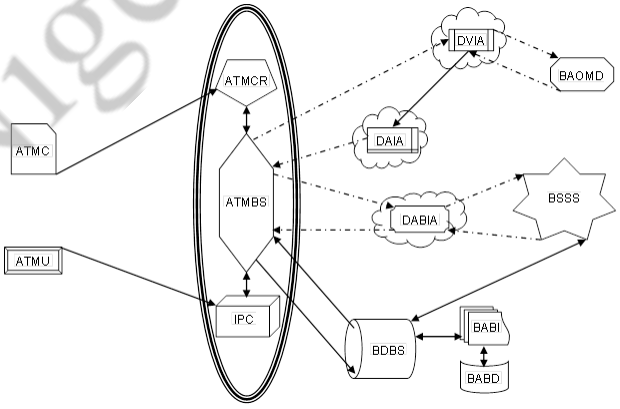


Fig. 1. Architecture of the ATM security system

The ATMBS is the main processor of all the ATM processes; and it is basically composed of the ATMDS, ATMKP, ATMCD, and ATMCSS. It manages and coordinates all communications from and to the banking financial systems. It prompts the user for actions; and displays the current status of transaction. It receives checks for deposits; and dispenses cash for withdrawals. It manages the connections with the BAOMD; and coordinates the communications with the BSSS. It interfaces with the ATMCR and the IPC.

To achieve a relatively high speed and low processing overheads (memory, processor time and network volume), agency technology was employed in the connection between the ATMBS and BAOMD, and the interaction between the ATMBS and BSSS. Between ATMBS and BAOMD, two dedicated intelligent agents are used. In this communication, DVIA handles the verification process. At the termination point of the verification, DAIA is invoked for authorization purpose. If verification fails, return is passed through the DAIA to the ATMBS, which consequently connects the

BSSS through DABIA for burglary alert, which initiates procedures for on-the-spot (live) arrest of suspect(s).

The solid arrow-headed connectors indicate direct (wired) connections among components; but the dotted arrow-headed connectors imply remote (wireless) connections. Some connections, together with their corresponding components, are visibly omitted from the architectural presentation in order to ensure clarity, simplicity, and readability, which is void of any ambiguity. Such components are considered to be basic to the features and operations of ATM.

BDBS is the reservoir of the several kinds of banking information. It consists of the BABI, which in turn interfaces with BABD for bank accounts security information. It gates all information to the bank account details. BABI contains basic information on bank accounts. All queries to BABD are routed through the BABI; and any request from BABI is channeled through the BDBS. This doubles the security layers for BABD. BDBS also interfaces with the BSSS for exchange and sharing of relevant security information.

The ATMCR reads the ATMC for authentication of the bank account. After the validity of the card cum the bank account has been ascertained, the IPC is invoked for capturing the facial image of the user. The ATMBS maps the user image with BABD contents for certification purpose. If the user is the owner of the bank account, a prompt to enter the withdrawal amount is displayed on the ATMDS. The ATMKP is used to key in the withdrawal amount, and the normal usual ATM procedures continue. If the user is not the owner of the bank account, the BAOMD is connected to allow the account owner to verify the authenticity of the usage of the ATMC. For the verification, the ATMBS communicates the facial image of the ATMU to the BAOMD so that the real owner of the ATMC is enabled to authorize the usage of the card, and set the maximum allowable withdrawal for that particular user. This withdrawal limit is passed to the ATMBS, which displays the set limit on the ATMDS as just information for the ATMU for some set duration of time. If verification declares a suspected burglary attempt, alert is passed to BSSS for physical interception of the suspect. Under such circumstances, authorization procedure is automatically bypassed.

Among all these components, the attribute from the IPC object is strategic to our design; mapping and matching the user's facial image with the BABD via the BDBS for authentication; collaborating with the BAOMD and the BSSS for verification, authorization and anti-burglary purposes.

A. Transactions Communication Flows for ATM Security

Real-time intelligence is time critical, and so are its security mechanisms. The design consists of IPC image capturing, image/message sending and receiving in a form of SMS/MMS through GSM network, SMS/MMS received by BAOMD, which returns authorization receipt to ATMBS, with communication details being tracked by BSSS. SMS/MMS are delivered within a few second where GSM coverage is available. GSM technology possesses the highest tolerance for network failure, so the delivery of message is guaranteed; even if the network is temporarily unavailable.

The design involves a single-cycle execution (IPC sends, and BAOMD replies), with just a pair of data (ATMU picture with authorization request) for sending and a single data (BAOMD authorization message) for replying. This indicates a negligible number of instructions and execution time. Moreover, with automatic, immediate delivery of user-created content, SMS/MMS (through GSM) supports international roaming with very low latency for messaging services for multiple users. Therefore, the tolerable delay, due to network failure, is considered as a worthwhile trade-off for securing ATM proxy usage. Even that delay could serve a positive purpose, as it is against the wish of burglars, because of burglary time consciousness.

B. The Graphical Models for the ATM Security

Suppositions basic to this design's outcome are that it is an additional layer of security; under excellent banking communication network that accommodates parallel and distributed computing, capable of online and real-time jobs delivery; with ATM subscribers taking adequate security responsibility for their mobile devices; in nations where ATM-fraud legislations with prompt litigations are in force.

For the ATM security design, using UML standard notations, the Use Case diagram is depicted in Fig. 2. Fig. 3 through Fig. 7 present the Activity diagrams. Fig. 8 to Fig. 11 present the Sequence diagrams. The Class diagram is presented in Fig. 12.

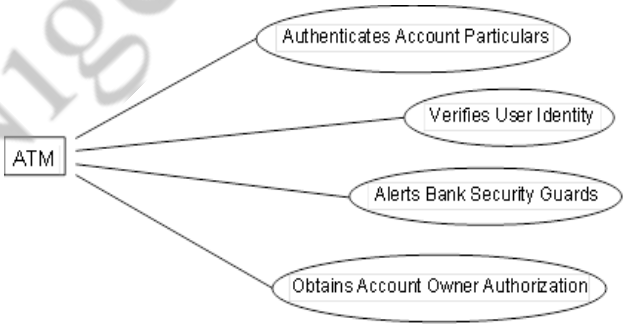


Fig. 2. Use Cases for the ATM security system

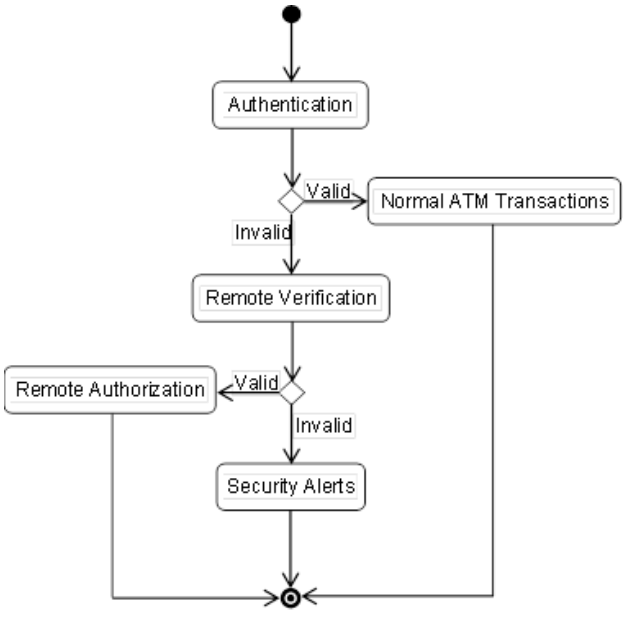


Fig. 3. Overall Activity Diagram for the ATM security system

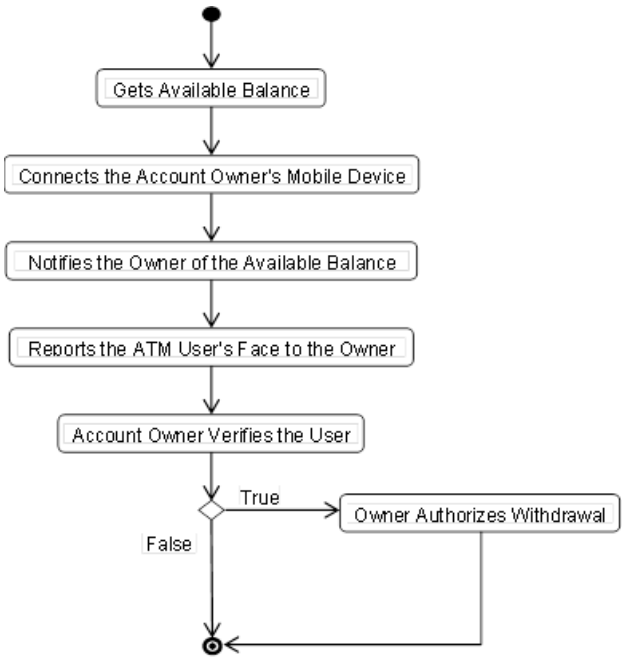


Fig. 4. Activity Diagram for account authentication

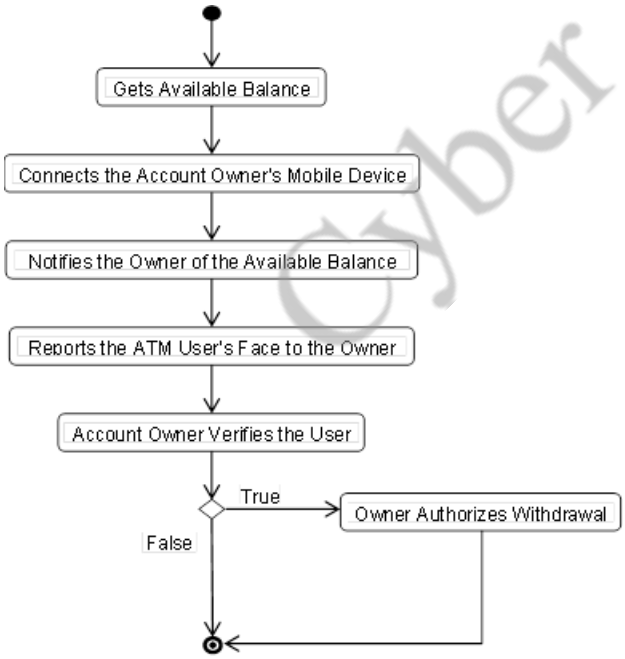


Fig. 5. Activity Diagram for remote verification of user by account owner

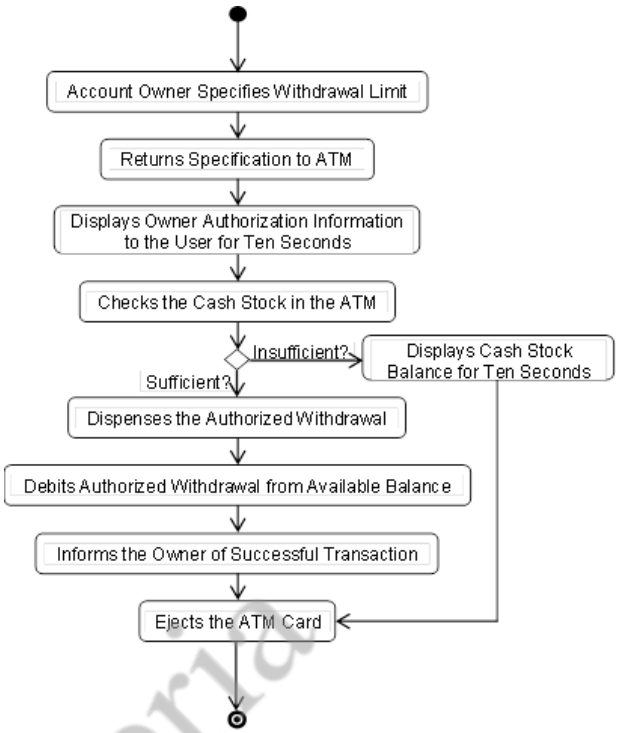


Fig. 6. Activity Diagram for remote authorization by account owner

Fig. 7. Activity Diagram for the burglary alert

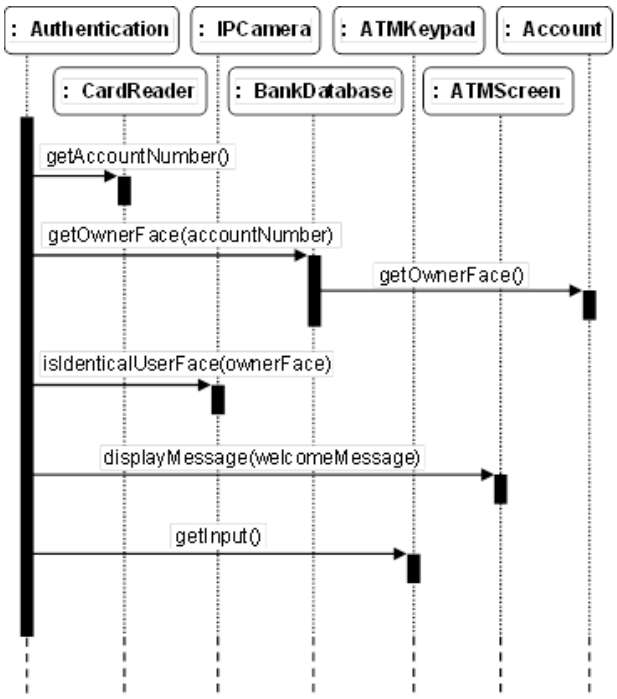


Fig. 8. Sequence Diagram for account authentication

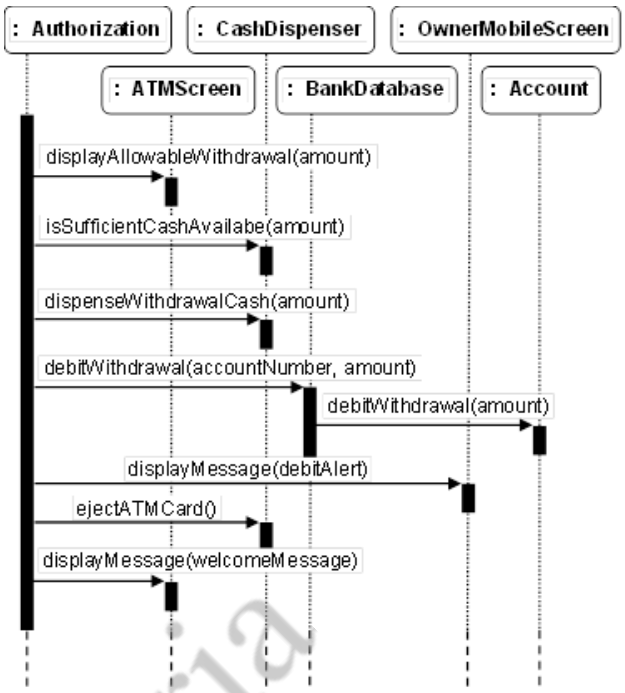


Fig. 10. Sequence Diagram for remote authorization of user by the owner

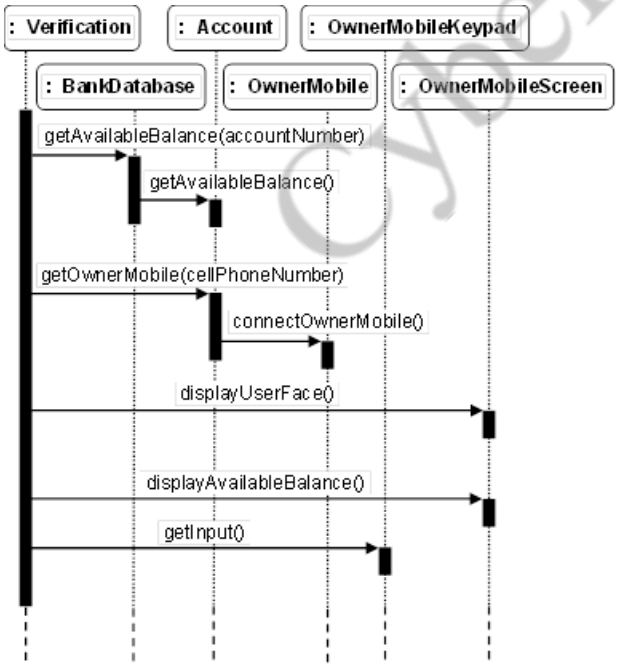


Fig. 9. Sequence Diagram for remote verification of user by the owner

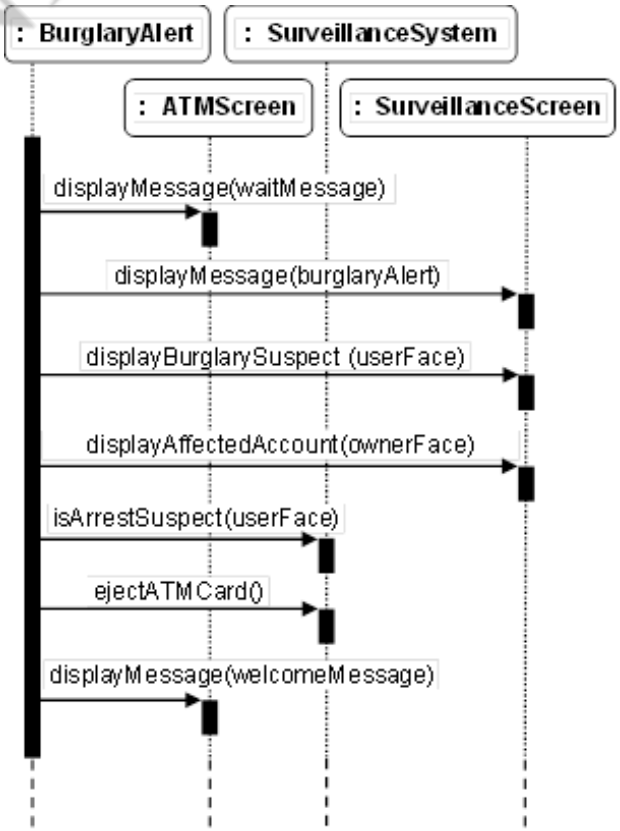


Fig. 11. Sequence Diagram for burglary alert

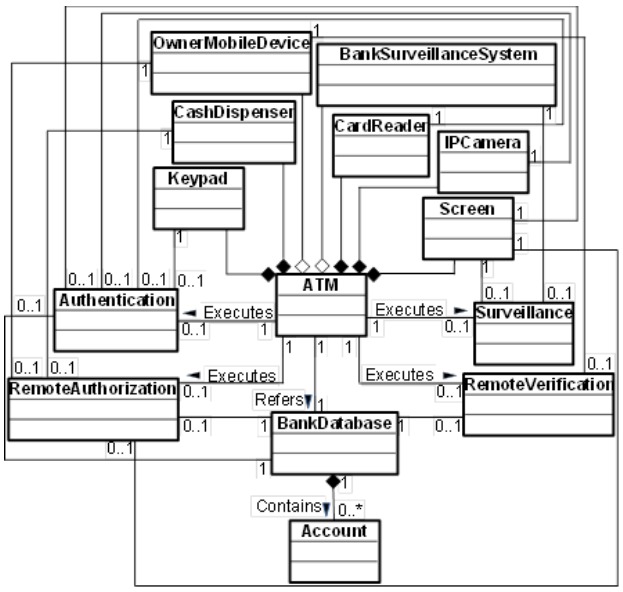


Fig. 12. Class Diagram for the ATM security system

C. *The Security Design Descriptions*

The Use Case contains all system activities that are significant to the users. The Use Case identifies the system users and the activities of each user in the system. Fig. 2 represents the system's Use Cases for authentication, verification, authorization and security surveillance. This describes, in the simplest manner, what the system is expected to do; highlighting the basic activities of the system. The authentication use scenario confirms the ownership of the bank account through the ATM Card; by wirelessly connecting to the bank accounts database. The verification use scenario certifies the current holder of the ATM Card (a proxy user), on the Mobile Device of the account owner, by using GSM SMS/MMS. The authorization use scenario approves a proxy usage of the ATM Card and withdrawal limit, or in case of suspected burglary, uses the Mobile Device of the account owner to alerts the bank security surveillance system for on-the-spot arrest by the bank security unit. The surveillance use scenario holds on the user until arrest is successful, by using a "WAIT…PROCESSING" prompt, and disabling the ejection of the ATM Card; through the security monitoring system of the bank, which finally ejects the ATM Card after successful arrest.

The Activity Diagram represents the state of doing something in the system. It models the workflow; describing what actions need to take place. Fig. 3 describes the overall general scenario comprising all the activities required of the system. Fig. 4 through Fig. 7 shows how the individual scenario takes place. These describe the detailed methodologies require to implement the use scenarios for all the use cases (Authentication, Verification, Authorization and Surveillance); using UML notations.

The Sequence Diagram reflects the interaction between objects; clarifying the behavior for a Use Case; showing how certain object works, and how various objects interact. Sequence diagrams are a refinement of Use Cases. Fig. 8 through Fig. 11 describes the timelines, the phases, the stages, and the steps through which the methodologies, depicted in the activity diagrams, would be carried out. These are descriptions of when what is to be done, how long each procedure should take, and the order which all the procedures should follow, from initialization point to termination point; using UML full representations.

The Class Diagram is most widely used diagram in modeling object-oriented system. It shows a set of classes, interfaces, associations and generalizations. It visualizes and documents structure models; constructing executable system with forward, reverse and round-trip engineering. Fig. 12 describes the basic components involved in the system's model architecture. It defines the associations, interfaces and relationships among these components; indicating the directional flows. Here, only the class names are indicated. For clarity purpose, the attributes and the operations of the classes are omitted. While the Owner Mobile Device and the Bank Surveillance System have aggregation relationships with the ATM, the ATM has composition relationships with the IP Camera, Card Reader, the Screen, the Keypad, and the Cash Dispenser. The Bank Database has a composition relationship with the Account. The Bank Database contains zero or more Accounts. The ATM references just only one Bank Database at a time. The ATM executes zero or one Authentication, Verification, Authorization and Surveillance Alert. The Card Reader, the IP Camera, the Screen, the Bank Database, and the Keypad are associated with zero or one Authentication at a time. The Owner Mobile Device and the Bank Database are associated with zero or one Remote Verification. The Owner Mobile Device, the Screen, the Bank Database, and the Cash Dispenser are associated with zero or one Remote Authorization. The Screen and the Bank Surveillance System are associated with zero or one Surveillance Alert at a point in time.

VI. The ATM Security Design Operations Evaluation

The image/message, which is sent in a form of SMS/MMS through GSM network, is received by BAOMD within a few seconds. Even, if the network is temporarily unavailable, delivery of message is guaranteed, because GSM technology possesses the highest tolerance for network failure.

Negligible number of instructions and execution time are required. Single-cycle execution (ATMBS sends, BAOMD replies); with just a pair of data for sending (ATMU picture and authorization request), and a single data for replying (BAOMD authorization response)

SMS/MMS (through GSM) supports international roaming; with automatic, immediate delivery of user-created content and very low latency for messaging services for multiple users. The tolerable delay, due to possible temporary network failure is a worthwhile tradeoff for securing ATM proxy usage, because such delay is against burglary timing-consciousness.

VII. Conclusion

ATM burglars advance in techniques and increase in number every day. Apart from many other means through which bank account security information could be fraudulently obtained, it is characteristic of human being to abuse trust. Even, bank accounts are becoming less attractive to hackers; instead the ATM machine has recently become the main target of attacks. Therefore, forensic approach to

banking frauds is becoming out-dated. Hence, stealthily tucking in biometrics into the nucleus of existing layers of defense might wade off some wiz sophistications; making the activities at the ATM posts visible to both the bank account owners and the bank security authority.

OOD possesses requirements for the design of a solution of such magnitude. It has capabilities for encapsulation, inheritance and polymorphism, which by themselves are implicitly enhancements for confidentiality, integrity and availability (CIA) of data. UML is one of the design tools that adapts adequately and appropriately to the definitions of OOD. Use Case is a major technique in UML; modeling places requirements in a certain context. Context is critical in security, in that the context can show how the use cases are related to the assets which the security mechanisms must protect.

The ATM security design involves, on real-time basis, the bank account owner in all the available and accessible financial transactions. Whenever all possible attempted ATM transactions, by a user, finally fail, the bank security unit is automatically connected for possible interception of suspects. The design is basically easy to read, implement, update, upgrade, and maintain; it is simple to understand, and self-documenting; permitting distributed and parallel computing implementations with seamless portability capability.

Summarily, often nature dictates PROXY attendance to issues; and ATM in banking is not an exception. Contemporary ATM proxy transactions are insecure, so additional biometrics security layer to the existing ATM layers of defense becomes inevitable. OOD approach was employed, for encapsulation, inheritance and polymorphism capabilities, to enhance the necessity for confidentiality, integrity and availability. UML tool was used in order to display explicit descriptions of use-case, activity, sequence and class of the security system. Designed to stealthily tuck into the nucleus of ATM processes, lightweight intra and inter communication mechanisms were employed. Agency technology intra-module communication was used in order to ensure very small system overheads, and very high processing speed. GSM/Internet inter-gadget connection was engaged to enable SMS/MMS messaging packets, and an excellent tolerance for temporary network failure; which possesses very low latency for messaging services for multiple users, with supports for international roaming. Thus, the possibility of achieving an end-to-end ATM security visibility (that is, visible to the banking security systems/authority, and simultaneously visible to the bank account owners) was successfully demonstrated.

VIII. Future Further Works

The formal verification of this design is important. In the near future, the mathematical formulations and formations of this graphical model would be constructed. Majorly, we hope to adapt the Sequence Diagrams to achieve the formal verification. This is because the sequence diagram illustrates the security mechanisms timelines: when what is to be done, how long each procedure should take, and the order which all the procedures should follow during ATM transactions.

Next in the future, the implementation of the design would be carried out. Both the mathematical and the graphical models would be useful to accomplish the implementation.

References

[1] O. C. Akinyokun, "Neuro-fuzzy expert system for evaluation of human resources performance," Public Lecture Series of the First Bank of Nigeria PLC Endowment Fund, 10 December 2002, Akurẹ, Nigeria. Akurẹ: The Federal University of Technology, 2002.

[2] O. S. Popoọla, O. D. Ajayi, and A. K. Salawu, "Electronic processing of examinations for educational systems (EPEES): A security framework," KIJE, vol. 2(1), pp. 193 – 206, 2014.

[3] S. K. Singh, Bank regulation. New Delhi: Discovery Publishing House, 2009, pp. 169 – 170.

[4] J. Preece, Y. Rogers, and H. Sharp, Interaction design: Beyond human computer interaction, 2nd ed., New York: John Wiley & Sons Inc., 2007.

[5] J. Bowen, How ATMs work. Available: http://money.howstuffworks .com/atm3.htm, 2010.

[6] M. Priestley, Practical object-oriented design with UML, 2nd ed., New York: McGraw-Hill Education, 2003.

[7] G. Andrew and P. Drew, "Use case diagrams in support of use case modelling: Deriving understanding from the picture," JDM, vol. 20(1), p. 124, 2009.

[8] I. Jacobson and N. Pan-Wei, Aspect-oriented software development with use cases. New York: Pearson Education, 2004.

[9] K. Bittner and I. Spence, Use case modelling. New York: Pearson Education, 2003.

[10] C. Raghavendra, S. Sivasubramanian, and A. M. Sameeullah, "High protection human iris authentication in new ATM terminal design using biometrics mechanism," JGRCS, vol. 3(11), 2012.

[11] N. A. K. Abiew, J. M. Dorgbefu, and S. O. Banning, "Design and implementation of cost effective multifactor authentication framework for ATM systems," AJRCOS, vol. 5(3), pp. 7 – 20, 2020.

[12] S. Mishra, A. Jain, S. Kumar, and A. Goyal, "Enhanced ATM security system using GSM, GPS and biometrics," IJETR, vol. 7(8), 2017.

[13] N. Ahmad, A. A. M. Rifen, and M. H. AbdWahab, "AES cardless automatic teller machine (ATM) biometric security system design using FPGA implementation," Proceedings of the International Engineering Research and Innovation Symposium (IRIS) on IOP Conf. Series: Materials Science and Engineering, vol. 160(2016), p. 012113, November 2016, Melaka, Malaysia. Bristol: IOP Publishing Ltd, 2017.

[14] S. Buvaneswari and V. V. Deepa, "An authentication of ATM system using DNA bar code," IJIRSET, vol. 4(8), 2015.

[15] O. M. Olaniyi, I. A. Ameh, L. A. Ajao, and O. R. Lawal, "Secure bio-cryptographic authentication system for cardless automated teller machines," JACET, vol. 5(2), 2019.

[16] V. Padmapriya and S. Prakasam, "Enhancing ATM security using fingerprint and GSM technology," IJCA, vol. 80(16), pp. 0975 – 8887, 2013.

[17] K. C. Okafor, C. C. Udeze, F. N. Ugwoke, I. Obinna, and N. Okwuelu, "AFIM: A high level conceptual ATM design using composite formal modelling with capture simulation pattern matching technique," IJSER, vol. 5(4), 2014.

A Distributed Denial of Service Attack Detection System using Long Short Term Memory with Singular Value Decomposition

Chukwuemeka Christian UGWU
Department of Computer Science
Federal University of Technology
Akure, Nigeria
ugwuemmy407@yahoo.com

Olumide Olayinka OBE
Department of Computer Science
Federal University of Technology
Akure, Nigeria
ooobe@futa.edu.ng

Olugbemiga Solomon POPOỌLA
Department of Computer Science
Ọsun State College of Education
Ila-Ọrangun, Nigeria
popsol7@yahoo.com

Adebayọ Olusọla ADETUNMBI
Department of Computer Science
Federal University of Technology
Akure, Nigeria
aoadetunmbi@futa.edu.ng

***Abstract*— The increase in online activity during the COVID 19 era has generated a surge in network traffics capable of expanding the scope of DDoS attacks. Cyber criminals can now afford to launch DDoS attacks massive enough to degrade the performances of conventional machine learning based IDS models. Hence, the need for an effective DDoS attack detective model with the capacity to handle such magnitude of DDoS attack traffics is required. This study proposes a deep learning based DDoS attack detection system using Long Short Term Memory (LSTM). The proposed model was evaluated on UNSW-NB15 and NSL-KDD intrusion datasets as Twenty-three (23) and Twenty (20) attack features were extracted from UNSW-NB15 and NSL-KDD respectively using Singular Value Decomposition (SVD). The result of proposed model shows significant improvement when compared with few convention conventional machine learning techniques such as Naïve Bayes (NB), Decision Tree (DT), and Support Vector Machine (SVM) with an accuracy of 94.28% and 90.59% on both datasets. Furthermore, comparative analysis of LSTM with other deep learning results reported in the existing literature showed the justification of choosing LSTM among its deep learning peers in detecting DDoS attacks over a network.**

Keywords*— Deep Learning, Distributed Denial of Service, LSTM, Machine learning, Naïve Bayes, SVD*

I. INTRODUCTION

The growing network infrastructure, and the enormous transition of critical information over the internet has incurred quite a number of challenges in making the internet a stable and secured system. There have been severe attacks that compromise the availability, confidentiality, and integrity of networks and its resources. Among these dominant threats on the internet is DDoS attacks. DDoS is a massive launch of network traffics at target systems or network resources via several compromised machines on the internet with the goal of denying access to such systems [1]. These machines are usually compromised with specialized malware, which prompts them to launch attacks at target systems or resources. The power of DDoS attack lies on both the massive number of attack sources, and the diversity of attacks. These two strengths make it difficult for traditional defense mechanisms such as firewalls, spam filtering and vendor specialized patches to defend against them. However, Intrusion Detection System (IDS) offers a more dynamic approach to combating DDoS attacks as it does not only detect successful intrusions, but also monitor attempts to break security that consumes system resources [2]. IDS uses two basic techniques to detect attacks on the network namely, Signature-based and Anomaly-based detection. The former maintains records of known attack patterns or signature which it uses to determine any misuse as occurring events or traffics are compared with these signatures. Signature-based methods are highly effective in identifying known attacks, but ineffective when it comes to detecting new or modified attack types. Anomaly-based detection on the other hand, is quite useful in detecting new attacks as the model keeps a profile of what is considered to be a normal traffic, and reports any deviance from this baseline to be a threat or attack [3]. However, anomaly-based methods are usually prone to high false positive rates.

Continuous research and study on ways to improve the detection of DDoS attacks and other intrusions, has prompted the use of machine learning (ML) algorithms as an alternative to handling the analysis of traffic data. The technique automatically learns or extract relevant patterns from existing network data as a reference for normal or irregular traffic behaviour profile for subsequent classification of network traffic [4]. This practice improves the predictive capability ML algorithms. Among the successfully applied ML model for detection of DDoS attack include DT, SVM, NB and more. However, the increase in online activity during the COVID-19 lockdown era has generated a surge in network traffics capable of expanding the scope of DDoS attacks that can degrade the performance of most conventional ML algorithms.

Hence, Deep learning (DL) comes as viable solution in handling large amount of network traffics, particularly where likely patterns in the data are unknown [5]. DL is a subdivision of machine known for its ability in extracting high-level data representations with little or no feature

engineering for better decision making [6]. DL has many benefit in the cybersecurity space such as effective prediction of known and novel attacks while mitigating the problem of low false positive rate. A commonly used deep learning technique in this research domain is the Recurrent Neural Network (RNN). Similarly to every neural network, RNN consist of input units, hidden layers, and the output layers, but the mode at which information travel through its layers differs [7]. Several RNN architectures have been proposed in recent times in an attempt to rectify some obvious limitations found in previous architectures [8]. One of the important achievements in RNN is the Long Short Term Memory (LSTM), a variant of RNN capable of solving vanishing gradient problems (that is the gradient value tending to zero during backward propagation) which arises as a result of long input sequence. Therefore, this paper proposes to detect DDoS attacks over a network using LSTM with the aim to improve accuracy, detection rate and reduce low false positive rate.

The remaining part of this paper is organized as follows: Section II presents the review of related works. Section III provides the proposed system architecture, the mathematical model, the description of datasets used, and performance evaluation metrics used in this study. The Experimental Setup is provided in Section IV, Section V presents the results and evaluation of the models. Section VI presents the conclusion.

II. RELATED WORKS

Extensive researches have been carried out on ways to defend against DDoS attacks, detailed reviews of some of these works are presented as follows:

In [9], a framework capable detecting of various DoS and DDoS attacks using RNN ensemble was proposed, but it was neither implemented nor evaluated. The authors in [10] employed Associative rule method to extract DoS attack patterns as ruleset for the detection of DoS attacks in incoming traffics. However, the proposed model requires lot of rules to capture the massive amount of attack variants in currently existing, while new rules must be created for new attacks. In [11], Principal Component Analysis (PCA) with Random Forest (RF) Classifier were applied in detecting DDoS attacks. PCA was used as reduction dimension technique to reduce the size of the original attributes from 41 attributes to 14 attributes, while RF was applied to distinguish normal traffics from DDoS attack traffics. The proposed model was quite effective, but key attack components such as Tcp and Icmp protocol attacks were not considered during attack detection. Whereas, authors in [12] applied different machine learning models (Multilayer Perceptron, Naïve Bayes and Random Forest) in an attempt to attain very high detection rate as well as detect all variant of DDoS attacks, but failed to detect flood DDoS attack types. The motivation of authors in [13] was detect and mitigate the occurrence of DDoS attacks on the Client side using SVM. The objective was to identify relevant attack feature and fed the selected features to support vector machine algorithm to effectively classify DDoS attacks. However, the features were arbitrarily selected as no feature selection or extraction techniques was mentioned to be used, nor was the process upon which features were picked was stated. RNN was employed as a classification model in [6] in developing an improved IDS. The methodology involved network data collection (live or offline dataset), data pre-processing, and classification. The model was implemented on python deep learning framework called Theano and the evaluation of the developed model was performed on NSL-KDD dataset. It was reported that the model performed relatively well in improving both the accuracy of intrusion detection for both binary and multi classification. A Restricted Boltzmann Machine -intrusion detection system (RBM-IDS) was proposed in [14]. The proposed model was evaluated on the NSL-KDD data set. However, the performance of RBM-IDS was not satisfactory with 73.23% accuracy and 62.33% detection rate. A Holistic Approach for Detecting DDoS attacks using Ensemble Unsupervised Machine Learning by [15] shows the practicality of combining both supervised and unsupervised models in detecting DDOS attacks. However, adopting five (5) unsupervised classifiers as base model and three (3) meta-classifier as combiners take up lot of memory space and resources. In [16], Network Intrusion Detection System using Supervised Learning Paradigm was presented. The data used was discretized using binarization method before selection of relevant feature by information gain and intrusion attack detection using ANN. However, the proposed model performance was relatively low which could be to the lost relevant information during binarization.

With the findings from the reviews conducted, low detection rate, inappropriate selection of relevant attack features, high positive rates, and inability to capture all attack types remain an issue to be resolved. Hence, this study will employ two modern intrusion datasets with variants DDoS attack vectors in a bid to capture all attack types, SVD will be applied to effectively extract key attack features form the datasets, and LSTM will learn the patterns of each extracted feature vectors for effective detection. Unlike other previous models used, LSTM has the capability of handling large data without performance degradation or gradient vanishing issues.

III. METHODOLOGY

The proposed system is basically partitioned into training and prediction stage. The training stage involved feeding offline labeled network data (NSL-KDD and UNSW-NB15) to train the proposed DDoS attack predictive model as the network data undergoes data preprocessing by way of feature conversion and data normalization. The feature conversion involved converting non-numeric feature values to numeric values, while normalization involved scaling network feature values into comparable value range using min-max normalization method. Thereafter, SVD was applied on the normalized data to extract significant network features. The reduced network features were fed into LSTM to learn the definition of both Normal and DDoS attack patterns from the dataset for detection of known and unknown DDoS attacks which takes place at the prediction stage. Finally, the proposed system is evaluated to determine its efficiency. The conceptual diagram of the system is presented in Figure 1.

A. MATHEMATICAL MODEL

Given that the training set of a network intrusion dataset is expressed as follows:

$$T = \{S_i, C_j\}; \forall S_i \exists\, f: f = \{1,2,3, \dots, x\} \quad (1)$$

where T represents the training set containing set of network traffics $S_i, i = 1,2,3, \dots, n$ with an assigned class label $C_j, j = 1,2,3, \dots, m$, and f represents set of feature in S_i. Arbitrary Assignment method is applied on T as non-numeric feature values $v_1, v_2, v_3, \dots \dots v_q$ of a feature category f_i were

converted into numeric sequential integer values $k, k+1, k+2, \ldots . k+q$. After numeric conversion, normalization using Min-Max method presented in equation (2) was applied on the data.

$$v' = \frac{(v)-(min_f)}{(max_f)-(min_f)} \quad (2)$$

where v' represents the new value, v denotes the observed value (that is, the value to be normalized), max_f and min_f are maximum and minimum values of feature f respectively. Thereafter, features from the normalized data were reduced using SVD feature reduction technique as follows: SVD is given as:

$$X_{(n*x)} = U\sum V^T \quad (3)$$

where $X_{(n*x)}$ represents a data matrix formed from S with n number of network instances as rows and x number of network feature. U and V are orthogonal eigenvectors of the matrix XX^T and X^TX respectively, such that the columns of U are the left singular vector of X, and the columns of V are the right singular vector of X. $\sum$ represents the diagonal matrix of the singular values σ_i presented in equation (4)

$$\sigma_i = \sqrt{\lambda_i} \quad (4)$$

λ_i is the eigenvalue of X^TX or XX^T using the formula presented in equation (5)

$$(W - I\lambda_i)v_i = 0 : i = 1,2,3, \ldots, z \quad (5)$$

where W represents either X^TX or XX^T, and v_i represents the eigenvector corresponding to λ_i. Thereafter, σ_i is

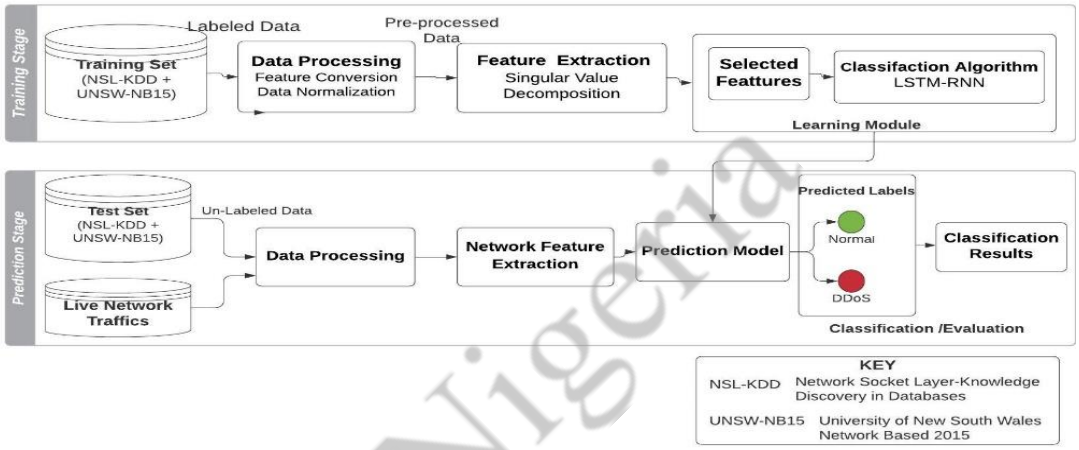


Figure 1: Architecture of the proposed model

arranged diagonally in $\sum$ and sorted in decreasing order such that $\sigma_i \geq \sigma_i \geq \cdots \geq \sigma_{\min(n,x)} \geq 0$. However, to obtain a reduced feature set, a rank constraint k is applied on SVD such that singular vectors U_k, V_k^T, and a cumulative singular value satisfies a particular threshold value using equation (6)

$$\frac{\sum_{i=1}^{k} \sigma_i}{\sum_{i=1}^{n} \sigma_i} \geq threshold \quad (6)$$

where $(k < n)$ as n represents the total number of singular values in Σ and k represents the number of truncated singular values.

The reduced feature subset is used to train LSTM classification algorithm in order to classify DDoS attacks. The structure of LSTM cell is depicted in figure 2. In training LSTM, network traffic data were represented as vectors, and each sequence vector v were passed to the LSTM cells with gated layers (I, f, and o) to produce classification output $\hat{c}$ using the following equations:

$$a_t = \tanh(W_a .v_t + U_a.h_{t-1} + b_a) \quad (7)$$
$$i_t = \sigma(W_i.v_t + U_i.h_{t-1} + b_i) \quad (8)$$
$$f_t = \sigma(W_f.v_t + U_f.h_{t-1} + b_f) \quad (9)$$
$$o_t = \sigma(W_o.v_t + U_o.h_{t-1} + b_o) \quad (10)$$
$$s_t = (a_t \odot i_t + f_t \odot s_{t-1}) \quad (11)$$
$$h_t = \tanh(s_t) \odot o_t \quad (12)$$
$$\hat{c} = h_t \quad (13)$$

where v_t is an input at time t. I, f, and o are input, forget, and output gate respectively,. f discards irrelevant from the cell, I updates the cell with new information, while o decides which information to be outputted. W and U represents the weight of the input and recurrent connections, b represents bias, h_t represents the output vector of the LSTM unit which referred to as $\hat{c}$. a_t represents the intermediate cell state, $\odot$ represents the element-wise product called Hadamard product, s_t represents the new state, and s_{t-1} represents the previous state. The non- linear functions σ and tanh represent sigmoid and tangent hyperbolic function which are given as:

$$\sigma(v_t) = \frac{1}{1+e^{-v_t}} \quad (14)$$
$$\tanh(v_t) = \frac{e^{2v_t}-1}{e^{2v_t}+1} \quad (15)$$

However, training LSTM-RNN requires adjusting W, U, and b to minimize the loss function in equation (16) across the training data.

$$E(c, \hat{c}) = \frac{(c-\hat{c})^2}{2} \quad (16)$$

where $E(c, \hat{c})$ represents the mean square error. The gradient of the error with respect to parameters $\theta_i, \theta = (W, U, b)$ is computed using chain rule differentiation formula presented as follows:

$$\delta_i = dE/d\theta_i \quad (17)$$

Thereafter, θ is updated in the direction via the gradient that helps minimize the loss.

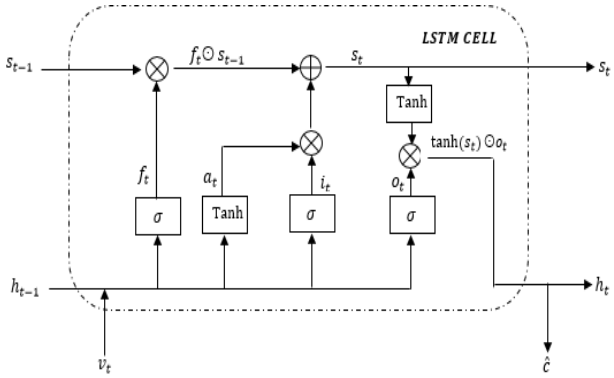


Figure 2: Structure of LSTM Cell

B. DESCRIPTION OF NETWORK DATASETS

a. UNSW-NB15 Dataset

UNSW-NB15 dataset was created in Cyber Range Lab of the Australian Center for Cyber Security (ACCS) using IXIA Perfect Storm tool to extract a mix of modern normal activities and attack patterns of network traffics. TCP dump tool was employed to capture over 100GB of raw traffics. Argus and BroIDS tools combined with Twelve (12) other models were used to extract 49 features from the captured network traffics which formed the instances of UNSW-NB15 dataset [17]. The 49 features were categorized into six groups namely: flow features, basic features, content features, time features, and addition generated features. UNSW-NB15 contains a total of 2,540,044 instances with assigned class label from Ten (10) class categories namely; Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms, and Normal. These instances were distributed into Four (4) different CSV files. However, the CSV downloaded for this study contains 82,332 training and 175,341 test records respectively. Table I shows the class distribution of UNSW-NB15

Table I. UNSW-15 Class Distribution

Class Label	Training	Testing
Normal	37000	56000
Generic	18871	40000
Exploits	11132	33393
Fuzzers	6062	18184
DoS	4089	12264
Reconnaissance	3496	10491
Analysis	677	2000
Backdoor	583	1746
Shellcode	378	1133
Worms	44	130
Total	82332	175341

b. NSL-KDD Dataset

NSL-KDD Dataset is an improved version of KDD'99 dataset [18]. It is considered a suitable replacement of KDD'99 due to its less duplicate and redundant network samples. In addition, experiments could be run on the complete network dataset without the need to randomly select a small portion as practiced in KDD'99 [19]. The full training set consist of 125,973 connection records, while the testing set contains 22,544 records. Each network sample is described by 41 attributes with an assigned class label as either normal or as an attack type. Like the KDD'99, NSL-KDD attack types were grouped into four categories namely DoS, Probe, R2L, and U2R. Table II shows the class distribution of NSL-KDD dataset.

Table II. NSL-KDD Class Distribution

Class Label	Training	Testing
Normal	67343	9710
DoS	45927	7459
Probe	11656	2421
R2L	995	2885
U2R	52	67
Total	125973	22542

C. IDENTIFICATION OF RELEVANT FEATURES

Identifying relevant network features for DDoS attack detection using SVD involved retaining the needed number of singular components (SCs) also known as new features. These new features were determined by Cumulative Percentage Variance (equation 6) as we set the variability threshold value to 95%. Having done that, we retained 23 and 20 new features from UNSWNB15 and NSL-KDD dataset respectively. The plot in Figure 3 and 4 present the percentage variance in selecting new features in UNSW-NB15 and NSL-KDD respectively.

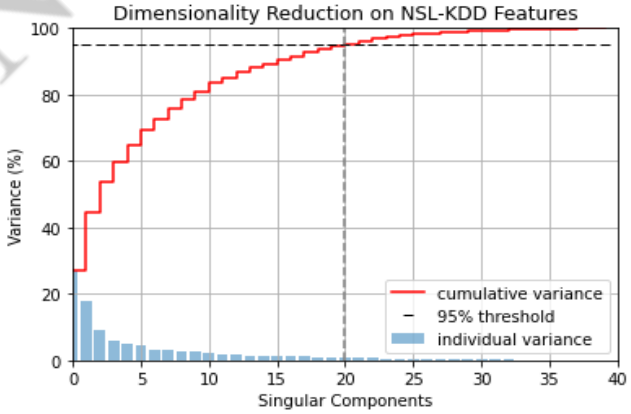


Figure 3: Scree plot of UNSW-NB15 SCs

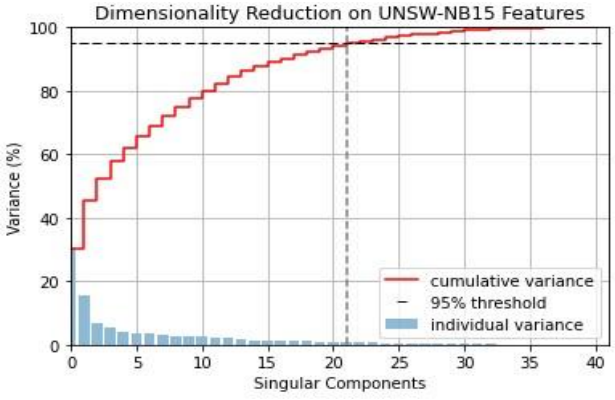


Figure 4: Scree plot of NSL-KDD SCs

D. EVALUATION METRICS

To estimate the percentage in which the proposed DDoS attack detection model correctly distinguish DDoS attack traffic from normal network traffics, we employed Accuracy (ACC), Detection Rate (DR), Recall, F1-Measure, and False Alarm Rate (FAR). The mathematical representations is given as:

$$\text{ACC} = \frac{TP+TN}{TP+TN\ FN+\ FP} * 100 \quad (18)$$

$$\text{DR} = \frac{TP}{TP+\ FP} * 100 \quad (19)$$

$$\text{F1} = 2 * \frac{Detection\ Rate * Recall}{Detection\ Rate + Recall} * 100 \quad (20)$$

$$\text{FAR} = \frac{FP}{TN+FP} * 100 \quad (21)$$

$$\text{Recall} = \frac{TP}{TP+FN} * 100 \quad (22)$$

where TP represents the number of DDoS attacks that was rightly predicted by the model as an attack, FP provides the figure of DDoS attack instances that were wrongly predicted to be normal, TN presents the amount of normal traffics that are correctly predicted to be normal, and FN represents the amount of normal traffics that are wrongly predicted to be DDoS attack traffics.

IV. EXPERIMENTAL SETUP

All the models in this study were experimented using a personal computer system with 2.3 GHz Intel (R) Core (TM) i5 4200U CPU @ 1.60 GHz 2.30 GHz and 8 GB of RAM. The codes were implemented with Python 3.7.6 programming language with scikit-learn library for data preprocessing and Keras framework for our LSTM model.

The records of instances used for the experiment constituted instances with DDoS and Normal labels only, as other attack types were expunged from the datasets. This is to ensure that the model effectively learn and predict DDoS attack traffics from normal traffics. Table III presents the distribution of network instances after expunging other attack types. However, grid search algorithm was used to loop through some of the hyper-parameters as we specify some search range (shown in Table IV), thereafter the best hyper-parameter set (Learning rate = 0.001, Batch Size = 200, Number of LSTM Layers = 4, Epoch = 20, and Adam optimization method) were applied in training the LSTM model.

Table III Records of DDoS Attack Datasets

Class Label	UNSW-NB15 DDoS		NSL-KDD DDoS	
	Training	*Testing*	*Training*	*Testing*
Normal	37000	56000	67343	9710
DDoS	4089	12264	45927	7459
Total	41089	68264	113270	17169

Table IV. Hyper-parameters and Ranges for DDoS Attack Classification

Hyper-parameters	Ranges
Learning Rate	0.1, 0.01, 0.001, 0.0001
LSTM Layers	2, 4, 6, 8, 10
Epoch	20, 40, 60,80,100
Batch Size	100, 200, 300,400, 500
Optimizer	'Adam', 'RMSprop', 'SGD'

V. RESULTS AND EVALUATIONS

This subsection provides the experimental results of this study. The section explains the performances of all the models used in terms of their accuracy, Detection rate, Recall, F1-measure, and False alarm rate.

a. LSTM Result

In our experiment, we obtained the performances of LSTM with SVD reduced feature set and LSTM with the original feature set. This was carried out to show the impact of feature reduction on the performance of the developed model. Table V and Table VI provide the confusion matrix and evaluation of their performances respectively.

Table V: Confusion Matrix of LSTM

Models	Dataset	TN	FP	FN	TP
LSTM + SVD	UNSW-NB15	54505	1495	2408	9856
	NSL-KDD	9429	281	1334	6125
LSTM Only	UNSW-NB15	52893	3107	7353	4911
	NSL-KDD	9630	80	2216	5243

Table VI. Performance of LSTM

Models	Datasets	DR	Recall	F1	ACC
LSTM + SVD	UNSW-NB15	86.83	80.37	83.47	94.28
	NSL-KDD	95.61	82.12	88.35	90.59
LSTM Only	UNSW-NB15	61.25	40.04	48.44	84.68
	NSL-KDD	98.49	70.29	82.04	86.62

Table V shows that LSTM + SVD correctly classified 64361 and 15554 instances of UNSW-NB15 and NSL-KDD respectively as compared to the correctly classified 57714 and 14873 instances obtained by LSTM without SVD.

The DR, FAR, Recall, F1, and ACC in Table VI shows the performances of LSTM+SVD and LSTM without SVD. In this study, LSTM+SVD recorded a superior performance over LSTM without SVD with ACC of 94.28% and 90.59%, recall of 80.37% and 82.12%, F1-score of 83.47% and 88.35% on both UNSW-NB15 and NSL-KDD dataset, except for DR on NSL_KDD with 98.49%.

b. Comparison of LSTM with Conventional Machine Learning Methods

Having realized that LSTM had performed better with SVD, we thereby compared its performance with selected conventional machine learning methods such as SVM, DT, and NB on the same reduced set. Scikit-learn was used in implementing the machine learning algorithms. Table VII and Table VIII shows the confusion matrix and evaluation results of these comparison.

Table VII. Confusion Matrix of Models

Models	Dataset	TN	FP	FN	TP
NB+SVD	UNSW-NB15	53355	2645	6678	558
	NSL-KDD	9607	103	2574	4885
SVM+SVD	UNSW-NB15	33503	22497	3386	8878
	NSL-KDD	8219	1491	1415	6044
DT+SVD	UNSW-NB15	52908	3092	2315	9949
	NSL-KDD	9342	368	1791	5668
LSTM+SVD	UNSW-NB15	54505	1495	2408	9856
	NSL-KDD	9429	281	1334	6125

Table VIII. Performance of Models

Models	Dataset	ACC	DR	Recall	F1
NB+SVD	UNSW-NB15	86.31	78.40	70.41	73.24
	NSL-KDD	84.43	88.42	82.20	83.11
SVM+SVD	UNSW-NB15	62.08	28.29	72.39	40.69
	NSL-KDD	83.07	80.21	81.03	80.60
DT+SVD	UNSW-NB15	92.08	76.29	81.12	78.63
	NSL-KDD	87.43	93.90	75.99	84.00
LSTM+SVD	UNSW-NB15	94.28	86.83	80.37	83.47
	NSL-KDD	90.59	95.61	82.12	88.35

The study in Table VIII shows LSTM had performed better on both datasets (UNSW-NB15 and NSL-KDD) in terms of ACC, DR, and F1-measure.

On UNSW-NB15, LSTM recorded 94.28% (accuracy), followed by DT's 86.83%, NB's 86.31%, and SVM's 62.08%. LSTM also performed best using detection rate with 86.83%, followed by NB's 78.40%, DT's 76.29%, and SVM very poor record of 28.29%. However, DT record on recall rate (81.12%) was slightly better than LSTM's 80.37%, followed by SVM's 72.39% and NB's 70.41%. In the f1-measure, LSTM recorded best with 83.47%, DT's (78.63%), NB's (73.24%), and SVM's (40.69%).

On NSL-KDD, LSTM recorded 90.59% (accuracy), followed by Decision tree's 87.43%, Naive Bayes' 84.43%, and SVM's 83.07%. LSTM recorded 95.61% (detection rate), followed by DT's 93.90%, NB's 88.42% and SVM's 80.21%. However, NB record on recall rate (82.20%) was slightly better than LSTM's 82.12%, followed by SVM's 81.03% and DT's 75.99%. In the f1-measure, LSTM's recorded 88.35%, DT's (84.00%), NB (83.11%), and SVM's (80.60%). Figure 5 and Figure 6 show the graphical representations of the model's evaluation on UNSW-NB15 and NSL-KDD dataset respectively.

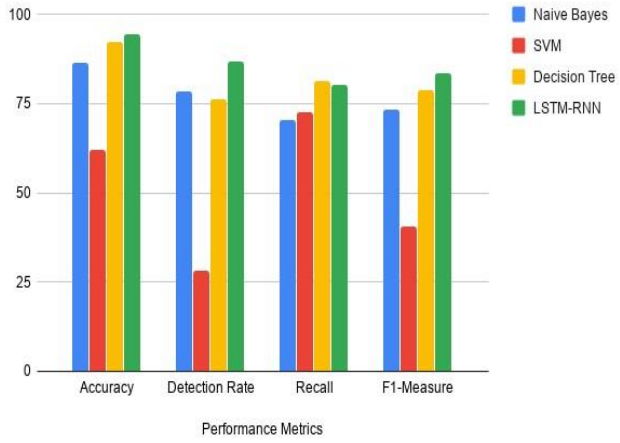


Figure 5: Performance of Models on UNSW-NB15

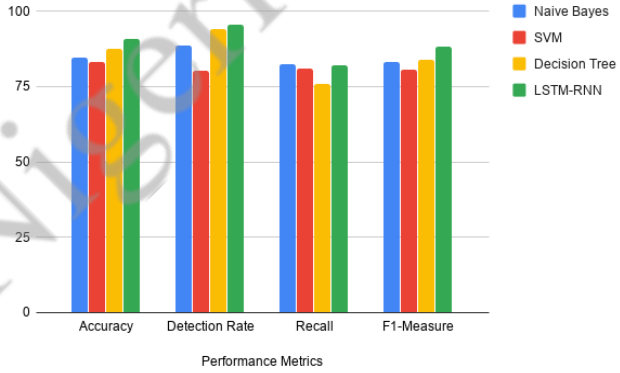


Figure 6: Performance of Models on NSL-KDD

A. Comparison of LSTM-RNN IDS with existing deep learning IDS using Detection Rate and Accuracy

Table 9 shows the comparison of the proposed model with some existing deep learning IDS when validated with NSLKDD Dataset. From the Table, the proposed model performed better than the enlisted models in terms with 90.59% (ACC) and 95.61% (DR).

Table 9: Proposed Model with existing deep learning IDS

Author and Year	Dataset Used	Technique Used	ACC	DR
Yin et al.,(2017)	NSL-KDD	Elman RNN	—	83.49
Imamverdiyer and Abdullayeva (2018)	NSL-KDD	RBM	73.23	62.33
Proposed Model (2020)	NSL-KDD	LSTM-RNN	90.59	95.61

VI. CONCLUSION

In this study, a DDoS attack detection system using LSTM with SVD was developed with the ultimate goal of addressing the objectives stated in this work. In addressing these objectives, UNSW-NB15 and NSL-KDD Datasets were used as benchmark datasets as they contain modern attack patterns as well as less redundant features suitable for present DDoS attack detection. The training and test set of these datasets were preprocessed using the arbitrary feature conversion method to convert non-numeric features to numeric features and Min-max method to scale the datasets into comparable size. Relevant DDoS attack features were determined by Singular Value Decomposition (dimensionality reduction) technique in order to achieve optimal performance. The reduced features were used in training and testing LSTM classifier to identify the DDoS attack connection. LSTM DDoS Detection model was evaluated and compared with Na¨ıve Bayes, Decision tree, and SVM on both datasets. The result shows that LSTM performed better on both UNSW-NB15 and NSL-KDD dataset with an Accuracy of 94.28% and 90.59% respectively.

REFERENCES

[1] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita. Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions. The Computer Journal, Oxfordjournals, vol 57(4), pp. 537–556, 2014.

[2] S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas. Modeling intrusion detection system using Intelligent Systems. Journal of network and computer applications, vol 30(1), pp. 114-132, 2007

[3] B. F. Gong. Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection. Santa Clara, Calif Network Associates, Inc. pp.1-10. Retrieved 8 March 2018 from http://www.networkassociates.com

[4] A. O. Adetunmbi, A. S. Oladele, and D. O. Abosede. Analysis of KDD'99 Intrusion detection dataset for selection of relevance features. In Proceedings of the World Congress on Engineering and Computer Science, vol 1, pp. 20-22, 2010.

[5] R. Vargas, A. Mosavi, and L. Ruiz. Deep Learning: A Review. Advances in Intelligent Systems and Computing vol 5(2): pp. 1-8, 2017.

[6] C. Yin, Y. Zhu, J. Fei, and X. He. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE, vol 5, pp. 21954–21961, 2017

[7] T. I. Poznyak, O. I. Chairez, and A. S. Poznyak. Background on dynamic neural networks. Ozonation and Biodegradation in Environmental Engineering, pp. 57–74, 2019.

[8] T. Katte. Recurrent Network and its various Architecture Types. International Journal of Research and Scientific Innovation vol 5(3): pp.1-6, 2019.

[9] A. B. M. A. A. Islam, and T. Sabrina. Detection of various denial of service and Distributed Denial of Service attacks using RNN Ensemble. 12th International Conference on Computers and Information Technology, pp. 603-608, 2009.

[10] O. O. Olashinde. Design and implementation of denial of service (Dos) detection system using Association rule. Thesis, Department of Computer Science, The Federal University of Technology, Akure, Nigeria, 2012

[11] S. Revathi, and A. Malathi. Detecting Denial of Service Attack Using Principal Component Analysis with Random Forest Classifier. International Journal of Computer Science & Engineering Technology (IJCSET). Vol 5(3), pp. 248-252, 2014

[12] M. Alkasassbeh, B.A. Hassanat, G. Al-Naymat, and M. Almseidin. "Detecting Distributed Denial of Service Attacks Using Data Mining", International Journal of Advanced Computer Science and Applications (IJACSA). Vol 7(1), pp. 436-445, 2016

[13] D. Kim, and Y. L. Li. Detection of DDoS Attack on the Client Side Using Support Vector Machine. International Journal of Applied Engineering Research IJARE, vol 12(20), pp. 9909-9913, 2017

[14] Y. Imamverdiyev, and F. Abdullayeva. Deep learning method for denial of service attack detection based on restricted boltzmann machine. Big Data, vol 6(2), pp. 159-169, 2018.

[15] S. Das, D. Venugopal, S. Shiva. A Holistic Approach for Detecting DDoS Attacks by Using Ensemble Unsupervised Machine Learning. In: Advances in Information and Communication Conference. Advances in Intelligent Systems and Computing. Springer, Cham. vol 1130, pp. 721-738, 2020

[16] J. M. Olamantanmi, O. D. Alowolodu, J. O. Mebawondu, and A. O. Adetunmbi. Network Intrusion Detection System using Supervised Learning Paradigm. Scientific African. Pp. 1-10, 2020

[17] N. Moustafa, and J. Slay.UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS), pp. 1-6, 2015

[18] M. Tavallaee, E. Bagheri, W. Lu, and , A. A. Ghorbani. A Detailed Analysis of the KDD CUP 99 Data Set. IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009

[19] A. Ozgur, and H. Erdem. A Review of KDD99 Dataset usage in ¨ Intrusion Detection and Machine Learning between 2010 and 2015, PeerJ Preprints , pp.1-21, 2016

Critical Requirements for Sustainable Deployment of IoT Systems in Nigeria

Gloria A. Chukwudebe
Dept. of Electrical and Electronic Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
gloria.chukwudebe@futo.edu.ng

Reginald Ekene Ogu
Dept. of Software Engineering
Federal University of Technology, Owerri
Owerri, Nigeria
reginald.ogu@futo.edu.ng

Jenny Ebitonere Fawei
Dept. of Electrical and Electronic Engineering
Niger Delta University
Bayelsa, Nigeria
jeoebicom@gmail.com

***Abstract*— The Internet of Things is finding innovative and interesting applications. Currently, it is being applied in transportation, healthcare delivery, agriculture, security surveillance and smart manufacturing. It has resulted to the development of smart cities, manufacturing, grid etc. When deployed, IoT nodes may collect sensitive personal information or become surface for cyberattacks, hence suitable policies and regulations need to be enacted at the global and national levels to ensure benefit realization and safe use. This paper reviewed already established IoT standards and best practices by notable organizations such as the Body of European Regulators for Electronic Communications, the GSM Association, the Institute of Electrical and Electronic Engineers, International Telecommunication Union, International Standards Organization, European Telecommunication Standards Institute etc. The regulation of IoT applications and systems is more challenging than existing ICT because of the complexity of numerous interactions involved in the Internet of Things ecosystem. The IoT regulatory efforts so far in USA, India and European Union were examined although standardization efforts are still ongoing. From the study, the critical requirements for a sustainable deployment of IoT systems; government support, appropriate spectrum allocation, connectivity, adaptability, security, privacy and trust were identified. Also, a robust IoT Policy and Regulatory framework for Nigeria was proposed and a multi-sectoral collaboration was recommended for full development and implementation of the proposed framework.**

***Keywords*— Connectivity, Data Privacy, IoT Policy, IoT regulations, Security, Trust**

I. INTRODUCTION

The Internet of Things (IoT) is a phrase formed by Kevin Ashton over two years ago that has affected electrotechnology and computing [1]–[3]. The "Internet of Things" technology has come at a time when ubiquitous computing is no longer a challenge. This is evident as the focus of the Internet and related technologies have metamorphosed to the connection of human beings and objects, to merge the real world with man-made artificial environments. Today, the IoT ecosystem consists of intelligent devices, people, and other objects that are informed of their context to telecommunicate with everything else, anytime and anywhere [4]. This implies that objects are required to be accessible unrestricted [1], [5], [6]. Hence the term: Internet of Everything (IoE). CISCO through the Lopez Research in [2], highlighted that people, places, objects and things constitute the Internet of Everything. From the description above, anything that exists can be equipped with a sensor (or actuator) and network access mechanism to participate in the IoT ecosystems.

This work is sponsored by the Nigerian Communications Commission

Through the three Cs: "Communication", "Control and Automation" and "Cost Savings", IoT is affecting the quality of life and businesses, as foresaw by CISCO in [2]. For instance, it is affecting healthcare delivery by expanding the communication path between objects by offering a more amalgamated communication setting where various sensor data such as location, blood pressure, heartbeat, etc. can be measured and tele-communicated between patients and doctors easily. In addition, IoT is helpful in automation and control process, whereby operators can effectively manage the status of objects via remote control panels. Through remote monitoring, IoT has proved to be cost-efficient in implementation, deployment, and maintenance processes [1].

As of 2018, the IoT segment of Nigeria's technological sector was underperforming relative to other markets in Africa like Kenya, South Africa, Egypt etc. However, it has been stated that Nigeria is ready for massive deployment of IoT devices following the penetration of Narrow Band communication network giants like Sigfox, through IoT Africa [7]. Today, there are functional IoT devices in Nigeria like Fasmicro's Zenvus and Obuno IoT Engine [8]. Globally, various organizations are developing IoT regulations and policies especially for the developed countries. As it relates to African countries, the AU Convention on Cyber Security and Personal Data Protection is inadequate for judicial and international cooperation amongst African States [11].

In view of the above and since connectivity, interoperability, and integration are the core aspects of the IoT ecosystem [1]; policy regulations to guide on how IoT systems can be implemented and managed to ensure reliable connection, safe use, social and economic benefits are needed if IoT must grow in Nigeria [5], [13], [14], [8] & [12].

The relevance of policy and regulation guidelines cannot be overstated. Without adequate regulation, there could be a scenario where inefficient, insecure, or defective IoT devices are deployed on networks. In such a case, the mobile network operator is faced with challenges because such devices can cause turbulence in the network. The above scenario can result to network disruption thereby affecting all users of the network [16].

In Section II of this paper, a brief review of IoT applications, the enabling technologies and the stakeholders in the IoT ecosystem is presented. In Section III, existing IoT Standards, the IoT regulatory efforts in USA, India and European Union are examined. The key advice agreed by the Body of European Regulators for Electronic Communications and GSM Association were highlighted. Section IV presents the study of the critical requirements for sustainable

deployment of IoT Systems in Nigeria. The essential functions of various government ministries, agencies and educational institutions, the roles of the key technical requirements: spectrum, connectivity, adaptability, security and privacy for safe deployment of IoT systems are discussed. In view of the complex nature of the IoT ecosystem and the possible great number of interactions amongst the 'things/objects', a robust Policy and Regulatory Framework for IoT deployment is proposed. The paper is concluded in Section V. Section VI recommends development of the proposed Policy and Regulatory Framework using already established standards and best practices according to the needs of the country.

II. IoT Applications and Ecosystem

IoT is a network of connected devices and technologies designed towards a specific goal, such as the creation of a smart city, an office surveillance system etc. IoT devices collect data and send it across the network to a platform that aggregates the data for future use by the designated stakeholders. Essentially, most IoT systems comprise of machines, sensors/actuators, data processing software, cloud facility, communication infrastructure, Internet bandwidth, and oftentimes Artificial Intelligence as shown in the Fig 1.

Presently, the IoT application areas include but not limited to agriculture, aviation, road transportation, infrastructure management, security systems, energy management, environmental monitoring, and healthcare systems. The application of IoT in the developed countries of the world has given rise to Smart Grids, Smart Cities and Smart farming to mention but a few. The IoT ecosystem is composed of People, Processes, Technology & Knowledge. The stakeholders of IoT technology include:

- Users/Customers
- Platform Providers
- Network Providers
- Device Manufacturers
- Tertiary and Research Institutions
- Standardisation Organisations and Policy makers

A. Enabling Technologies

Technologies like the traditional ethernet, embedded systems, Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), Cloud Computing and telecommunication Transmission technologies have enabled the emergence of the Internet of Things applications and systems.

The telecommunication network is the channel through which the devices 'talk' to one another and communicate with/receive commands from the server/cloud. The telecommunication networks and spectrum usage have over the years been under regulation because of the numerous applications and diverse requirements. From the studies so far, the spectrum used in IoT can be dedicated (licensed) or shared (unlicensed), each has its own benefits and disadvantages. National Mobile Network providers (LTE, GSM) use dedicated spectrum for wide area IoT applications. While, some new service providers such as LoRa use license-free sub-gigahertz RF bands in Europe (433 MHz and 868 MHz). LoRa allows long-range transmissions (>10 km in rural areas) with low energy usage.

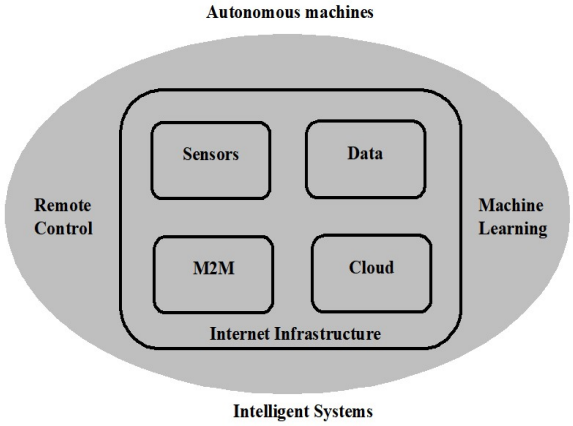


Fig. 1. IoT System Components.

III. Existing IoT Standards and Policy Regulations

Regulating IoT is different from the normal telecommunications and ICT because of the numerous interactions amongst applications, related devices, and sensors. Some of the challenges with IoT applications are Privacy and security. These challenges arise because in an IoT environment, data is collected and shared automatically by devices, and some may be critical in nature. Other challenges include how to switch the IoT nodes in times of changing operators, and the adequacy of IP addresses since some organizations are still on IPv4 to IPv6 transition.

Some public and proprietary standards have been developed to address issues such as interoperability amongst entities in the IoT ecosystem. This required cross-sectoral collaboration since IoT system are deployed in multiple sectors. The Standards development for IoT interoperability is still ongoing [17]. Notable organizations involved in IoT standardization include: International Telecommunication Union (ITU), the European Telecommunication Standards Institute (ETSI), the American National Standards Institute (ANSI), the Telecommunications Industry Association (TIA), the International Standards Organization (ISO) and the International Engineering Consortium (IEC). Others are the World Wide Web Consortium (W3C), the Institute of Electrical and Electronic Engineers (IEEE), the Industrial Internet Consortium (IIC) and the Internet Engineering Task Force (IETF). The focus areas for these organizations are highlighted as follows.

- ETSI is focused on the development of an Application-independent M2M horizontal service platform.
- P2413, a Standard for an Architectural Framework for IoT was developed by IEEE.
- Development of IoT related standards and application on Smart Cities are being worked on by ITU-T.
- The IETF has focused on Authentication and Authorization for Constrained Environments and IPv6 over Low power WPAN (6lowpan).
- The Web of Things, "standards for identification, discovery and interoperation of services across platforms" is being worked on by W3C.

Though, establishment of standards come before regulation, some countries are not waiting for all the standards to be developed and published, they have rolled out policies and regulatory guidelines for IoT so that they will not miss out from the huge benefits postulated for IoT systems and its role in Industry 4.0. Some of the regulatory efforts are presented in the following section.

A. National and Regional IoT Regulatory Efforts

In USA, the National Institute for Standards and Technology (NIST), released a draft Framework for Cyber-Physical Systems in 2014. The Framework serves as a guide for the development of quality systems, like IoT devices.

In India, an IoT Policy framework was proposed to be implemented through a five pillars approach. The pillars are Demonstration Centres, Capacity Building & Incubation, R&D and Innovation, Incentives and Engagements, and Human Resource Development [18].

BEREC has laid down some guidelines for IoT implementation and management in European countries. Equally, the GSM Association (GSMA) has been trying to harmonize IoT guidelines from many sources. The GSMA has responded to BEREC regulations and agreed to conform to three key topics listed as follows:

1) Necessity for relevant unbiased policies.

BEREC stated that to realize the potentials and enjoy full benefits of IoT, governments must enact relevant, flexible and technology unbiased regulations and policies. In reaction, GSMA is concurring and reaffirming the above statement for not only Europe but the global community. According to GSMA, the reason for adopting this statement is because excessive or biased policies can thwart the development of IoT systems.

2) Global Implementation Models.

The GSMA advocates that all stakeholders involved in IoT systems (design, manufacturing, deployment, regulation etc) should have the freedom to select a suitable model. The freedom to select a model of choice will ensure that high quality IoT systems are rapidly developed and economically deployed. By this statement, no party should be forced to adopt a model if the best is to be gotten from IoT technology. However, the choice of model should depend on requirements of the mobile network operator, the IoT service provider and the consumer, the scale and geographical footprint of the deployment, the type of IoT application, the device lifetime, its accessibility and the bandwidth requirements.

Thus, the GSMA presented three models that may be useful to the deployment of IoT connected services.

a) Machine-to-Machine Roaming Model: This involves the use of a roaming-enabled Subscriber Identity Module (SIM) from a Mobile Network Operator (MNO) by an IoT device. Through roaming, the IoT system will enjoy seamless connectivity even when it is outside the area of coverage of its MNO. By this, the IoT system will rely on international roaming partners of the MNO to function outside the coverage of its MNO.

b) Localized Connectivity Model: This entails the use of domestic mobile methods using GSMA specifications for specific geographic communication.

c) Hybrid models: This involves the application of the two models mentioned above. In this, M2M and localized connectivity models are combined to achieve international roaming and seamless local connectivity.

According to GSMA, any of the models is viable and can be selected by a party involved in the IoT technology.

3) Data Protection and Privacy

The GSMA concurs that IoT users' privacy needs to be respected and protected to achieve confidence and trust from the consumers. By this any party involved in IoT technology need to strive to protect the privacy of users.

Hence, there is need for consistency in applying privacy and data protection regulations by all the parties involved with IoT systems. From its wealth of experience in addressing privacy and security issues, the GSMA is collaborating with all the stakeholders to bring adequate privacy and security in IoT design, deployment, maintenance etc.

IV. Critical Requirements for Sustainable Deployment of IoT Systems in Nigeria

From the foregoing, the European Union, USA and many other countries are already establishing regulatory policies to ensure safe and beneficial deployment of IoT applications. In Nigeria, some entrepreneurs have started rolling out IoT applications. In view of the many benefits and potential threats in such systems, it has become important that Nigeria should put in place the critical requirements for a sustainable deployment of IoT systems. Some of these requirements are technical while some require government and stakeholder actions.

A. Government Role and Support

The Nigerian government has the responsibility of providing the enabling environment, policies and laws for the benefit realization of IoT applications and services. The Federal Government functions through Ministries, Departments and Agencies (MDAs). The MDAs whose statutory roles include enabling and regulating IoT and emerging technologies are the Federal Ministry of Communication Technology and Digital Economy, the Nigerian Communications Commission (NCC), and the National Information Technology Development Agency (NITDA). The legislative arm of the government has the role of promulgating the necessary laws for IoT applications and services, while other entities such as educational institutions also have important roles to play in sustainable deployment of IoT systems in Nigeria. Table 1 shows the various government entities, their functions and functional areas in the IoT ecosystem [19].

TABLE I. Entity Roles and Functional Areas in the IoT Ecosystem

S/N	Functional Area	Function	Government Entity
1	Information and Education	• Information dissemination • Education and training • Technical assistance	• Tertiary Institutions, NCC, NITDA, Federal Ministry of Communications

		• Research Funding	Technology and Digital Economy.
2	Technology Development	• Scientific research • Technology demonstration • Intellectual property management •	• Tertiary Institutions, NITDA, NOTAP.
3	Policy and Regulation	• Policy formulation, • Policy implementation • Standards development	• Federal Ministry of Communications Technology and Digital Economy, NCC, NITDA, Legislature (Senate and House of Representatives).
4	Market Development	• Market Solutions, assessment and analysis. • Trade development and export assistance • Business incubators and small business assistance • Financing mechanisms, assistance, and incentives.	• Entrepreneurs, Federal Ministry of Communications Technology and Digital Economy, NITDA, NOTAP.

B. Technical Requirements

There are several technical requirements that must be in place for a sustainable deployment of IoT systems. Some of the critical technical requirements are described in the following sections:

1) Spectrum Requirement

In most cases, IoT devices are designed to use Wireless communication technologies of various bandwidth needs, for long-range and short-range communication purposes:

- Narrowband IoT (NB-IoT): NB-IoT is suitable for standalone IoT nodes operating at the physical layer of the ecosystem.
- Low-Power Wide-Area Networks (LPWANs): Through this, IoT nodes are powered by low-cost batteries for long-range communication purposes. LPWANs are suitable for connecting IoT nodes in networks that span geographical regions or a localities. LPWANs are often used for remote monitoring especially for infrastructure tracking.
- Zigbee: This is employed for short-range, low-power wireless networks to create IoT mesh network by rebroadcasting data over several sensory nodes.

In most countries, it is the National Telecoms regulator in charge of Spectrum management that should ensure that appropriate frequency bands are made available to cater for the various applications.

2) Connectivity Requirements

Ubiquitous connectivity with real-time transmission of data is a crucial requirement for the operation of IoT systems. In most IoT ecosystems prompt data transmission and reception are needed and only good connectivity can guarantee reputable performance. Examples include IoT applications in critical mission tasks like in healthcare and autonomous transportation. In such applications, latency in communication can have dangerous consequences.

Oftentimes, ubiquitous connectivity involves the integration of mobile devices, smart networking devices like routers and people in the loop as controllers [1]. Only an appropriate regulation of service will ensure that satisfactory real time transmission is achieved.

3) Adaptability Requirements

The IoT ecosystem consists of several nodes that are connected via the Internet. Due to factors like poor connectivity and power shortage, IoT nodes can be attached and detached from the ecosystem randomly. Also, the state, location and computing speed of these nodes are bound to changes. In a physical environment this constitutes a challenge, IoT applications should be designed to be self-adaptive to handle the communication between them and the services connected to them [4].

4) Security Requirements

Security is one of the most significant challenges of IoT deployment. For the IoT ecosystem, security involves Privacy, Trust, Confidentiality and Integrity [20]. Since the IoT applications use data from a variety of sources with various forms and speed, it is important that every system design incorporates Trust mechanisms. These mechanisms are to enforce privacy and confidentiality as data is shared between IoT systems. Also, IoT application must be embedded with mechanisms to check data integrity to avoid the erroneous operation of IoT systems [4].

Furthermore, IoT applications are backed by networks that connect the hardware and software components and involves a huge amount of data traveling through several connected devices interfering with the personal spaces of users. With such enormous data online, it is vulnerable to cyber-attacks and hacking [21]. Thus, addressing only network security will not be adequate, the following security considerations must be in place for a safe IoT system:

- Data Exchange Security: data encryption protocol for data transfer from IoT sensors & devices to a platform or gateway to the cloud must be in place.
- Physical Security: since IoT devices are usually autonomous, to avoid tampering by the hackers, physical security measures must be in place.

5) Data Privacy Requirement

Privacy is a crucial element in trust relationships [23]. As stated in [24], the continual increase in the number of IoT devices is threatening the fundamental right to digital privacy across many jurisdictions. According to [24], the Global Privacy Enforcement Network (GPEN) has highlighted privacy challenges facing IoT technology. These challenges include:

- lack of control and information asymmetry: By this challenge, the users have no control over all aspects of data generation, transmission, reception and storage in the IoT systems.
- quality of user consent: This is a challenge because by default users ought to be informed before the IoT data is processed. However, users are not always aware of data processing done by all the IoT devices.
- secondary usage of data: This is a scenario in big data analysis whereby data obtained for a specific purpose is inappropriately used for another purpose without the consent of the user.
- aggregation of data: Without proper anonymization of data from several sources, specific habits and preferences of users can be known. This scenario may be termed intrusive and thus a challenge to data privacy.

Nowadays, data privacy is a socio-cultural and economic issue. As stated in [25], the European Union General Data Protection Regulation (GDPR) guarantees the protection of human beings as it relates to the processing of personal data. Similarly, the data privacy protection laws of some states in the USA are focused on protecting personal information only. In Singapore, the Personal Data Protection Act (PDPA) is focused on protecting the data of human beings only. In Ghana, the Data Protection Act governs the processing of personal data of human beings.

Over the years, data privacy and protection has evolved in Nigeria. A remarkable development is the enactment of the Nigerian Data Protection Regulation ("NDPR"), which was extracted from the GDPR [26].

The important requirement to look out for by regulators is Privacy-by-Design concept that should be adhered to in the development of IoT systems [27]. The Privacy-by-Design concept includes the following:

i. Encryption and Hashing of data in transit between IoT devices and IoT platforms, artificial intelligent platforms, users or partner systems.

ii. Anonymization of personal data to prevent correlation of records through the de-identified data.

iii. Transparency, choice and control on how personal data will be used and shared.

iv. Data ownership traceability on how data is being used within systems, transferred between systems, and used for purposes such as analytics and machine learning.

C. Proposed Policy and Regulatory Framework

A Policy and regulatory framework is key to sustainable IoT roll out and beneficial use in Nigeria. The country already has an established a Ministry and relevant Agencies that can play key roles in the process. In this section, a draft Framework is proposed that will facilitate unleashing of the benefits of IoT with adequate control of the risks. Fig. 2 shows the components of the proposed framework.

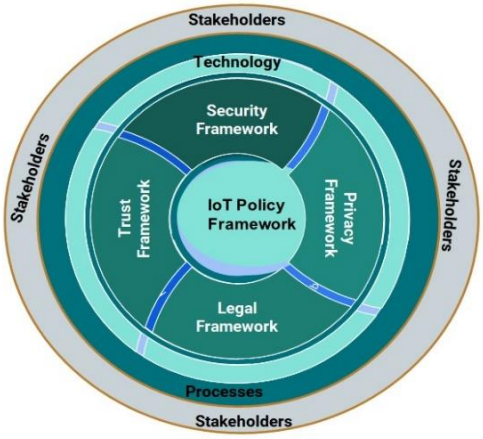


Fig. 2. Proposed Policy and Regulatory Framework.

The process owner for this framework should be the Federal Ministry of Communication Technology and Digital Economy and its agencies. As a result of the complexity of the interactions in the IoT ecosystem, it is recommended that the Security, the Trust, the Legal and the Privacy frameworks be developed holistically to ensure adequate coverage. Furthermore, there will be a need to work together with all relevant stakeholders in the IoT ecosystem to ensure development of a fit for purpose detailed Policy and regulatory framework on IoT the country. Some guidelines for the detailed development of the framework components are presented in the following sections.

1) Legal Framework

IoT has led to new systems (products/services) where machines will take decisions based on available data. A Legal framework need to be developed for issues that might arise from IoT related systems. Entrepreneurs in the country are already developing and deploying standalone solutions typically for security applications in homes and for agriculture. Some of these solutions are using the GSM Mobile Networks to provide connectivity.

The Legal Framework should cover the entire spectrum of IoT stakeholders to ensure proper engagements in IoT systems. The framework should take care of business ethics, social responsibility, data protection, contractual arrangements, and all necessary rules of engagement.

For instance, the legal framework should empower the regulator, NCC and other relevant agencies to type-approve all IoT devices and accessories shipping into Nigeria, in addition to monitoring IoT equipment Vendors and Service Providers for compliance. Furthermore, IoT Device Application developer should be monitored for compliance to National Data Protection Act.

2) IoT Trust Framework

Trust in the IoT context refers to the expected behaviour of the IoT components, such as persons or services. It is an important element in negotiations and transactions. Understanding the different aspects of Trust is important in developing regulations and policies for the IoT technology. Therefore, it is important to evaluate, monitor, compare and develop different methods and products to tackle specific trust objectives.

Trust has several meanings and is used in different contexts. In the IoT context, it is paramount to establish acceptable thresholds for privacy, security, reliability, availability, and integrity as it relates to human and machine behaviour. The complexity of interactions involved in IoT requires addressing the trust at every layer of the IoT ecosystem and at the interfaces. The three-layered architecture for trust management control presented in [28], will be suitable for developing the Trust Framework. The layers of the architecture are sensor, core and application. In the IoT architecture, every layer has its own specific trust management scheme. Through the control mechanism, the user is bestowed the capability of taking the final decision according to the collected trust information and policy.

The primary objective of an IoT Trust framework as part of the Policy is to have the legal instruments for ensuring a Trusted and Safe Environment for IoT. The process owner needs to have the trust Framework developed in detail to be able to address various scenarios.

3) IoT Privacy Framework

Privacy, a measure of propensity to share data, is a fundamental human right. Privacy involves the ability of a "thing (human or object)" to control information about itself. The connection between privacy and autonomous things is an evolving theme that requires continuous research. IoT applications are affecting privacy and personal data protection because they rely on personal data to effectively deliver services.

The distributed architecture and numerous nodes in the IoT ecosystem have made privacy a challenge than in other computing applications. For instance, control of personal data is more difficult due to the huge number of distributed sources of data. Also, the existence of many personal data processing entities and chain of providers of IoT services have made the enforcement of data protection law complex.

The concepts of security and privacy have complex inter-relationships. Security enables privacy in a specific case. Many security approaches and methods are useful in enhancing privacy and protecting data of an entity. Encryption cryptographic algorithms and hashing functions are useful for effective identity while access management solutions protect from unauthorized access and usage of data.

Security techniques support data privacy and protection. However, these techniques do not guarantee the principles of privacy in its entirety. For example, in the IoT ecosystem where a device may gather and store more data than needed for its services, an e-Commerce transaction secured with HTTPS may lack the principles of data minimization. Thus, research is still on going to address some of the complex privacy challenges, but in the meantime, the principle of "Privacy by Design" introduced under Article 25 of the GDPR for processing of personal information under EU Law can be used by Nigeria. Hence the rules for privacy-by design are:

By default, the collection and storage of personal data is governed by regulations.

- As-If' X-by-Design: This is the requirement that IoT systems (products and services) are developed as-if they will collect and process personal data at some point when deployed.
- De-Identification by Default: This refers to the deletion of personal data immediately the legal basis for storing them expires.
- Data Minimization by Default: This involves the deletion of personal data where and when not required. By this, storage and processing of personal data take place where and when required.
- Encryption by Default: This is the process of encrypting personal data from the start.

4) IoT Security Framework

IoT technology involves the participation of stakeholders: suppliers, integrators, operators, regulators, users, etc. A robust security framework that can address all the various perspectives and domains is required. The IoT Security framework to be developed will need to take into consideration the already established CIA triad of Confidentiality, Integrity, and Availability, some existing standards, and some additional properties in view of the several layers of IoT devices and stakeholders. Some of these additional properties include:

- Reliability: The level of continuous correct service, the guarantee that data will get to its destination in the form it was transmitted by IoT systems.
- Safety: This is the level at which the IoT systems and humans are free from danger (the safety of users, the systems and the environment).
- Maintainability: This is the ability for systems to be modified and repaired at ease.
- Transparency: This is a measure of an adequate level of clarity of the security and privacy that can be understood and reconstructed at any instant.
- Intervenability: This is the ability of relevant partners to intervene in security and privacy issues.

Furthermore, some of these properties have already been addressed by established standards that need to be studied and taken into consideration in developing a sustainable IoT Framework for the country. Some of these standards include:

- Privacy-by-Design - defined in ISO/IEC 27550 and GDPR.
- Resilience-by-Design - the NIST cybersecurity framework36.
- Big data security and privacy (ISO 20547 part 4).
- Smart city business process framework (ISO 30145-1).

V. CONCLUSION

The United States, India and the European Union are taking advantage of already developed standards on IoT to establish policies and regulations to ensure benefit realization of IoT. The key advice agreed by the Body of European Regulators for Electronic Communications (BEREC) and GSM Association on the need for flexible and technology unbiased policies, some global deployment models and Data Protection and Privacy best practices may be useful for any country yet to develop a policy on IoT.

The development of a robust policy and framework that will meet the needs of the country will require a multisectoral approach in view of the complex nature of the IoT ecosystem and the possible great number of interactions amongst the 'things/objects'. Since entrepreneurs are already deploying IoT systems, the country can no longer continue to wait because there are some already established standards and best practices that may be utilized in developing the proposed Policy and Regulatory Framework according to the needs of the country.

VI. Recommendations

Sustainable benefits can only be realized if an appropriate IoT policy framework is developed to meet the country's needs. It will not be beneficial to just adopt another county's policy because Nigeria may not be at the same level of development, though there are some established global standards discussed in the previous sections that should be adopted for the development of an appropriate policy framework.

Since IoT is very complex with a huge number of interconnected things, the development of the proposed policy and regulatory framework requires collaboration of stakeholders in the IoT ecosystem. In considering challenges such as privacy, security, and standardization, governments should resist the temptation to create specific rules and national standards for IoT that may restrict trade.

Furthermore, the policy implementation should make provision for a Program Management Unit, a Governance Committee, and an Advisory Committee. The Program Management Unit will have the responsibility to provide implementation support to various initiatives within the IoT policy and track performance. The Governance Committee will be drawn from representatives from government, industry and academia to drive policy implementations of all IoT initiatives. While the Advisory Committee will also have representatives from Government, industry and academia to provide expert guidance in the emerging area of IoT.

References

[1] F. Khodadadi, A. V. Dastjerdi, and R. Buyya, "Internet of Things: An Overview," in Internet of Things, Elsevier Inc., 2016, pp. 3–27.

[2] "An Introduction to the Internet of Things (IoT)," no. November. Lopez Research LLC, pp. 1–6, 2013, [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf.

[3] T. Kramp, R. van Kranenburg, and S. Lange, "Introduction to the Internet of Things1," in Enabling Things to Talk, Springer, 2013, pp. 1–10.

[4] I. S. Udoh and G. Kotonya, "Developing IoT applications: challenges and frameworks," IET Cyber-Physical Syst. Theory Appl., vol. 3, no. 2, pp. 65–72, 2018, doi: 10.1049/iet-cps.2017.0068.

[5] "GSMA response to the draft BEREC Report for public consultation on enabling the Internet of Things," no. November. GSMA, pp. 1–18, 2015, [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2016/09/GSMA-response-to-BEREC.pdf.

[6] S. Albishi, B. Soh, A. Ullah, and F. Algarni, "Challenges and Solutions for Applications and Technologies in the Internet of Things," Procedia Comput. Sci., vol. 124, pp. 608–614, 2017, doi: 10.1016/j.procs.2017.12.196.

[7] F. Eleanya, "Nigeria has enough bandwidth to cater for the Internet of Things - IoT Africa Networks Ltd CEO - Businessday NG," 2019. https://businessday.ng/interview/article/nigeria-has-enough-bandwidth-to-cater-for-the-internet-of-things-iot-africa-networks-ltd-ceo/ (accessed Dec. 01, 2020).

[8] A. Okunola, "What Does IoT Look Like In Nigeria Right Now? | TechCabal," 2018. https://techcabal.com/2018/06/06/what-does-iot-look-like-in-nigeria-right-now/ (accessed Dec. 01, 2020).

[9] P. Osuagwu, "Nigeria: Why Nigeria's IoT Market May Hit $1bn in Five Yrs - allAfrica.com," 2019. https://allafrica.com/stories/201911200059.html (accessed Dec. 01, 2020).

[10] O. J. Kunle, O. A. Olubunmi, and S. Sani, "Internet of things prospect in Nigeria: Challenges and solutions," in 3rd International Conference on Electro-Technology for National Development, NIGERCON 2017, 2017, pp. 736–745, doi: 10.1109/NIGERCON.2017.8281942.

[11] U. J. Orji, "Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?," Int. Conf. Cyber Conflict, CYCON, vol. 2015-Janua, no. October, pp. 105–118, 2015, doi: 10.1109/CYCON.2015.7158472.

[12] O. Vermesan et al., "IoT Policy Framework." European Commission, 2017.

[13] C. Maple, "Security and privacy in the internet of things," J. Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017, doi: 10.1080/23738871.2017.1366536.

[14] A. Rennie, "Exploring the regulatory and legislative landscape for IoT devices," 2020. https://www.inlinepolicy.com/blog/regulatory-landscape-for-iot-devices (accessed Dec. 02, 2020).

[15] A. Khanna and S. Kaur, Internet of Things (IoT), Applications and Challenges: A Comprehensive Review, vol. 114, no. 2. Springer US, 2020.

[16] "Official Document TS.34 - IoT Device Connection Efficiency Guidelines." GSM Association, 2020.

[17] OECD, "The Internet of Things - Seizing the Benefits and Addressing the Challenges," 2016. [Online]. Available: http://search.proquest.com/docview/1797548811?accountid=8144%5Cnhttp://sfx.aub.aau.dk/sfxaub?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:book&genre=unknown&sid=ProQ:ABI%2FINFORM+Global&atitle=&title=THE+INTERNET+OF+THINGS+SEIZING+THE+BENEFITS+AND.

[18] "Draft Policy on Internet of Things." Department of Electronics and Information Technology, Ministry of Communication and Information Technology (DeitY), p. 17, 2015, [Online]. Available: http://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy_0.pdf.

[19] J. Pietruszkiewicz, "What are the Appropriate Roles for Government in Technology Deployment? A White Paper with Author's Response to Comments," 1999. Accessed: Dec. 04, 2020. [Online]. Available: http://www.doe.gov/bridge.

[20] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.

[21] Emorphis, "IoT Application Development Challenge," 2020. https://blogs.emorphis.com/iot-application-development-challenges/ (accessed Dec. 01, 2020).

[22] E. Kuzemchak, "How to overcome challenges in IoT application development | Software Design Solutions," 2020. https://softwaredesignsolutions.com/blog/how-to-overcome-challenges-in-iot-application-development/ (accessed Dec. 01, 2020).

[23] Internet Society, "Internet Society Policy Brief: IoT Privacy for Policymakers," no. September. Internet Society, 2019, [Online]. Available: internetsociety.org.

[24] C. Okoriekwe, "Internet Of Things (IoT) And Digital Privacy Right: Drawing The Dividing Line In Nigeria - Privacy - Nigeria," Nigeria, 2020.https://www.mondaq.com/nigeria/data-protection/938728/internet-of-things-iot-and-digital-privacy-right-drawing-the-dividing-line-in-nigeria (accessed Dec. 01, 2020).

[25] B. Scott and S. Eke, "NDPR And The Protection Of Personal Data Of Legal Entities In Nigeria - Privacy - Nigeria," Nigeria, 2020. https://www.mondaq.com/nigeria/privacy-protection/961432/ndpr-and-the-protection-of-personal-data-of-legal-entities-in-nigeria?type=related (accessed Dec. 01, 2020).

[26] B. Scott and S. Eke, "A Review Of The Nigerian Data Protection Bill 2020 - Privacy - Nigeria," Nigeria, 2020. https://www.mondaq.com/nigeria/privacy-protection/983116/a-review-of-the-nigerian-data-protection-bill-2020?type=related (accessed Dec. 01, 2020).

[27] "Protecting Privacy and data in the internet of things." GSMA, 2019, Accessed: Dec. 04, 2020. [Online]. Available: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf.

[28] U. M. Mbanaso, G. A. Chukwudebe, B. Adebisi, "Holistic Security Architecture for IoT Technologies", 2017 13th International Conference on Electronics, Computer and Computation (ICECCO), pp. 11- 16.

Conceptual Modelling of Criticality of Critical Infrastructure N^{th} Order Dependency Effect Using Neural Networks

U. M. Mbanaso
Centre for Cyberspace Studies,
Nasarawa State University, Keffi,
Nigeria
https://orcid.org/0000-0003-2784-7415

J. A. Makinde
Centre for Cyberspace Studies,
Nasarawa State University, Keffi,
Nigeria
Julius.makinde@bazeuniversity.edu.ng

Abstract–This paper presents conceptual modelling of the criticality of critical infrastructure (CI) n^{th} order dependency effect using neural networks. Incidentally, critical infrastructures are usually not stand-alone, they are mostly interconnected in some way thereby creating a complex network of infrastructures that depend on each other. The relationships between these infrastructures can be either unidirectional or bidirectional with possible cascading or escalating effect. Moreover, the dependency relationships can take an n^{th} order, meaning that a failure or disruption in one infrastructure can cascade to n^{th} interconnected infrastructure. The n^{th}-order dependency and criticality problems depict a sequential characteristic, which can result in chronological cyber effects. Consequently, quantifying the criticality of infrastructure demands that the impact of its failure or disruption on other interconnected infrastructures be measured effectively. To understand the complex relational behaviour of n^{th} order relationships between infrastructures, we model the behaviour of n^{th} order dependency using Neural Network (NN) to analyse the degree of dependency and criticality of the dependent infrastructure. The outcome, which is to quantify the Criticality Index Factor (CIF) of a particular infrastructure as a measure of its risk factor can facilitate a collective response in the event of failure or disruption. Using our novel NN approach, a comparative view of CIFs of infrastructures or organisations can provide an efficient mechanism for Critical Information Infrastructure Protection and resilience (CIIPR) in a more coordinated and harmonised way nationally. Our model demonstrates the capability to measure and establish the degree of dependency (or interdependency) and criticality of CIs as a criterion for a proactive CIIPR.

Keywords: Critical Infrastructure, critical information infrastructure protection, recurrent neural networks, degree of infrastructure criticality degree of infrastructure dependency.

I. INTRODUCTION

The increasing dependency of Critical Infrastructure (CI) on Information and Communications Technology (ICT) undoubtedly, has continued to raise unprecedented systematic cybersecurity risks and threats. These are capable of undermining national security, economic prosperity and the ordinary lives of citizens. Incidentally, no critical infrastructure is standing alone, they are mostly interconnected in some ways, which create a complex network of infrastructures that depend on each other. The relationships between these infrastructures can be either unidirectional or bidirectional with possible cascading or escalating consequences. Moreover, the dependency relationships can take an n^{th} order, implying that a failure or disruption in one infrastructure can cascade to n^{th} order interconnected infrastructure. The n^{th}-order dependency and criticality problems demonstrate a sequential characteristic, which can result in multipath cyber effects with different risks [1], [2]. The implication is that measuring the criticality of infrastructure involves the calculation of the impact of its failure or disruption on other interconnected infrastructures. This is a complex problem that requires the understanding of the multifaceted relational behaviour of n^{th} order associations amongst interconnected infrastructure.

We model the behaviour of n^{th} order dependency using Neural Networks (NN) to analyze the n^{th} degree of dependency and criticality of the dependent infrastructures. The outcome, which is to quantify the Criticality Index Factor (CIF) of a particular infrastructure as a measure of its risk influence, can facilitate a collective response in the event of failure or disruption. Using our NN approach, a comparative view of CIFs of infrastructures or organizations can provide an efficient mechanism for Critical Information Infrastructure Protection and Resilience (CIIPR) in a more coordinated and harmonized way nationally. In this way, a single view to measure and establish the degree of dependency (or interdependency) and criticality of such infrastructures can predictively aid in proactive CIIPR.

This paper attempts to model how to determine the criticality of N^{th} Order Dependency Effect (NODE) of critical infrastructure using NN. The NN can help model the complexity of n^{th} order dependency to deepen the understanding of the relational influence of multilayer dependencies.

In the rest of this article, section II presents background and related works; section III describes the methodology; section IV presents the modelling of n^{th} order dependency effects. Section V discusses the results and section VI concludes the paper.

II. BACKGROUND AND RELATED WORKS

A. Cascading and Escalating Effect of Dependency

It has been established in the literature that modern infrastructures are interdependent [3][4][5]. This interdependency introduces a multipath problem in determining the criticality of infrastructure because the interdependency can extend to n^{th} degree order. First, the

This work is sponsored by TETFund National Research Fund (NRF).

dependency of infrastructure on others is conceptually demonstrated in figure 1. It shows that infrastructure C depends on infrastructure A and B, i.e., C operationally depends on the functions or services provided to it by A and B. This is referred to in the literature as upstream since A and B are external to C [6]. In contrast, D and E depend on

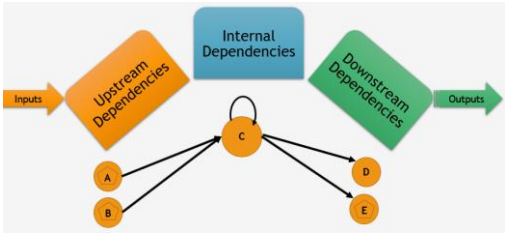


Figure 1: Complexity of dependency

C, which can be described as downstream [7]. The implication is that malfunction of A or B or both can affect C as well as D and E. Undoubtedly, the effect can be cascading or escalating to the n^{th} order. Notwithstanding, infrastructure C, may have its internal components of which the failure or disruption, can affect it as well. To this extent, it can be alluded to the complexity of relational relationships of modern infrastructures, further expatiated in the sections that follow.

B. Cluster of Dependencies

Figure 2 shows a unidirectional dependency of one to many with the corresponding weighted value that illustrates how much an infrastructure depends on another. Infrastructure B, C, D and E depend on A. In this relation arrangement, the failure or disruption of any of the dependent infrastructures cannot affect B, C, D and E. The disruption of any of these infrastructures will not affect infrastructure A but events in A can influence the other infrastructures.

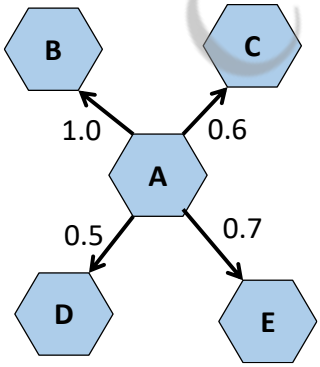


Figure 2: Unidirectional dependency

In figure 3, another dimension of interdependency between infrastructures are introduced. The relationship between A and B is referred to as bidirectional [8]. It conceptualises the fact that a disruption in B can be cascaded to other dependent infrastructures through infrastructure A.

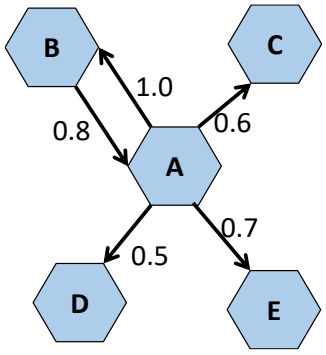


Figure 3: Bidirectional dependency

Figure 4 illustrates a multipath dependency. This amplifies the complexity of interdependences. However, determining the criticality of infrastructures in a multipath structure is not trivial; the complex structure requires scientific modelling and simulation.

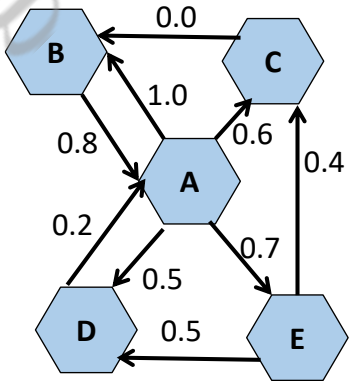


Figure 4: Multipath (or Multimode) dependency

C. Order of Dependencies

Figure 5 exemplifies the concept of depth of dependency which can be n^{th} order. For instance, telecom infrastructure depends on power, financial systems depend on telecom, and the healthcare sector depends on financial systems. The n^{th}-

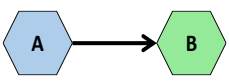


Figure 5.1: First order

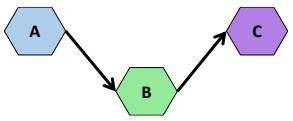


Figure 5.2: Second order

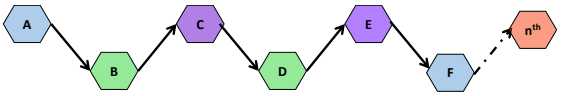


Figure 5.3: n^{th} order

order dependency introduces another intricacy. The implication is that the criticality of any infrastructure will also hinge on how its failure or disruption can affect the n^{th} order dependent infrastructures.

The notions of dependency and interdependency of critical infrastructures are well researched in the critical infrastructure research community. Cheng proposed Asymmetric Dependency Matrices (ADM) to classify a set of parental dependencies of which failure will cause a cascading effect on the independents [2]. This work measures the strength of dependency between a node and another node.

Bloomfield et al. in Preliminary Interdependency Analysis (PIA), used an empirical modelling approach to determine the failure patterns between critical infrastructure to ascertain the type of risk to be guided against [9]. The work failed to take into cognizance the escalating effect on n^{th} order interdependency. 1^{st} order dependency may not be sufficient to understand the complex critical nature of dependency. Our approach considers the relational influence in the n^{th} order dependency.

III. METHODOLOGY

The concept of Neural Networks (NN) is not new but hardly has it been extended to critical infrastructure study. It is a suite of algorithms that can help understand underlying relationships in a set of data, which mimics the manner the human brain functions [10], [11]. Another important characteristic is the ability of NN to adapt to dynamic input, which can produce anticipated output without redesign. The complexity of the n^{th} order cluster of critical infrastructures can fit into NN. We model the cluster of CIs as nodes and show how they are linked together. Using MATLAB, we create the complex CI network and apply chosen NN algorithms. The weights of the nodes are systematically modified to simulate the influence of changes on the independent node to the dependent nodes.

IV. MODELLING OF N^{TH} ORDER DEPENDENCY

A neural network simulates a lot of interconnected cells that learn things or patterns to predict or take decision with artificial neurons [12]. It plays a vital role in artificial intelligence to determine the cause and effect of events.

Figure 6 is a model architecture of core critical infrastructure and the relational dependencies. We consider a layered neural network, with input, output and hidden layers, where the independent infrastructure is the input, the hidden layer represents the n^{th} order dependency which can be one or many and the output is the effect of the input on the hidden layer. The dependency factor weight *(dfw)* is the measure of reliance of infrastructure on the other, ranging between 0 and

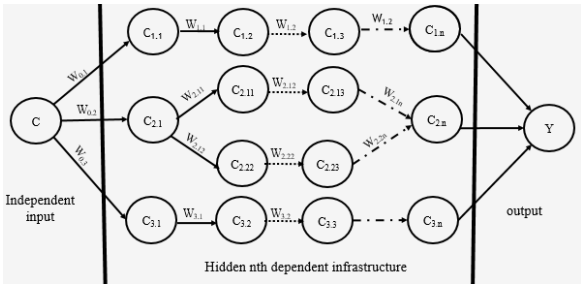


Figure 6: Neural network of n^{th} order dependency Architecture

1. In other words, it is the measure of dependency of infrastructure on the other. The higher this value is, the higher the influence. We first applied *dfw* to relational dependents as seen in figure 6 (W0.1, W0.2, W1.1, etc). We then measure quantitatively, the criticality of the core infrastructure in the n^{th} order relational dependency to comparatively assess the criticality of dependency effects of relational interconnected infrastructures (or cluster of infrastructures).

Taking a node as an infrastructure, the effect of dependency of a node is calculated as the product of the input and the weight added to the bias. In figure 6, the effect of C on infrastructure is as seen in equation 1:

$$y = wc + 1 \quad \text{---------} \quad 1$$

Where w is the dfw, C is the output of the preceding infrastructure and b is the bias that is always 1. The result of each iteration serves as the input to the next infrastructure. We then sum up the weighted sum 'y' to have the final value of Y as seen in equation 2. Y is the cumulative sum of the all-Dependency Effects (DE).

$$Y = \sum y \quad \text{-------------} \quad 2$$

We then apply a transfer function of sigmoid 'S' to normalise Y in the range of 0 to 1 as a composite value for effective comparative analysis of criticality factors of interrelated infrastructures., Thus, equation 3.

$$\text{Sigmoid (S)} = \frac{1}{1 + e^{-Y}} \quad \text{-------} \quad 3$$

Dependencies of infrastructures of n^{th} order are generally complex and unobtrusive [13] but the consequences of cascading effect of disruption of an independent CNI to other CNI contributes to the overall criticality of such an infrastructure. In figure 7, we consider a multilayer dependency, where the criticality effect of the core infrastructure C_1 can be a functional value C_{nif} (criticality index factor), which is the sum of y_0, y_1 and y_2 as shown in Figure 7.

Figure 7 illustrates how much a set of critical infrastructure depends on C_1, demonstrating a one-to-many relationship. The first-order set of infrastructure *dfw* is 0,3, 0.4 and 0.2 respectively. As illustrated in figure 7, the *dfw* shown in the n^{th} order path depicts the relational weight from

the previous node in the directional path. Where a critical infrastructure has a multipath dependency, each path is

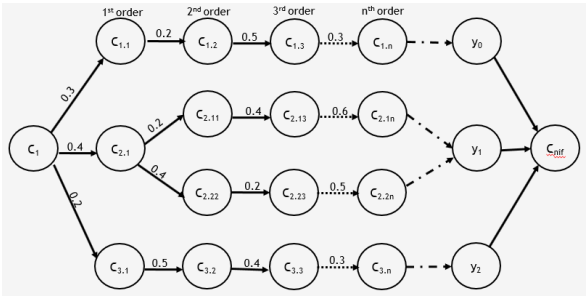


Figure 7: Critical infrastructure (C_1) with applied dependency factor weight (dfw)

calculated based on the different weights that sum up the path.

Using MATLAB, we can simulate the n[th] order dependency of an infrastructure C_1 to determine the criticality effect caused by n[th] order dependents. First, the *dfw* value of C_1 can be initialized based on the potential effect of a perturbation(disaster) or a cyber-attack. The initial state of node C_1 is set to 1, which implies that the C_I is functioning in its optimal capacity.

Applying equation 1 to figure 7 with C_1 set to 1 for its optimal operation, we have:

$y_0 = ((0.3x1) +1) +((0.2x1.3) +1) +((0.5x1.26) +1) +((0.3x1.63) +1))$

$y_0 = 5.679$

Applying the same equation for y1 and y2,

$y_1 = 12.0272$

$y_2 = 5.932$

Applying equation 2:

$C_{nif} = y0 + y1 + y2 = 23.6382$

Applying equation 3 to derive C_{nif} for based on sigmoid function:

Cnif = 1/〖1+e〗^(-23.6382)

Therefore,

$C_{nif} = 0.999999999945792$

Therefore, it is evident from the derivation that the criticality index factor at full optimal operation is 1.

V. DISCUSSION OF RESULTS

The conceptual modelling has demonstrated the ability to use neural network principles to derive the criticality of n[th] order dependency of critical infrastructures. The C_{nif} at optimal function shows there is a correlation that *dfw* has a direct effect on the criticality of n[th] order dependency. The *dfw* is a function of how a dependent infrastructure depends on the independent infrastructure. The cascading relationship dictates the depth of the dependency, which has an impact on its directed path. For comparative analysis of critical infrastructures, the quantitative approach provides numerical values in the form of critical index factor of individual independent infrastructures to enable comparison. The idea is that infrastructures can hardly have the same criticality in varying environmental context.

VI. CONCLUSION

We apply NN to address the complexity of the n[th] order interdependency effect of Critical Infrastructure based on its underlying principles. This is ongoing research on the application of NN to determine the n[th] order dependency effect.

In future work, we intend to develop a cluster of n[th] order dependency infrastructures to simulate critical infrastructures from different sectors and the interdependency. This can help derive the C_{nif} of many CI organisations, which can provide the basis for comparative analysis.

References

[1] G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in North America Europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[2] Q. Cheng, "A new mathematical framework and spatial decision support system for modeling cascade interdependency of critical infrastructure during geo-disasters," *J. Earth Sci.*, vol. 28, no. 1, pp. 131–146, 2017.

[3] A. N. Singh, M. P. Gupta, and A. Ojha, "Identifying critical infrastructure sectors and their dependencies: An Indian scenario," *Int. J. Crit. Infrastruct. Prot.*, vol. 7, no. 2, pp. 71–85, 2014.

[4] Public Safety Canada, "Role of Critical Infrastructure in National Prosperity," 2015.

[5] M. Iturriza, L. Labaka, J. M. Sarriegi, and J. Hernantes, "Modelling methodologies for analysing critical infrastructures," *J. Simul.*, vol. 12, no. 2, pp. 128–143, Apr. 2018.

[6] M. Iturriza, L. Labaka, J. M. Sarriegi, and J. Hernantes, "Modelling methodologies for analysing critical infrastructures," *J. Simul.*, vol. 12, no. 2, pp. 128–143, Apr. 2018.

[7] E. M. B. C. (EMBC) Provincial Emergency Program (PEP), "Critical Infrastructure Rating Workbook," British Columbia, 2007.

[8] N. Sharma, F. Nocera, and P. Gardoni, "Classification and mathematical modelling of infrastructure interdependencies," *Sustain. Resilient*

Infrastruct., vol. 00, no. 00, pp. 1–22, 2020.

[9] R. E. Bloomfield, P. Popov, K. Salako, V. Stankovic, and D. Wright, "Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment," *Reliab. Eng. Syst. Saf.*, vol. 167, no. March, pp. 198–217, 2017.

[10] S. Sharma, S. Sharma, and A. Anidhya, "Understanding Activation Functions in Neural Networks," *Int. J. Eng. Appl. Sci. Technol.*, vol. 4, no. 12, pp. 310–316, 2017.

[11] Y. Almoghathawi, K. Barker, C. M. Rocco, and C. D. Nicholson, "A multi-criteria decision analysis approach for importance identification and ranking of network components," *Reliab. Eng. Syst. Saf.*, vol. 158, pp. 142–151, 2017.

[12] U. Güçlü and M. A. J. van Gerven, "Modeling the dynamics of human brain activity with recurrent neural networks," *Front. Comput. Neurosci.*, vol. 11, Feb. 2017.

[13] R. Setola, V. Rosato, E. Kyriakides, and E. Rome, *Studies in Systems, Decision and Control 90 Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach*. 2016.