IEEE

Advancing Technology for Humanity

1ST IEEE MULTI-CONFERENCE SERIES

August 25th-30th 2020

ONLINE

THEME:

TRANS-DISCIPLINARY SCIENCES, ENGINEERING & INFORMATION SYSTEMS AND COMPUTING APPLICATIONS, 2020 (TEICA-2020)

IEEE HAC | IEEE SIGHT FUNDED PROJECT COVID-19

IEEE Nigeria Consultants' Network (CN)

American University of Nigeria

IEEE Computer Society

IEEE young professionals

IJMEC

Unified Academy of Innovation New Zealand

CONFERENCE ORGANIZING COMMITTEE

Conference Host

Dr. Dawn Dekle, President, American University of Nigeria (AUN)

International Program Chair

Prof. Sam Goundar, Department of Information Systems, Victoria University of Wellington, New Zealand.
Prof. Khalil Drira, CNRS, LAAS, University of Toulouse, France

General Conference Chair

Prof. Longe Olumide, Dean, American University of Nigeria, Yola, Adamawa State Nigeria
Dr. M.M. Inallou, Unified Academy of Innovation, Wellington, New Zealand (Co-Chair)

Technical Program Committee

Dr. Kennedy Chinedu Okafor, Mechatronics Engineering, FUTO Nigeria & IEEE, Nigeria Section. (Chair)
Prof. Thierry Villemur, CNRS, LAAS, University of Toulouse, France
Dr.Nawal Guermouche, CNRS, INSA, LAAS, University of Toulouse, France
Dr.Samir Medjiah, CNRS, LAAS, University of Toulouse, France
Dr.Gabriele DAntona, Energy Department, Politecnico di Milano, Milan, Italy
Dr.Aniedu Azubuike Nzubechukw , Nnamdi Azikiwe University, Nigeria)
Prof. Richard Boateng , University of Ghana, Legon, Accra, Ghana
Prof. Khalil DRIRA (CNRS, LAAS, University of Toulouse, France
Dr. Kamak Ebadi (NASA Jet Propulsion Laboratory, Santa Clara University, CA, USA
Dr. Richard Evans, University of Westminster, London, UK.
Dr. Zhen Gao, Mc Master University, Hamilton, Ontario, Canada
Dr. Brij Gupta, National Institute of Technology Kurukshetra India
Dr. Mehdi Khalili, Payame Noor University, Tehran, Iran)
Dr. Javad Khodabakhsh, Power Electronic Lab., Western University, Ontario, Canada.
Prof. Edward Santiago Blaiswe, Sullivan College, State University of New York, USA.
Prof. Tao Tan Technische Universiteit Eindhoven, Nijmegen, Netherland
Collin Tharkur, Durban University of Technology, South Africa
Prof. H. Towsyfyan, Institute of Sound and Vibration Research (ISVR), University of Southampton, Southampton, UK..
Prof. Friday Wada, University of Hartford, West Hardford, Connecticut, USA)
Prof. Viranjay Srivastava, University of KwaZulu-Natal, Durban, South Africa.
Engr. Mrs. Ehinomen E. Atimati, FUTO Nigeria.

Digital Publication Chair

Oluleke O. Babayomi
Opara Benjamin

Finance Committee Chair

Emmanuella O.N

Editors

Longe Olumide
Kennedy C. Okafor
Ehinomen E. Atimati

Table of content

Uncertainty Resolution in Machine Learning Using Statistical Methods

Ridwan Salahudeen, SandipRakshit, GarbaAliyu, Hassan JimohOnawola
School of Information Technology & Computing
American University of Nigeria.
Yola, Nigeria
ridwan.salahudeen@aun.edu.ng, sandip.rakshit@aun.edu.com, garba.aliyu@aun.edu.ng, hassan.onawola@aun.edu.ng

***Abstract*—Identification of a machine-learning algorithm that will universally achieve the best predictive accuracy with both the current available dataset and future streams of dataset is a big challenge in the area of machine learning uncertainty.Suppose Neural Network is proven to be the most accurate algorithm for a classification problem using a dataset named A, the accuracy of this Neural Network cannot be guaranteed for a future stream of that same dataset, because of some noise or emission from the sensor generating the data. This paper discusses the potentials of statistical methods in handling such uncertainty in machine learning to achieve robust predications, the paper proposed a probabilistic model for a machine to automatically determine the machine learning model with most accuracy among all other equally suitable model for a given machine learning problem.**

Keywords— Machine Learning, Uncertainty, AI, Probabilistic models

I. INTRODUCTION

An electronic device can become intelligent by training them through the abundant data at its disposal,using relevant machine learning techniques. The training is similar to the way humans learn through the experiences they are been exposed to. Accordingly, a machine also can learn through its exposure to a huge volume of data and make more better and intelligent decisions in its operations[1].

Machine learning techniques are categorized as either supervised, unsupervised, or reinforcement learning. Each of these categories has its specific strength on various types of datasets and has its peculiar way of training a dataset into a model that can be used for a plethora of intelligent purposes[2]. The supervised learning methods normally requires itsdataset to be in the form of input and output labels in order to form a model. Once a model is formed, an unseen input data can be used to predict a possible output label from the model. Unsupervised learning, on the other hand, does not require explicit labels as input and output, it basically clusters its dataset into groups based on commonality in the data features[3]. In the case of reinforcement learning, learning is done by exposing an electronic agent to an environment. This agent has the capability of perceiving its environment using hardware such as sensors and actuators.A model is then created from the experiences the agent perceives from its environment,and then periodic feedbacks in the form of either a reward or punishment are received to moderately adjusting the model[1]. Figure 1 illustrates a general workflow of how machine learning works.

However, identifying the most suitable category of machine learning techniques to be adopted for any particular dataset is a difficult task to be done by machines autonomously and intelligently. This is because data are prone to uncertainty due to their expressivity in natural languages that are mostly reflections ofhuman ambiguous thoughts, consequently making these data inherently infused with imprecision and/or incompletion[4]. In addition, machine-learning models are not intelligent enough to guaranty all kinds of future predictions the models can come up with[4].

On the other hand, statistics being a discipline of science that has excellence in analysing data associations and dependencies, has a great similarity with machine learning in understanding patterns in a dataset[2]. A subfield in statistics known as the probability has proven to be effective in evaluating the chances of having an event to occur. This is therefore very useful framework for modelling uncertainties in unseen data. Probability theorieshave achieve great milestones different areas of artificial intelligence, robotics and machine learning[4].

This research work intends to investigate the untapped potentials of probability in machine learning models in order to address issues of uncertainties that are inherent in machine learning techniques and proposed a probabilistic model for a machine to automatically determine the machine learning model with most accuracy among all other equally suitable model for a given machine learning problem.

II. LITERATURE REVIEW

[2]proposed an uncertainty resolution scheme in the segmentation of images using the Bayesian model. The method outputs an intelligent pixel-wise segmentation of an image and gives a measure of the uncertainty factor for each class in the segmentation.

[5]proposed to model some classes of uncertainties for an intelligent pixel-wise image segmentation and depth regression tasks. In their work, they argued that epistemic uncertainty is the most crucial class of uncertainty needed for safety-critical applications and in situations where training is done with small datasets.

[6]developed an uncertainty estimator for an intelligent pixel-wise classification for urban remote sensing images. They argued that the estimated uncertainty in the pixel-wiseclassification is fit to indicate the correctness of pixel labelling in image processing.

[7]usedthe Bayesian network to generate an uncertainty map for super-resolution of diffusion magnetic resonance imaging in assessing brain images for clinical usage of the super-resolved images.

In all of these related works, no work addresses the challenge of summing up allthe approximations made by these researchesinto the mainstream machine learning procedures. This research therefore seek to address this problem using probability techniques.

III. PROBABILISTIC MODELLING IN MACHINE LEARNING

Machine learning has received many appraisals in its plethora of breakthroughs in practical areas such as computer visions, speech recognitions, self-driving cars, recommender systems, financial predictions, automated empirical data analysis, automated trading, and more.

All of these breakthroughs are possible because of the availability of data in abundance. The more data are available for training a machine the merrier. This abundance of these data, the formation of models from such data, the visualizations and interpretations of the data are the basic ingredients statistics share in common with machine learning and other techniques in the field of artificial intelligence. Hence, there is a strong relationship between the fields of statistics and computing when dealing with artificial intelligence.

Researches that are currently benefiting on the fusion of the fields of statistics and artificial intelligence are[8]:

1) Probabilistic programming paradigm, which is a way of expressing probabilistic models as computer code.

2) A Bayesian optimization model that uses Bayesian network to optimize computer algorithms.

3) A hierarchical learning model for understanding the relationship among machine learning models that strive to achieve the same purpose.

4) Probabilistic theories for data compressions techniques.

5) Automation of interpretable data model and data discovery.

The main functionalities in machine learning could be seen as a form of probability, this is based on the fact that machine learning uses feature's similarities in a dataset to form patterns and make future predictions by inferring from a given dataset to uncertain quantifications, just as similar to the way probabilistic models measures likelihoods of events.

In any machine learningtask, the goal is deriving a predictive model that would stand the test of high performance metrics at different circumstances the future may present. Basically, thetasks of machine learning vary on their levels of difficulties, from simpletasks such as arithmetic computations to even more complex ones like classifying DNA expressions or image segmentations. Furthermore, machine learningmodels are majorly aimed at helping the decision-making process of humans. A robust machine learning technique is smart in identifying the most suitable models from an observed dataset[9].

The achievement of these tasks all-together is a very challenging issue to deal with in the natural phenomenon in a real world domain, this is due to the possibility of uncertainty in the representation of natural languages used in representing the dataset. Therefore, identification of the most accurate or most suitable model in decision-making and for anytypical machine-learning problem is not easily attainable due to many uncertain future data that are yet unseen. For instance, to ascertain that a linear regression would be the best model to classify allunobserved data sample in a supervised learning task or a neural network would be better is an uncertain task. If peradventure we were able to determine that a neural network model will be the most appropriate for the task, then another uncertain situation would be deciding what number of layers will be best fitted for training the data.

IV. PROPOSED PROBABILISTIC MODEL FOR PREDICTIONS

Probability is a very useful mathematical technique in representing uncertainties in unseen data of a particular model. The uncertainties could be as a result of noisiness in a data, mix-structured data, outliers or uncleanliness of data. With probability, the uncertainties in the data can be effectively measured and the unobserved data could be inferred given the observed data.

Based on the known definition of probability as the ratio of occurrences of favorable outcomes of an event and the total number of equally likely occurrences of the event [8]. The proposed probabilistic model is defined as follow:

$$P(m_A) = \frac{m_A}{M}.$$

$m_A$represents the number of occurrences of a particular machine learning model A as the most accurate/suitable model, while M represents the total number of suitable machine learning models for a particular dataset.

Now, having known the probabilities of each suitable machine learning models for a given machine learning problem, the future prediction can be modelled as:

$$\hat{y} = \max [P(m_A)].$$

Where $\hat{y}$is the predicted outcome,which represents the model with the maximum of probability among the entire equally suitable model for the given machine learning problem.

V. CONCLUSION

The worldis living in the era of "Big Data" where digital devices are generating massive data content in rapidly growing velocity. This is making data availability very abundant and is inspiring the rapid motivation of making digital componentssmart and intelligent to the extent that device could learn itself through the same data it is producing. However, there is a high possibility of uncertainties in these data; this could be due to some errors in the form of noises or omissionwhen recording or representing the data. Furthermore, during the prediction phase of a machine-learning model, there could also be prevalence of uncertainties,since it might be very difficult to ascertain what model among many equally suitable models in any category of machine learning would give the most desired prediction to all the future unseen data.

To address this problem, investigative research on how probability theories could be used to optimize machine-learning's decision making when there are possibilities of uncertainties.

Thisresearch proposed a probabilistic model for predicting the machine learning model with the most accurate outcome among all other suitable machine learning models for a particular problem. The paper can also serve as a technical guide for a future work to dig more into the area of machine learning optimization.

REFERENCES

[1] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, New Jersey: Prentice-Hall, Englewood Ciffs, 1995.

[2] A. Kendall, V. Badrinarayanan and R. Cipolla, "Bayesian segnet: Model uncertainty in deep convolutional encodering applied to fall prevention assist by autonomous mobile robots in the hospital," *Big Data and Cognitive Computing,* vol. 2, no. 2, p. 13, 2018.

[3] M. Usama, J. Qadir, A. Raza, H. Arif, K.-L. A. Yau, Y. Elkatib, A. Hussain and A. Al-fuqaha, "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," *IEEE Access,* vol. 7, pp. 65579-65615, 2019.

[4] K. P. Murphy, Machine learning: a probabilistic perspective, MIT Press, 2012.

[5] A. Kendall and Y. Gal, "What uncertainties do we need in bayesian deep learning for computer vision?," *Advances in neural information processing systems,* p. 5574–5584, 2017.

[6] M. Kampffmeyer, A. B. Salberg and R. Jenssen, "Semantic segmentation of small objects and modeling of uncertainty in urban remote sensing images using deep convolutional neural networks," in *IEEE conference on computer vision and pattern recognition workshops*, 2016.

[7] R. Tanno, D. E. Worrall, A. Ghosh, E. Kaden, S. N. Sotiropoulos, A. Criminisi and D. C. Alexander, "Bayesian image quality transfer with cnns: exploring uncertainty in dmri super-resolution.," in *International Conference on Medical Image Computing and Computer-Assisted Intervention*, 2017.

[8] M. Jordan, Z. Ghahramani, T. Jaakkola and L. Saul, "An introduction to variational methods in graphical models," *Machine Learning,* vol. 37, pp. 183-233, 1999.

[9] C. Ning and F. You, ""Data-Driven Adaptive Nested Robust Optimization: General Modeling Framework and Efficient Computational Algorithm for Decision Making Under Uncertainty," *AIChE Journal,* vol. 63, pp. 3790-3817, 2017.

An Approach to Cybersecurity of Information Systems in Smart Organizations

Bukhari Badamasi, Ago K. MacGranaky Quaye, Longe Babatope Olumide, Auwal Alhassan Tata
School of Information Systems and Computing
American University of Nigeria
Yola, Nigeria
bukhari.badamasi@aun.edu.ng, aquaye@aun.edu.ng, olumide.longe@aun.edu.ng, auwal.tata@aun.edu.ng

***Abstract*—In smart organizations, the security of the information systems is important. In the last decade, cybercrime has taken on various forms due to advancements in technology. In fact, as criminal activities tend to flourish in organizations where cybercriminals exploit opportunities to participate in acts that endanger global security. It is therefore equally important for organizations, especially smart organizations, been the most vulnerable to have a good security posture in order to improve their comprehensiveness by adopting a strong approach to cybersecurity. When it comes to protecting organizational data, the human dimension (administrative approach to cybersecurity) is mostly silent. As such, this work aims to tackle smart organizations by taking a systematic approach to delivering and sustaining the security culture using a decision model of cybersecurity.**

Keywords—Cybersecurity, decision-model, Smart organizations

I. INTRODUCTION

Digital technologies have diffused organizations, and organizations have received computerized advances in recent times. Computerized advances are changing organizations into smart organizations [1]. Smart organizations are organized, knowledge-driven, and research-intensive organizations [2]. The most profitable, productive, the most successful and respected organizations are considered to be smart organization. For example, many of the Fortune 500 firms are classified as intelligent and smart, because they need a networked environment to thrive and survive. Digital technologies have increased productivity [3], employee engagement, high turnover, high profitability, strengthened customer relations and customer satisfaction [4].

Cybersecurity challenges in the context of cybercrime are never the less a persistent issue for smart organizations [5]. Via loss of customers, monetary loss, humiliation, reputational harm, and litigation, organizations suffer each year from setback. Many of the digitally related organizations, such as the telecommunications industries [6], Microsoft Inc. [7], FBI [8] and other smart organizations, each of the them were compromised resulting in loss of customer interest and litigations, reputational damage, or financial losses.

Researchers nowadays, focuses more on the technical security control measures in curtailing cybersecurity challenges in most organizations while leaving the human aspect of silence. However, a holistic approach to cybersecurity would be considered in this study in reducing cybersecurity challenges in smart organizations. In a holistic approach, both technical and administrative approach considers acceptable measures in reducing cybersecurity challenges in smart organizations.

II. LITERATURE REVIEW

A. Cybersecurity

Cybersecurity is the method of integrating information, technologies, and procedures to protect the operating system from digital attacks within the entire organizations. Cybersecurity, according to Fritzvold [9] is a method of protecting information, information systems, individuals and the whole organizations from being harm or targeted by cybercriminals. This claimed that the basic requirements of protection are "integrity, reliability, availability, usefulness, confidentiality, and possession" Rees, *et al.* [10, p. 3]. Lichtenstein [11] defined security as a framework that provides multiple policies, security education, security management, and a variety of security mechanisms used on the organizational network to attain a common purpose. According to Businge, *et al*. [12], the purpose of protection is not only to protect organizational information, but also to protect different departments of the organization's information systems such as hardware and software. Safety and security supports organization in many ways by choosing and implementing protection mechanisms to secure their physical assets and financial liabilities, as well as other tangible and intangible properties. Therefore, cybersecurity has certainly gained global recognition in recent years, resulting in a possible gain if it is implemented on an organizational network.

Nader, Carsten, Tim, and Rossouw [13] in their paper titled; "motivation and opportunity based model to reduce information security in organizations" stated that greater attention should be given to factors that pose management challenges to cybercrime. Such challenges include employee engagement, recognizing and classifying environmental factors with respect to threats, psychological factors, and adequate training and employee knowledge on information security.

Despite the progression of cybersecurity, however, the question remains of unauthorized access to corporate information and information systems. Three approaches to security of the information systems are evident in smart organizations, though. Such approaches include technological security, socio-technical security and cybersecurity behavioural approach. The Technological protection approach applies to the use of access control systems and eliminates the unauthorized use of sensitive data across a network within a physical framework [14]. According to Sobell [15], the variety of technical security

controls is far-reaching and includes numerous technologies such as file integrity auditing software, encryption methods, network authentication, smart card use, minutiae use, and use of access control list.

A socio-technical strategy is a structured approach applied on a complex network of organizations. This acknowledges on-the-job experiences between people and technology. Ashenden [16] notes that the socio-technical approach is the relationship between the dynamic structures of society and human actions. The Socio-technical approach is an ongoing authentication of applications based on user behaviour analysis, by leveraging numerous input signals or pieces of evidence that involve soft biometrics such as keystroke dynamics, and contextual factors such as the particular service being used, the computer used to access certain services, and user locations. Sittig and Singh [17] in their study claimed that the most successful method of minimizing, preventing and recovering from any form of attack in complex and/or smart organizations is the socio-technical approach.

The behavioral strategy consists of designing and applying organizational network security policies. Bulgurcu, et al. [18] described security policy as "a description of employees' roles and responsibilities in safeguarding their organization's information and technology resources". While policies are known as weak in some organizations, Brown and Zafar [19] claimed that violation of an organization's policies is what makes it weak, but if employees completely comply with the policies given, protection of information systems in smart organizations will be achieved.

Samiksh [20], identified basic approaches to smart organizations information systems. Samiksh [20] further added that organizations need to ensure successful program and resource protection. Thereafter, it is important to recognize that ideal protection is not only offered, but that it must be accomplished for the entities to be maintained in order to meet the purposes they have been acquired and covered.

Many organizations today have introduced mobile device encryption, automatic disabling of BlueTooth features on mobile devices, control access to corporate networks, identity and access management, control of company network access, data loss prevention (DLP) technology, use of DMZ network, secure socket layer (SSL), use of Mikrotic software, Cyberoam as well as use of complete AAA [21]. Although other organizations promote international collaboration, policy, awareness raising, capacity for law enforcement, capacity for criminal justice and public-private partnership [22]. This approach has the benefit of exploiting trusted resources and creating an economic context. Sadly, damages that affects most 21st century smart organizations has yet to be overcome. Nevertheless, there is a compelling need to explore certain facets of cybersecurity, and how cybersecurity issues in smart organizations can be curtailed.

Moreover, a framework by Lichtenstein [11] was developed as a guide to reduce cybersecurity challenges in the organizations. The framework depicted in Figure 1 provides a guide for defining Internet-related threats, which are then applied to the other threats faced by the organization.

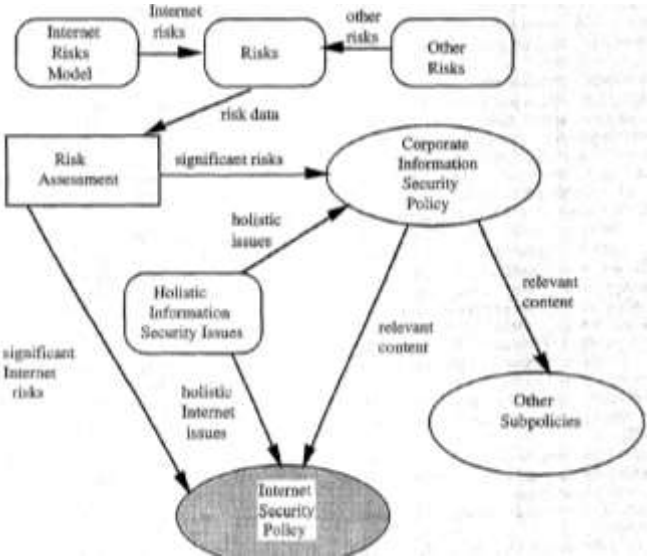


Figure 1. Framework for developing a user organization's Internet Security Policy. Source: Lichtenstein [11]

The effective deployment of the Internet protection policy as provided in Figure 1, serve as an approach to curtail cybersecurity challenges in smart organizations.

B. Concepts of Cyber Security

Organizations face various kinds of risks that vary from physical to virtual caused as a challenge of cybersecurity. In the field of computing, cybersecurity has specific description and principles. As Wamala [23] has said, it involves cyber threats in the form of breach of the organizational security posture. Wamala [23] also noted that cyber threats are a possible violation of the organization's information security infrastructure and assets. Accidental attacks are another cybersecurity term that happens without purpose. Accidental threats only happen without predetermine intent. Accidental threats is another concept of cybersecurity that happens without intention. The idea of threats typically occurs due to malfunction of device software or failure of the physical system. Data vulnerability is another intruder-caused concept in cybersecurity and it is intentional action against organizational properties. Another term of cybersecurity is active threat. Active threat occurs due to certain system operational changes, such as alteration or physical equipment malfunction. Passive threat is regarded as a concept of cybersecurity. It is a threat that does not require a change in equipment quality, it just cleans information from a device without affecting the system itself [24]. Wamala [23] identified the source threat as the concept of cybersecurity that could stand as an entity that wants a compromise to take place.

In the literature, researchers highlights the existing approach to beat cybersecurity challenges in smart organizations. A number of the approaches include technical security control measures like using strong antivirus software, controlling access to information systems, use of firewall, Mickrotic server, encryption method, and use of passwords. However, the objective of this study is to provide a holistic approach that comprises of technical and administrative security control measures to safeguard smart organizations.

III. Problem Statement

Organizations are saddled with a tremendous amount of data and information, subsequently; smart organizations attempt to solve the issue of protection of the information system. Smart organizations are digitally in nature and networked world that improved organizational working conditions and productivity [25]. In 2019, cybercriminal breached Microsoft's network, where the simple codes were accessed [3]. The risk of accessing the basic codes, according to the study, is that malicious hackers might write new viruses of other programs based on undisclosed vulnerabilities in the code and spread them to other organizational networks.

Similarly, in recent years, schools, universities, and other educational institutions have been facing cybersecurity challenges. American University of Nigeria got hacked in 2019. Mr. Murtala Abdul claimed that a student at the University infringed the security protocols and manipulated the outcomes of their tests and exams, according to a study by the Acting Director of the University's ICT. Likewise, due to inadequate implementation of security measures or non-use of a systematic approach to cybersecurity, several vulnerabilities were also infiltrated by cybercriminals [26]. Records of 300,000 students and faculty at the University of Maryland were hacked. Within the stolen documents are information about staff, and personal information about students. According to the Newspaper of the University of Maryland (i.e. Diamondback), "The database accessed included information about everyone who has obtained a university ID from the campuses of College Park or Shady Grove since 1998." Also hacked was the University of North Dakota where a server that held nearly 350,000 staff and students personal information was compromised. Likewise, hackers at Butler University secretly accessed the network, and about 200,000 student and faculty members' records were revealed. Names of graduates, social security number (SSN), bank data, date of birth, and licenses are among the information that has been hacked at the University. Indiana University has suffered a data breach, in which around 146,000 students and employees personal information were exposed The data breach leads to the names, emails, and social security numbers of the students being revealed. The data breach cost about one hundred and thirty thousand US dollars ($130,000) to the University. [26].

Financial organizations sometimes known as smart organizations. Owing to the emergence of new forms to aid payment system, such methods support technologies such as artificial intelligence, the Internet of Things (IoT), the Internet of Everything (IoE), the blockchain, and Near Field Communication (NFC). In particular, cybercriminals use devices such as NetWire, DarkComet, LumonosityLink, NanoCore, Remcos and Imminent Monitor to remotely access compromising networks by recording keystrokes, tracking webcams, accessing network resources and providing remote desktop connections. [27]. Mallick [27] added that cyber-attacks cost Nigeria sum of $649 million annually in organizations. The way organizations handle security in their respective networks is obstinate. The areas that scholars put greater focus on protecting organizational information systems are geared towards technological security controls. In the meantime, much has been done on technological security monitoring, although scholars are silent directly on the human dimension of the employees in smart organizations. As such, this research focuses on both the technological and human (administrative) dimensions of information system security in smart organizations.

IV. Methodology

The concept of cybersecurity cannot be overemphasized. Different methodologies have been implemented to secure the organizational network but cybercrime is still on the rise. In this study, a model is proposed as depicted in Figure 1, to reduce cybersecurity challenges. Failure to fully deploy and use the model will render organization useless and that will lead to cybercrime in organizations.

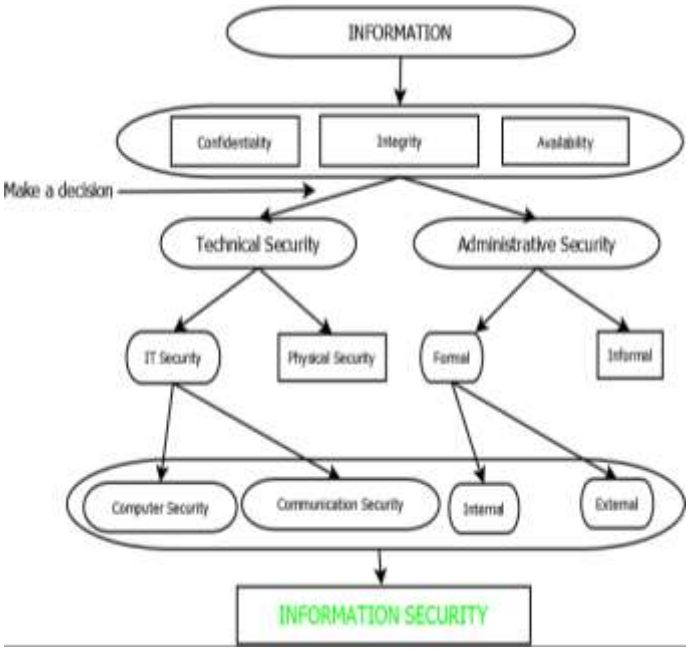


Figure 2: A Security Model for Smart Organizations

That organization's success depends primarily on the end design that such organizations are to accomplish. Organizations' strategic readiness to provide coherent security measures to ensure the safety of information resource, safeguard critical information systems and organizational presence in cyberspace would create a secure cyber community that forms a smart organization [28].

"Information" is shown as un-secure in Figure 2, as it has not yet full-filled any of the three information security characteristics. Smart organizations must use both technical and managerial methods for the three characteristics (confidentiality, integrity, and availability) to be completely achieved. Further subdividing the technical approach into IT security and physical security. though the adinistrative approach can be formal or informal. Therefore, to truly secure smart organizations and solve the challenges of cybersecurity, it has to follow all four requrements. Such requirements include computer security, communication security, physical security and administrative security. after implementation of these security measures, smart organizations can be completely securitres and safe from any adversaries inside or outside the organizations.

V. Conclusion

In the past decade, cybercrime has taken shape due to technical advancements in smart organizations. While the usage of digital technology in organizations continues to grow, cybercriminals are exploiting incentives to participate in activities that endanger global security with these

technology. Hence it is equally important for organizations to have effective and comprehensive protection stands to curtail cybersecurity challenges, particularly in smart organizations been the most vulnerable. In this study, a proposed and comprehensive approach to cybersecurity towards the provision and maintenance of security culture in smart organizations was presented, focusing primarily on smart organizations. It is because smart organizations are directly or indirectly regards information as their principal asset. Significant value effort to systematic approach and a more comprehensive investigation is needed.

This study indicates that management in smart organizations should pay attention to the administrative approach in their respective organizations, or that both approaches should be considered (technical and administrative). This study demonstrates how important it is to merge the holistic approaches component of cybersecurity within smart organizations.

It is recommended that smart organizations review and update IT security policies, provides quality assurance and audit of IT-related facilities on the authorized environment regularly, perform environmental application testing before moving to the live environment, improve IT security management procedures, develop and enforce security awareness software, continuously checks a network for faults, find and close any unused open port. Unless these problems are handled properly, the cybercrime rate would drastically decrease, and the safety challenges in the smart organization will be address.

VI. ACKNOWLEDGMENT

The authors would like to thank Mal. Aliyu Garba of the department of Computer Science, Ahmadu Bello University, Zaria for his helpful comments and observations.

VII. REFERENCES

[1] A. Shibeika and C. Harty, "Diffusion of digital innovation in construction: a case study of a UK engineering firm," Construction management and economics, vol. 33, pp. 453-466, 2015.

[2] S. Rybalko and T. Seltzer, "Dialogic communication in 140 characters or less: How Fortune 500 companies engage stakeholders using Twitter," Public relations review, vol. 36, pp. 336-341, 2010.

[3] C. McAfee, "Net losses: Estimating the global cost of cybercrime," Technical report, McAfee and the Center for Strategic and International Studies2018.

[4] D. Rigby and B. Bilodeau, "Management tools & trends 2011," Bain & Company Inc, 2011.

[5] J. Chapman, "How safe is your data? Cyber-security in higher education," Higher Education Policy Institute Policy, 2019.

[6] G. Naveen. (2020, 12/04/2020). Telecommunication Companies across the world are hacked. Available: https://www.cybersecurity-insiders.com/telecommunication-companies-across-the-world-are-hacked/

[7] J. Scambray and M. Shema, Hacking Exposed Web App: Tata McGraw-Hill Education, 2006.

[8] K. Hagelberg, Wicked Akron: Tales of Rumrunners, Mobsters and Other Rubber City Rogues: Arcadia Publishing, 2010.

[9] E. Fritzvold, "Cyber Security in Organizations," University of Stavanger, Norway, 2017.

[10] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "PFIRES: a policy framework for information security," Communications of the ACM, vol. 46, pp. 101-106, 2003.

[11] S. Lichtenstein, "Developing Internet security policy for organizations," in Proceedings of the Thirtieth Hawaii International Conference on System Sciences, 1997, pp. 350-357.

[12] P. M. Businge, M. Kareyo, and Z. Muwanga, "ASSESSING THE IMPLEMENTATION OF INFORMATION SECURITY POLICY IN UGANDAN UNIVERSITIES," GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES, p. 7, 2016.

[13] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," Journal of information security and applications, vol. 40, pp. 247-257, 2018.

[14] F. Dalpiaz, E. Paja, and P. Giorgini, Security requirements engineering: designing secure socio-technical systems: MIT Press, 2016.

[15] M. G. Sobell, A Practical Guide to Fedora and Red Hat Enterprise Linux: Pearson Education, 2013.

[16] D. Ashenden, "Information Security management: A human challenge?," Information security technical report, vol. 13, pp. 195-201, 2008.

[17] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," Applied clinical informatics, vol. 7, pp. 624-632, 2016.

[18] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," MIS quarterly, vol. 34, pp. 523-548, 2010.

[19] D. Brown and H. Zafar, "Information Security Policy Quality and Enforcement: Is Compliance a Solution to Fraud," 2017.

[20] S. Samiksh, "Basic Security Approaches towards Information Technology Systems," 2020.

[21] M. Souppaya and K. Scarfone, "Guidelines for managing the security of mobile devices in the enterprise," NIST special publication, vol. 800, p. 124, 2013.

[22] T. K. Yerjanov, Z. M. Baimagambetova, A. M. Seralieva, Z. Zhailau, and Z. T. Sairambaeva, "Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan," Journal of Advanced Research in Law and Economics, vol. 8, pp. 2286-2301, 2017.

[23] F. Wamala, "ITU national cybersecurity strategy guide," International Telecommunications Union, vol. 11, 2011.

[24] A. AlKalbani, H. Deng, B. Kam, and X. Zhang, "Information Security compliance in organizations: an institutional perspective," Data and Information Management, vol. 1, pp. 104-114, 2017.

[25] E. Brynjolfsson and A. McAfee, Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy: Brynjolfsson and McAfee, 2012.

[26] W. Colin, "Phishing attack exposes personal information," 2020.

[27] B. Mallick, "Cybersecurity Challenges of the Nigerian FinTech Sector," 2019.

[28] O. Osho and A. D. Onoja, "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis," International Journal of Cyber Criminology, vol. 9, 2015.

A Generalized Security Policy for Rural Community Networks

Auwal Alhassan Tata, Longe Babatope Olumide, Ago K. Macgranaky Quaye, Bukhari Badamasi
School of Information Technology and Computing
American University of Nigeria,
Yola Nigeria
Auwal.tata@aun.edu.ng, olumide.longe@aun.edu.ng, aquaye@aun.edu.ng, bukhari.badamasi@aun.edu.ng

Abstract **Community Networks (CN) are being sponsored across rural communities in Africa under an implement and hand over scheme. This leaves the management of the network and in particular the security of the network under the management of an ill experienced team of management steering committee. Most drafts on security policies are presented in an advanced manner beyond the comprehension of rural communities. This is a technical paper that attempts to develop a generalized security policy based on a simple frame work for adoption by rural CNs. The CNs can begin to build upon it as they gather experience and more education from the management of their network.**

Keywords: Community Networks(CN), Security Policy, Security Framework, PFIRES

I. INTRODUCTION

Despite the progress achieved in connecting half of the world population in just about a decade, more effort is necessary in order to continue connecting the next billion to further address global digital divide. Interestingly enough, most of the 3.5 billion Internet user are concentrated in the urban areas[1]. This informed the major players of the world in the Internet realm to push for the extension of Internet services in the rural communities. The major providers of Internet services in the African continent are the commercial mobile telecommunication industries. Being a commercial venture, they hardly provide broadband services to rural communities due to its non-financial viability [2]. This prompted the campaign for the establishment of rural community networks for the under-served or not served communities of Africa.

The current global rise in cybercrime has underscored the need for massive global effort towards mitigating its effect. This is even more precarious in Africa where illiteracy, poverty and lots of other socio-economic challenges make it even more difficult to mitigate effects of cybercrime. Consequently, Africa needs to rise up to the challenges of cyber security so as to forestall being easy target or being used as a gateway to attack other parts of the world. With the recent proliferation of community networks across several underserved and not-served regions of Africa, the security risk becomes even higher.

This technical paper proposes a security policy that takes into account the peculiarities of CNs in rural Africa such as illiteracy, low level of security awareness and socio-cultural peculiarities. It starts by reviewing the emergence, advancement and adoption of security frameworks in diverse localities. It then goes on to adopt the Policy Framework for Interpreting Risk in E-Business Security (PFIRES) [3] in creating a generalized security policy that can be used by rural CNs in Africa. PFIRES exhibit just four component as illustrated in "Fig. 1" in its security framework thereby reducing the complexity associated with other security frameworks and thus eases its adoption especially by a network largely administered by rural dwellers.

II. RELATED WORK

The ability of the world to maintain a safe and secured computing infrastructure for storage, managing and transfer has been extremely challenging. This is occasioned by the paradigm shift from proprietary networks to an open, distributed and heterogeneous setup of the new Internet architecture [4]. This has resulted in several initiatives to come up with policy frameworks to mitigate the resulting security challenges. Some of these initiatives started as far back as the birth of Transmission Control Protocol/Internet Protocol (TCP/IP) [5] and some quite recent [6]. Policies are derivatives of management goal which defines the behaviour of distributed heterogeneous systems, applications and networks [7]. More specifically information security framework provides a well laid out and comprehensive security strategy and solutions to security challenges in relation to the business objectives of an organization [4]. It attempts to maintain network and system availability, improving performance, enhancing security while bringing down operating overhead thus reducing the total cost of ownership of Information and

Communications Technology (ICT) infrastructure [7]. Reference [8] did an excellent work in creating a security policy framework in the African context. However it was targeted at African cyber security agencies and associated regulatory bodies for the promotion of cyber security awareness. Rural dwellers such as rural CN management team will find it difficult to comprehend. Another work by [4] x-rayed best practices in the formulation of security policy for e-commerce. The framework code named METASeS Information Security Framework incorporated five concepts; risk management, hierarchical policy structure, guideline definition, threat and vulnerability policies and their interpretations. The model however present complexities that might be difficult to adopt by rural CNs. Not all security policy frameworks were implemented using models alone. The work of [9] implemented its security policies using firewall rules. They then went further to define hierarchies to distribute policy specification over several security components along the hierarchy. Similarly [10] presented a complex ACL based security framework which analysed the security implementations in a network by comparing it with the security policy of the organization to establish the level of compliance. This however is way beyond the comprehension of the management team of an African rural community network. Policy Framework for Interpreting Risk in E-Business Security (PFIRES) is a creation of [3]. It was initially designed to tackle e-commerce activities and later on expanded to include all types of organizations dealing in computing and Internet operations. It presents information that provides useable security policy and strategy for implementations done in line with ICT development life cycle. All of these align with the core security need of rural Africa CNs resulting in its adoption as the framework of choice. Additional knowledge was extracted from the patent US 9,571,524 B2 [11] for the generation of the controls for the policy framework.

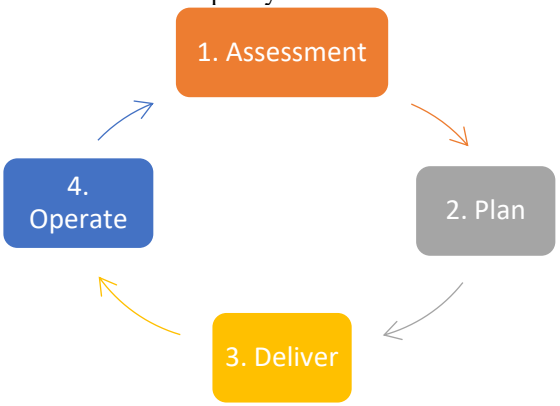


FIG.1 PFIRES Life Cycle Model [3]

III. METHODOLOGY

As mentioned in the introduction, PFIRES life-cycle is adopted as the framework of choice because of its simplicity and ease of comprehension occasioned by its small number of components. Each component is now developed into an aspect of the security policy.

A. *The Assessment Stage:*

This is the first component of PFIRES comprising of two sub stages; the policy assessment and risk management stages.

1) Policy Assessment Sub Stage: Since this is the maiden version of the policy, the policy assessment simply comes up with strategic security policy statement that defines management overall goal. For the CN, the strategy is to ensure that rural dwellers make use of the services implemented for communication, information dissemination, education and business. The infrastructure should not only afford them the opportunity of accessing the world but also allow them advertise their local content to the world for better financial gains in a secured manner.

2) Risk Assessment Sub Stage: Identification of business assets as well as their associated threats is done in this stage. To ease this process, a schematic diagram of the CN is drawn in “Fig. 2”

For simplicity, the risk assessment is presented in Table 1.

B. *Plan Stage:*

This is the second component. It involves creating and defining the policy for protecting the identified assets. It is composed of two sub stages; policy development and requirement definition sub stages.

1) The Policy Development Sub Stage creates and update security strategy for securing identified assets in line with defined policy of the company. Thus the security strategy will be created in relation to each asset as follows:

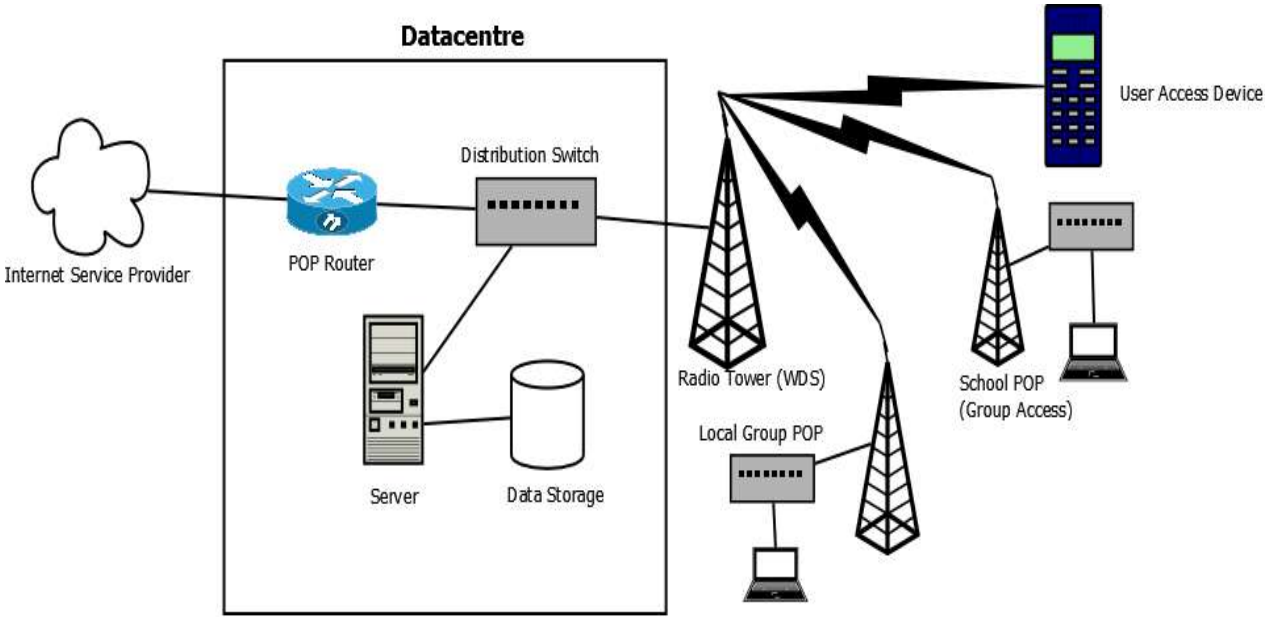


Fig. 2 Schematic diagram of a typical rural CN

TABLE 1: RISK ASSESSMENT ANALYSIS

S/N	Business Asset	Function	Classification	Potential Threats/ Vulnerability	Mitigation
1	The Servers	Store and run all software for services provisioning. Stores non-DB data.	High Risk	If compromised can lead to compromise in sensitive data	Physical and Software security
2.	Database (DB)	Handles all DB	High Risk	If compromised can lead to compromise in sensitive data	Physical and Software Security
3	Distribution Switches	Link up several nodes to the network	High Risk	MAC Address spoofing, Traffic Sniffing	Physical and Software Security
4	Point of Presence (POP) Router	Link up the network of the Internet Service Provider (ISP) to the Local Area Network (LAN) of the (CN)	High Risk	Sniffing Attack	Software Security
5	Wireless Distribution System (WDS)	Extends the link from the ports of the switch to access devices wirelessly.	Medium Risk	Sniffing Attack	Software Security
6.	Access Devices	Used by end users to access services provided within and outside the CN	Medium Risk	Denial of Service Attacks(DOD) Identity Theft Malware attack Data theft	Software Security

i. The Data Centre

a. The building housing the servers and all critical equipment needs to be secured and monitored all the time.
b. Access to the building should be regulated with a concise register for keeping records of access to the building.

ii. The Server

a. Access to the server needs to be authenticated.
b. A proper monitoring of entry and entry attempt into the server must be kept with a log of activities performed.
c. The entire storage needs to be strongly encrypted.

d. Only genuine licenced software should be installed on the server and must be updated as at when due.

iii. The Databases

a. Access to the databases must have additional need for authentication.
b. The data therein must be strongly encrypted.

iv. The Distribution Switches:

a. All unused component must be disabled to prevent attacker from taking advantage of such components.
b. The underlying software that drives the switch must be regularly updated as at when due.
c. Appropriate monitoring tool must be employed for keeping a log of activities on the switches.

v. Point Of Presence (POP) Router:

a. Access to the router must be authenticated.
b. A proper monitoring of activities on the router must be kept for all times.
c. All software on the router must be licenced and updated regularly as at when due.
d. Remote access to the router must use secure and encrypted line.

vi. Wireless Distribution System (WDS):

a. Access to the WDS must be authenticated
b. Proper monitoring of activities on the WDS must be kept at all times.
c. All software driving the WDS must be updated regularly as at when due.

vii. Access Devices:

a. All access devices must be registered on the CN
b. Activities from any access device must be monitored at all times.
c. All software for accessing services on the access devices must be genuine and updated regularly.
d. There must be a strategic awareness campaign to educate members of the community on how best to utilize the system in a secured manner.

2) The Requirement Definition Sub Stage analyses the developed security policy and comes up with the required security infrastructure necessary to implement the policy. In this regards, the requirement definition is developed as listed:

i. The building of the Data Centre (DC) must be locked with physical lock. Only the head of the technical crew and whoever is delegated within the crew will be allowed inside the building.
ii. For monitoring access to the DC, Close Circuit Television (CCTV) system will be deployed to cover the building. All access must be recorded and backed up remotely.
iii. All authentications to devices must be via strong passwords
iv. All encryptions must use strong encryption algorithm that cannot be easily cracked by unauthorized person.
v. To minimize cost, one server will be used and virtualization technology be deployed to abstract all required servers. All virtual systems will be backed up to a cloud storage.
vi. Only licenced interoperable operating systems such as Microsoft operating systems and Linux operating systems will be used as appropriately for any system deployment. The technical crew will decide which is suitable for each system deployment.
vii. For the routers and switches, only products of blue-chip companies that support interoperability such as CISCO, Mikrotic, HP etc. will be used and their monitoring capabilities will be used to log usage information.
viii. Traffic between the CN infrastructure and the Internet Service Provider (ISP) must be filtered to bar unwanted traffic from entering the network.
ix. All logs must be backed up and analysed annually for policy evaluation.
x. All new users must enrol into a recurring training programme on best practices in a CN

C. *The Deliver Stage:*

This stage identifies the control necessary for the implementation of each line item of the requirement definition. This is achieved from the designed infrastructure. The resulting system is then evaluated to avoid duplications in requirements. The resulting controls are then implemented and tested. Usually there should be pilot testing especially in a situation where there exist an old policy item that is about to be changed or upgraded. However, this policy is for a fresh implementation. So the pilot implementation will take the form of using test users to ascertain the level of compliance to the policy statements. Once successful, the system will be rolled out fully.

1) Control Definition and Implementation

i. All members of the CN steering committee will be identified with badges that clearly define their level of privilege in the CN infrastructure.

ii. There must be a minimum of two CCTV cameras at the vicinity of the DC. One must be positioned inside the building and directed at the equipment inside and the other positioned outside monitoring the movement in and out of the premises.
iii. The keys to the door of the CN must be kept by an assigned door keeper who also keeps a book register for all sign-ins and sign-outs.
iv. Simple Network Management Protocol; the protocol that monitors device utilization and their health status, will be activated on the server and all network devices. Nagios; a software that collects, analyses and presents activity log data in graphical form for easy understanding will be deployed.
v. All passwords must be a minimum of eight characters long and must contain a combination of uppercase and lowercase letters, special symbol and numbers.
vi. All passwords must be changed every three months and must be totally different from previous password.
vii. Only Rivest, Shamir, and Adleman (RSA) algorithm can be used in all encryption requirement.
viii. Proxmox virtualization software will be the host platform for all virtual machines. It must be set to automatically install security updates.
ix. All operating systems must be set to automatically install security updates.
x. The operating systems should be configured to keep a log of all activities for troubleshooting purposes in the event of failure.
xi. Back-up of the virtual machines should be made incrementally every night and a full back-up every month. These should be uploaded to the cloud account from 00:00hours after the last back-up.
xii. The firewall functionality of the router should be configured to block all unwanted traffic from the Internet to the CN.
xiii. A training schedule should be prepared for training the community on best practices and recruitment of young promising members of the community to ensure knowledge transfer on every town hall meeting day.
xiv. On every last Saturday of the month, there should be held a monthly CN security steering committee meeting to assess the progress and security challenges of the CN.

D. *The Operate Stage:*

This is a recurring stage that continues to monitor the controls on a daily basis for the security assessment and incidence handling. In this stage all monitoring tools put in place are constantly being watched for any sign of security breach.

The Operate stage is handled in the CN by making available a graphical illustration of the situation report of the various controls setup on the CN system. All members of the technical crew should have access to this illustration via mobile device.

At the end of the year, a security meeting will be held to analyse incidences and the efficiency of the adopted mitigation strategies at combating threats and ascertain if the entire PFIRES process will be invoked again for possible upgrade.

IV. CONCLUSION

This technical paper has succeeded in creating a security policy that can be adopted by rural CNs across Africa and other under-served/not-served communities. It presents the basic security implementations required by CNs to become secured. As time goes by, the security team will begin to gather more knowledge about innovations in security affording them the opportunity to further enhance the security of the CN

REFERENCE

[1] Navarro, L., *An IGF2016 report: notes and links around community networking.* 2016.

[2] Williams, I., M. Falch, and R. Tadayoni, *A Public Management Framework for wireless broadband development in rural Sub-Saharan Africa.* Marketing i Zarządzanie, 2017. **50**: p. 89-116.

[3] Rees, J., S. Bandyopadhyay, and E.H. Spafford, *PFIRES: a policy framework for information security.* Communications of the ACM, 2003. **46**(7): p. 101-106.

[4] Palmer, M.E., R. Craig, P.C. Jody, and M.P. Edward, *Information Security Policy Framework: Best Practices for Security Policy in the E-commerce Age.* Information Systems Security, 2001. **10**(2): p. 1-15.

[5] McHugh, J. and A.P. Moore. *A security policy and formal top level specification for a multi-level secure local area network*. in *1986 IEEE Symposium on Security and Privacy*. 1986. IEEE.

[6] Moody, G.D., M. Siponen, and S. Pahnila, *Toward a unified model of information security policy compliance.* MIS quarterly, 2018. **42**(1).

[7] Wies, R. *Using a classification of management policies for policy specification and policy transformation*. in *International Symposium on Integrated Network Management*. 1995. Springer.

[8] Dlamini, I., B. Taute, and J. Radebe, *Framework for an African policy towards creating cyber security awareness*. 2011.

[9] Cuppens, F., C. Nora, S. Thiery, and M. Alexandre, *A formal approach to specify and deploy a network security policy*. in *IFIP World Computer Congress, TC 1*. 2004. Springer.

[10] Bera, P., S.K. Ghosh, and P. Dasgupta, *Policy based security analysis in enterprise networks: A formal approach.* IEEE Transactions on Network and Service Management, 2010. **7**(4): p. 231-243.

[11] Dotan, Y., C. Duane, and D. Knjazihhin, *Creation of security policy templates and security policies based on the templates*. 2017, Google Patents.

5G Network and COVID-19: Ignorance and the Conspiracy of Truth

Nwakamma Mary Nkechinyere
Department of Electrical Electronics Engineering
Federal Polytechnic Nekede,
Owerri, Nigeria.
marygerrynwakamma@gmail.com

Uchenna Obioma Nwogu
Department of Electrical Electronics Engineering
Federal Polytechnic Nekede,
Owerri, Nigeria.
losengineering@yahoo.com

***Abstract*— Before the COVID-19 outbreak even began, 5G was being blamed for everything from cancer to infertility. The viral conspiracy theories typically only infected the usual tin-foil hat corners of the internet, but they have recently spread to the real world. Mixing unfounded 5G fears with the panic brought about by a global pandemic has seen people set Telecommunication towers on fire and harass broadband workers in the street. Some posts on social media claim that 5G's alleged impact is just the latest in a string of electromagnetic wave-induced pandemics. Despite the conspiracy theories surrounding 5G, this paper has created a contextual use case for 5G technology while presenting findings to debunk the connectedness of 5G and COVID-19. Furthermore, an adaptive architecture for 5G network optimized using radio access gateways for disruptive technologies is presented in this research.**

Keywords—5G, COVID-19, Emerging Technologies, Conspiracy Theory, IoT, Cloud Computing, AI, Big Data

I. INTRODUCTION

On December 1, 2018, South Korea became the first country to offer 5G technology [1]. Clearly, the mobile industry has made appreciable advances since the first mobile phone call was made back in 1973 [2]. Large-scale adoption began in 2019 and today virtually every telecommunication service provider in the developed world is upgrading its infrastructure to offer 5G functionality [2]. Also most countries plan to start adopting 5G in 2020 [3] and this is set to help drive the Internet of Things (IoT) [4], Big data [5], Cloud computing [6], AI [7] as well as other disruptive technologies [8]. A robust model is fully needed.

Granting that 5G and COVID-19 are now branded as global phenomena that became prominent in 2020, it however creates surprises to note all the conspiracy theories around the two concepts [9]. In fact, to understand 5G, it becomes pertinent to understand few abbreviations, viz: G stands for generation, so 5G is the fifth generation of wireless communications technologies supporting cellular data networks. 5G communication requires the use of communications devices (mostly mobile phones) designed to support the technology. 5G is similar to 4G, but it has much better speed, low latency and has capacity to take more users 10]. It has the capability to enhance the broadband we know today to do more, connect more people and devices and generate more revenue.

Hence, this technology is indeed super-fast and has a much smaller cell site than what we already know. And that is no surprise as the world seems to be going smaller, especially in the world of technology. Comparably, 5G is a unified platform that is more capable than 4G.

While most generations have technically been defined by their data transmission speeds, each has also been marked by a break in encoding methods, or "air interfaces," that make it incompatible with the previous generation such as 1G (analog cellular/voice), 2G technologies (digital voice), (such as CDMA, GSM, and TDMA). The first and second generation of digital cellular technologies paved way to 3G technologies (voice and mobile data). 3G evolution included EVDO, HSPA, and UMTS with speeds from 200kbps to a few megabits per second [11]. 4G technologies, such as WiMAX and LTE, were the next incompatible leap forward, and they are now scaling up to hundreds of megabits and even gigabit-level speeds.

Unlike the traditional 4G LTE, 5G operates on different spectrum bands, which is divided into high-band, mid-band, and low-band spectrum [12]. Low-band operates in frequencies below 2GHz. These are the oldest cellular and TV frequencies. These travel great distances, though there are no wide channels available, and many of those channels are being used for 4G. Low-band channels are from 5MHz in width up to 20MHz. As such, these are not roomier than 4G. Mid-band 5G is in the 2-10GHz range which is widely deployed and which covers most current cellular and Wi-Fi frequencies, as well as frequencies slightly above these. These networks have decent range from their towers, often about half a mile. As such, in most other countries; these are the workhorse networks carrying most 5G traffic.

Again, high-band spectrum often referred to as mmWave (millimeter wave) is the fastest, with actual speeds often being 1–2 Gbit/s down. Frequencies are above 24-GHz, reaching up to 72 GHz, which is above the extremely high frequency band's lower boundary. The reach is short, so more cells are required. Millimeter waves have difficulty traversing many walls and windows, so indoor coverage is limited.

For Nigerian public that is already jittery about computer viruses and 5G wireless cellular technologies, the coming of COVID-19, a complex and devastating global pandemic, perhaps manipulates fear in some people's minds. For instance, people are afraid of being attacked by pandemic viruses or malevolent cells—even the type associated with 5G cell phones. The fact is that there is no link-connectivity between the COVID-19 virus and 5G cell phone technology or 5G base-station communication towers. These are totally different constructs.

Till date, none of the conspiracy theories that made efforts to link 5G and the coronavirus make provides any logical sense scientifically. The electromagnetic radiation from 5G devices

and systems is not carrying the COVID-19 virus or any other microbe that humans can come into contact with or that infects anyone [9].

Recall, that even with current technological advances, the demand and performance challenges clearly vary immensely from the low to high bands. By design default or spectrum necessity, the bandwidth performance will be accomplished only by leapfrogging to the high-band 5G, 20GHz bandwidth. For biological matters, it is not obvious whether the biological responses to high-band 5G radiation will be akin to earlier generations or low-band 5G radiations, given the distinctive characteristics of mm-wave and its interaction with the complex structure and composition of pertinent biological tissues [9].

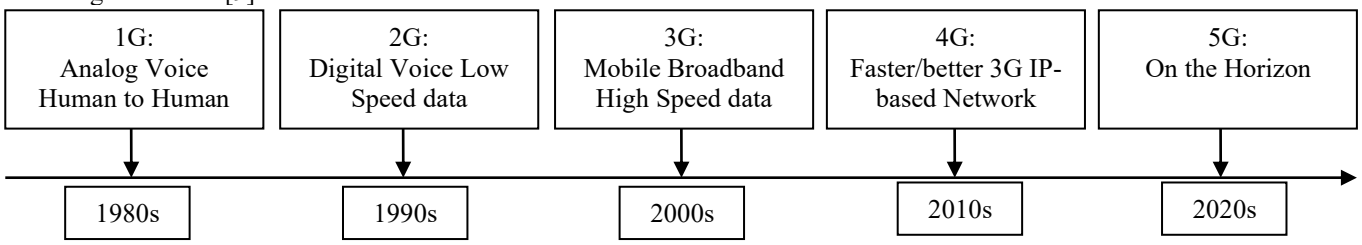


Figure 1. Dynamic 5G evolution.

In this paper, a perspective of radio access network (RAT) for 5G that encompasses frequency ranges from 3 to 60 GHz and beyond is considered. Also, a discussion on the merits of 5G technology was presented.

II. Related Research Efforts

In this section, a summary of instant literatures on 5G and COVID-19 myth is discussed while justifying a suitable 5G framework for driving disruptive technologies that can be used to combat COVID-19. In [9] various COVID-19 reports concerning the 5G rollout was discussed in the context of conspiracy theories. The work in [13] looked at the effect of COVID-19 on the world's economy while exploring disruptive technologies such as Internet of Things (IoT), Unmanned Aerial Vehicles (UAVs), Blockchain, Artificial Intelligence (AI), and 5G, etc to mitigate the impact of COVID-19 outbreak. Also, it is obvious that COVID-19 outbreak has attracted massive attention in [14]–[22]. Other representative literatures in 5G technologies were discussed in [23]–[30].

From these works, it is very clear that there is no functional relationship between COVID-19 and 5G technologies. However, it is clear that with 5G technologies, various use cases of COVID-19 applications can be achieved seamlessly. A conceptual framework for 5G architecture that will fix the following vertical industries will be widely accepted. These industries include: Automotive industry [31], aviation industry [32], tourism industry [33], oil industry, construction industry, food industry, healthcare industry, telecommunication industry [35], among others.

III. Proposed 5G architecture for disruptive integrations

In this paper, Figure 3 shows a feasible 5G network architecture for wireless and mobile networks interoperability needed for driving the previously highlighted disruptive technologies. The framework comprises user terminals including various isolated autonomous radio access technologies. Inside every of the terminals each of the radio access technologies is perceived as the IP link to the external world. A different radio is depicted for each Radio Access Technology (RAT) in the mobile terminal.

For instance, to deploy for RATs, there will be a need to have four different accesses (specific interfaces in the mobile terminal,) and to have all of them active simultaneously.

To activate the framework and make the architecture very operational, the first two OSI levels (data-link and physical levels) could be used to define the radio
access technologies. This can provide access to the Internet with optimal QoS support mechanisms. This is also dependent upon the access technology (e.g., 3G and WiMAX have explicit QoS support. The WLAN seems not be fully QoS compliant.

Across the OSI-1 and OSI-2 layers are the network layer which is IP (Internet Protocol) as designated in the Communication environment (IPv4 or IPv6) irrespective of the radio access technology. The IP is is used to support control data (in IP header) for proper routing of IP packets belonging to a certain application connections-sessions between client applications and servers somewhere on the Internet.

As shown in Figure 3, the 5G mobile network architecture application connections are realized between clients and servers in the internet via sockets. In the framework, Internet sockets are introduced. These are endpoints for data communication flows in the network. Each socket of the web is a unified and unique combination of local IP address and appropriate local transport communications port, target IP address and target appropriate communication port, and type of transport protocol. IoT and AI driven devices can leverage these functionalities to enhance system performance.

Considering that, the establishment of communication from end to end between the client and server, using the Internet protocol is necessary to raise the appropriate Internet socket uniquely determined by the application of the client and the server. This means that in case of interoperability between heterogeneous networks and for the vertical handover between the respective radio technologies, the local IP address and destination IP address should be fixed and unchanged. For a medical robot that runs on the Internet, putting these parameters will ensure effective handover transparency to the Internet connection end-to-end, when there is a mobile user at least on one end of such connection.

In order to preserve the proper layout of the packets and to reduce or prevent packets losses in Figure 2, full duplex routing to the target destination will use link same path.
In context, every radio access technology that is available to the user for connectivity with the relevant radio access is presented with appropriate IP interface. Each IP interface in the terminal is characterized by its IP address and net mask and parameters associated with the routing of IP packets across the network In regular inter-system handover the change of access technology (i.e., vertical handover) would mean changing the local IP address. Then, change of any of the parameters of the socket means and change of the socket, that is, closing the socket and opening a new one. This means, ending the connection and starting new one.

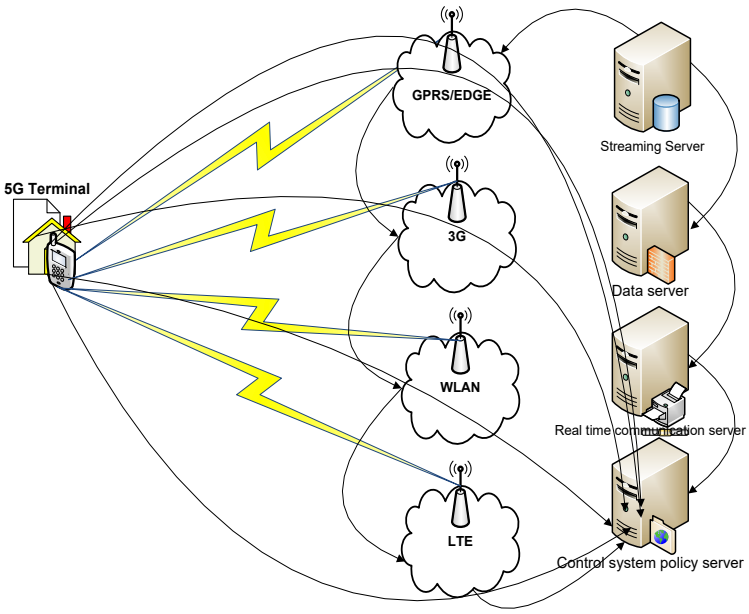


Figure 2. Proposed 5G Architecture for Disruptive technologies

IV. ADVANTAGES OF 5G

So far, it has been established that there is no relationship between 5G technology and COVID-19. Qualcomm [37] has provided few advantages of 5G network and these include:

A. Enhanced Mobile Broadband

5G will not only make our smart phones better, but it will also usher in new immersive experiences, such as VR and AR, with faster, more uniform data rates, lower latency, and cost-per-bit.

B. Mission-critical Communication

5G will enable new services that can transform industries with ultra-reliable/available, low latency links—such as remote control of critical infrastructure, vehicles, and medical procedures. Figure 3 is a typical use case scenario where the proposed 5G network could be deployed [38].

Figure 3. IoT-Fog Cloud use case for 5G Architecture

C. Massive Internet of Things:

5G will seamlessly connect a massive number of embedded sensors in virtually everything through the ability to scale down in data rates, power and mobility to provide extremely lean/low-cost solutions.

D. Health care:

One of the most important areas that 5G technology will prove to be transformative is in the field of medicine. When it comes to matters of life and death, just a few seconds can make all the difference. 5G technology will dissolve borders and allow doctors to reach patients from every corner of the globe. The potential for medical advancements, through 5G technology, is limitless and absolutely incalculable.

E. Capability:

A defining capability of 5G is also the design for forward compatibility—the ability to flexibly support future services that are unknown today. In essence, this is technology that will redefine the way communication happens. It will affect the method of entertainment, shopping, etc. If 3G and 4G changed the aforementioned, , then, 5G will transform those domains.

V. COVID 19

The world health organization (WHO) [36] has identified COVID-19 as an acronym for Coronavirus Disease 2019. This is an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). The disease was first identified in December 2019 in Wuhan, the capital of China's Hubei province, and has since spread globally, resulting in the ongoing 2019–20 coronavirus pandemic. Common symptoms include fever, cough and shortness of breath. Other symptoms may include fatigue, muscle pain, diarrhea, sore throat, loss of smell and abdominal pain.

The time from exposure to onset of symptoms is typically around five days, but may range from two to 14 days. While the majority of cases result in mild symptoms, some progress to viral pneumonia and multi-organ failure. The virus is mainly spread during close contact and by small droplets produced when those infected cough, sneeze or talk. These droplets may also be produced during breathing; however, they rapidly fall to the ground or surfaces and are not generally spread through the air over large distances. People may also become infected by touching a contaminated surface and then their face. The virus can survive on surfaces

for up to 72 hours, it's most contagious during the first three days after onset of symptoms, although spread may be possible before symptoms appear and in later stages of the disease. The World Health Organization (WHO) declared the 2019–20 coronavirus outbreak a Public Health Emergency of International Concern (PHEIC) on 30 January 2020 and a pandemic on 11 March 2020.

To end it, 5G network is not an ionizing radiation, and poses no harm to the body, well not anyone that has been experience now. Some allegedly claims that 5G towers are the cause of the spread of the pandemic due to radiation, which is not true. 5G speeds are achieved by speeding up the bandwidth of the 4G about 20 times over. This makes it much faster than anything we've ever seen, but also brings the limitation that it has a short wavelength. In other words, 5G network cannot travel far, with an average coverage distance of about 20 meters.

It therefore means that for 5G to work there need to be thousands of cell towers in one small city to compensate for poor coverage distance. In other words, use quantity of cell towers to cover for poor quality of coverage. Due to the closeness of cell towers with average distance of about 20 meters, has tighten the claim that 5G towers are the engine that foster the wide spread of Covid-19. Unlike the 4G which requires less cell towers to travel afar.

Categorically speaking, there is no evidence that 5G networks are harmful to health. Like the previous generations of wireless network technology (4G, 3G and 2G), 5G mobile data is transmitted over radio waves. Other types of technology that use radio waves include smart meters, TV and radio transmitters, and radar and satellite communications. Most modern medical laboratory equipment use radio waves some use nuclear radiation, but applied within licensed standards.

Obviously, the radio waves are a small part of a wider electromagnetic spectrum of waves, which all emit energy called electromagnetic radiation. Radio waves are found at the low-frequency end of the spectrum and—alongside microwaves, visible light and heat—only produce non-ionizing radiation. This means that these waves cannot damage the DNA inside cells, which is how waves with higher frequencies (such as x-rays, gamma rays and ultraviolet light) are thought to cause cancer. To improve the speed and capacity of our wireless technology, 5G uses a higher frequency of radio waves compared to its older generations.

The frequency of this new wireless technology remains very low: the maximum levels of electromagnetic radiation measured by OFDM were about 66 times smaller than the safety limits set by international guidelines. Public Health England states that “the overall exposure is expected to remain low relative to guidelines and, as such, there should be no consequences for public health. The world health organization (WHO) [36] that electromagnetic waves emit electromagnetic radiation, which at high frequencies are believed to pose a risk of causing cancer. However, low frequencies - such as 5G frequencies - produce a non-ionizing form of radiation that is not thought to be able to penetrate and damage cells. 5G frequencies may be higher than that of 4G and other earlier networks, but they are still far lower than the limits stipulated in international guidelines. From the detailed guidelines reported by WHO, on the mobile network, it is obvious that there is "no adverse health effect that is linked with exposure to wireless technologies.

VI. CONCLUSION

This paper has discussed the context of 5G network for disruptive technologies and have cleared the misconceptions about 5G/COVID-19 myths. Facts are facts, fiction is fiction. Science is fact not fiction. We are all exposed to lots of different carcinogens in our life. Some we can avoid and some we can't (such as sunlight). In the long run we are all dead, so said the fatalistic Social Economist Thomas Keynes. With various technologies in the world such as televisions, refrigerators, microwaves cookers and ovens, wireless electronics, computers and all sorts of mobile devices in addition to the radiations around humans, 5G cannot be a major cause of COVID. The very real benefits from 5G far outweigh the very miniscule risk from 5G that may not even exist. But for now, highlights from literature about 5G networks shows that there’s no reason to be worried as 5G will have a transformational impact on our lives and enable fundamentally new things.

ACKNOWLEDGMENT

Special thanks to Engr. Dr. M. C. Arimanwa, Rector Federal Polytechnic Nekede, Owerri Imo state, Nigeria.

REFERENCES

[1.] Q. Yuan, Q. Qian, Y. Mo and H. Chen, "Research on Mixed Planning Method of 5G and LTE," 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, pp. 489-493, doi: 10.1109/ICICT50521.2020.00084.

[2.] U. B. Shukurillaevich, R. O. Sattorivich and R. U. Amrillojonovich, "5G Technology Evolution," 2019 International Conference on Information Science and Comm., Tech., (ICISCT), Tashkent, Uzbekistan, 2019, pp. 1-5, doi: 10.1109/ICISCT47635.2019.9011957.

[3.] A. Zafeiropoulos et al., "Enabling Vertical Industries Adoption of 5G Technologies: A Cartography of Evolving Solutions," 2018 European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, 2018, pp. 1-9, doi: 10.1109/EuCNC.2018.8442656.

[4.] J. Leng, Z. Lin and P. Wang, "Poster Abstract: An Implementation of an Internet of Things System for Smart Hospitals," 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), Sydney, Australia, 2020, pp. 254-255, doi: 10.1109/IoTDI49375.2020.00034.

[5.] W. Du, Z. Zhu, C. Wang and Z. Yue, "The Real-time Big Data Processing Method Based on LSTM for the Intelligent Workshop Production Process," 2020 5th IEEE International Conference on Big Data Analytics (ICBDA), Xiamen, China, 2020, pp. 63-67, doi: 10.1109/ICBDA49040.2020.9101345.

[6.] G. Fox and S. Jha, "Conceptualizing a Computing Platform for Science Beyond 2020: To Cloudify HPC, or HPCify Clouds?," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, CA, 2017, pp. 808-810, doi: 10.1109/CLOUD.2017.120.

[7.] Z. Aung, I. S. Mikhaylov and Y. T. Aung, "Artificial Intelligence Methods Application in Oil Industry," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 563-567, doi: 10.1109/EIConRus49466.2020.9039330.

[8.] T. N. Dinh and M. T. Thai, "AI and Blockchain: A Disruptive Integration," in Computer, vol. 51, no. 9, pp. 48-53, September 2018, doi: 10.1109/MC.2018.3620971.

[9.] J. C. Lin, "5G Communication Technology and Coronavirus Disease [Health Matters]," in IEEE Microwave Magazine, vol. 21, no. 9, pp. 16-19, Sept. 2020, doi: 10.1109/MMM.2020.2999236.

[10.] T. Sharma, K. Ritesh, N. Chauhan and S. Agarwal, "Analogous study of 4G and 5G," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 2137-2140.
[11.] A. Furuskär, J. Rao, M. Blomgren and P. Skillermark, "LTE and HSPA for fixed wireless broadband: Datarates, coverage, and capacity in an Indian rural scenario," 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, 2011, pp. 1-5, doi: 10.1109/WIRELESSVITAE.2011.5940858.
[12.] F. Balteanu, H. Modi, Y. Zhu, S. Drogi and S. Khesbak, "Envelope Tracking System for High Power Applications in Uplink 4G/5G LTE Advanced," 2018 Asia-Pacific Microwave Conference (APMC), Kyoto, 2018, pp. 863-865, doi: 10.23919/APMC.2018.8617571.
[13.] 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," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341.
[14.] L. Fang G. Karakiulakis and M. Roth "Are patients with hypertension and diabetes mellitus at increased risk for COVID-19 infection?" Lancet. Respiratory Med. vol. 8 no. 4 pp. e21 2020.
[15.] S. H. Wong R. N. S. Lui and J. J. Y. Sung "Covid-19 and the digestive system" J. Gastroenterol. Hepatol. 2020.
[16.] R. Baldwin and E. Tomiura Thinking ahead about the trade impact of COVID-19 pp. 59 2020.
[17.] V. Surveillances "The epidemiological characteristics of an outbreak of 2019 novel coronavirus diseases (COVID-19) China 2020" China CDC Weekly vol. 2 no. 8 pp. 113-122 2020.
[18.] H. Chen J. Guo C. Wang F. Luo X. Yu W. Zhang et al. "Clinical characteristics and intrauterine vertical transmission potential of COVID-19 infection in nine pregnant women: A retrospective review of medical records" Lancet vol. 395 no. 10226 pp. 809-815 Mar. 2020.
[19.] D. Wang B. Hu C. Hu F. Zhu X. Liu J. Zhang et al. "Clinical characteristics of 138 hospitalized patients with 2019 novel coronavirus–infected pneumonia in Wuhan China" J. Amer. Med. Assoc. vol. 323 no. 11 pp. 1061 Mar. 2020.
[20.] N. Chen M. Zhou X. Dong J. Qu F. Gong Y. Han et al. "Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan China: A descriptive study" Lancet vol. 395 no. 10223 pp. 507-513 Feb. 2020.
[21.] S. Henry, A. Alsohaily and E. S. Sousa, "5G is Real: Evaluating the Compliance of the 3GPP 5G New Radio System With the ITU IMT-2020 Requirements," in IEEE Access, vol. 8, pp. 42828-42840, 2020, doi: 10.1109/ACCESS.2020.2977406.
[22.] L. Yala, S. Cherrared, G. Panek, S. Imadali and A. Bousselmi, "5G Experimentation Framework: Architecture Specifications, Design and Deployment," 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2020, pp. 159-161, doi: 10.1109/ICIN48450.2020.9059458.
[23.] S. Sriraam, S. Sajeev, R. Joshi, A. Vithalkar, M. Bansal and H. Jagadeesh, "Implementation of 5G Authentication and Key Agreement Protocol on Xbee Networks," 2020 International Conference on Communication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 696-698, doi: 10.1109/COMSNETS48256.2020.9027314.
[24.] N. Nonaka et al., "28 GHz-Band Experimental Trial at 283 km/h Using the Shinkansen for 5G Evolution," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 2020, pp. 1-5, doi: 10.1109/VTC2020-Spring48590.2020.9129578.
[25.] L. He, Q. Guo, J. Zhong, X. Wang, M. Li and Y. Teng, "5G Network Performance Analysis and Verification Based on Ubiquitous Electricity Internet of Things," 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2020, pp. 2613-2617, doi: 10.1109/ITNEC48623.2020.9084822.
[26.] Q. Yuan, Q. Qian, Y. Mo and H. Chen, "Research on Mixed Planning Method of 5G and LTE," 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, pp. 489-493, doi: 10.1109/ICICT50521.2020.00084.
[27.] A. K. Singh, H. Katiyar, R. Kumar and S. Dixit, "Revolutionizing 5G: Cognitive Machine Learning," 2020 International Conference on Electrical and Electronics Engineering (ICE3), Gorakhpur, India, 2020, pp. 17-20, doi: 10.1109/ICE348803.2020.9122803.
[28.] I. Kim, J. Um and S. Park, "Implementation of SDR-based 5G NR Cell Search Equipment," 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang,, Korea (South), 2020, pp. 350-353, doi: 10.23919/ICACT48636.2020.9061404.
[29.] E. Garro et al., "5G Mixed Mode: NR Multicast-Broadcast Services," in IEEE Transactions on Broadcasting, vol. 66, no. 2, pp. 390-403, June 2020, doi: 10.1109/TBC.2020.2977538.
[30.] R. Vidhya, P. Karthik and S. Jamadagni, "Anticipatory QoE Mechanisms for 5G Data Analytics," 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 523-526, doi: 10.1109/COMSNETS48256.2020.9027358.
[31.] P. Sivakumar, R. S. Sandhya Devi, A. Neeraja Lakshmi, B. VinothKumar and B. Vinod, "Automotive Grade Linux Software Architecture for Automotive Infotainment System," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 391-395, doi: 10.1109/ICICT48043.2020.9112556.
[32.] Y. Li, X. Wang and H. Lei, "Construction and weighting of investment risk index system of general aviation industry based on entropy method," 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 2020, pp. 784-787, doi: 10.1109/ICCEA50009.2020.00171.
[33.] P. M. Chango-Cañaveral, K. E. Alvarado–León and P. A. Quezada-Sarmiento, "Use of Social Networks and Development of the Servqual Method in the hotels of I, II, III, IV and V category of the city of Loja as tools for continuous improvement on tourism industry," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain, 2020, pp. 1-5, doi: 10.23919/CISTI49556.2020.9140815.
[34.] Z. Aung, I. S. Mikhaylov and Y. T. Aung, "Artificial Intelligence Methods Application in Oil Industry," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, 2020, pp. 563-567, doi: 10.1109/EIConRus49466.2020.9039330.
[35.] S. Rachchompoo, N. Intarawiset, S. Akatimagool and K. Chaiyawong, "Development of Learning Innovation of DTV Antennas for Telecommunication Education," 2020 7th International Conference on Technical Education (ICTechEd7), Bangkok, Thailand, 2020, pp. 41-44, doi: 10.1109/ICTechEd749582.2020.9101236.
[36.] F. E. S. de Leon, P. Nicklin, C. Rhodes and S. Y. Kwankam, "Promoting appropriate eHealth technologies in the developing world: The Sharing eHealth Intellectual Property for Development (SHIPD) initiative of the World Health Organization," 2008 5th IET Seminar on Appropriate Healthcare Technologies for Developing Countries, London, 2008, pp. 1-3, doi: 10.1049/ic:20080587.
[37.] R. H. Stern, "FTC and Apple Sue Qualcomm for Cell Phone Standardization Skullduggery, Part 2: Apple's Claims," in IEEE Micro, vol. 37, no. 4, pp. 72-81, 2017, doi: 10.1109/MM.2017.3211106.
[38.] R. Jindal, N. Kumar and H. Nirwan, "MTFCT: A task offloading approach for fog computing and cloud computing," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 145-149, doi: 10.1109/Confluence47617.2020.9058209.

A feasibility study of cluster-based energy harvesting aware routing protocol for body nanosensor network

Sikiru. O. Zakariyya
Department of Electricl and Electronics Enigineering
University of Ilorin
Ilorin, Nigeria
zakariyya.os@unilorin.edu.ng

Abdulmalik. S. Yaro, Aliyu. D. Usman, Suleiman. M. Sani, Abdoulie. M. S. Tekanyi
Department of Electronics and Telecommunication Engineering
Ahmadu Bello University
Zaria, Nigeria
asyaro@abu.edu.ng, aliyuusman1@gmail.com, smsani@abu.edu.ng, amtekanyi@abu.edu.ng

***Abstract*—Wireless nanosensor network (WNSN) are networks of interconnected nano-nodes communicating at terahertz frequency. The nano-node range of communication as well as the overall performance of the WNSN is affected mainly by the path loss of the terahertz frequency band and also by the very limited nano-nodes resources and capacity. For that reason, there is need for a suitable routing protocol that will guarantee multihop communication in WNSN. Clustering technique has been proving to be a cost-effective method to provide successful communication for body WNSNs. However, the nanonode elected as the nano-cluster head diminishes its energy dynamically. This will result into loss of monitored data in the cluster and reduce the reliability of the network. Existing clustering techniques in WNSN proposed for health care application did not take the energy exhaustion of the nano-cluster head into consideration. Hence, this work gives a review of work done to date on WNSN routing protocol, identifies their weaknesses and then suggest the implementation of an energy harvesting aware protocol that employs cluster-based hierarchical architecture by considering two different scenarios (using a back-up cluster head technique and using a wireless energy transfer technique) with a view to ensuring lifetime operation of the nano-node, minimize packet loss and conserving energy.**

Keywords—Backup Cluster, Nano-devices, Nanosensor, Routing, Terahertz.

I. INTRODUCTION

The emergent of nanotechnology has enabled the engineering community to develop a new set of nano-scale devices that have the ability to carry out simple operations like actuation, sensing, data storing and computing. The nano-scale devices are however limited with energy constraint and low processing capability. The limitation of energy constraint, sensing capability and data processing capability of individual nanoscale device can be overcome by interconnecting them to form a wireless nanosensor network (WNSN). It differs from the typical Wireless Sensor Network (WSN) because the nanodevices have the ability to detect events at the nano-scale. The area of Wireless Nanosensor Networks (WNSN) is attractive in many monitoring applications for civilian, biomedical and military use [1]. Different communication paradigms including acoustic, nano-mechanical, electromagnetic and molecular communication have been suggested overtime on the basis of the chosen transmission medium for WNSN. Nonetheless, acoustic and mechanical communication is unsuitable for WNSN in human body [2 3] while molecular and electromagnetic communication paradigm have been very promising [4]. Eventually, electromagnetic communication for nano-node-nodes is expected to work in the 0.1-10 THz band, which is different from the traditional wireless carrier-based communication model. The overall network performance of the nano-nodes communicating at terahertz band frequency will be affected significantly by path loss due to high molecular absorption and low transmission power [5]. In health care applications, communication between networks of nano-nodes implanted in the human body is referred to as Body Area Nano-Networks (BANNs) [6]. These nodes communicate with each other in the network and information is routed through a gateway to the external interface and then to the health monitoring unit. Since the medical information are critical, loss of data is crucial in this application. Hence, a routing protocol is needed to guarantee the delivery of data.

The existing information routing protocol in the WSN is not directly applicable to WNSN due to their nano-scale properties which limit the amount of complex protocol that could be run on them and also their method of harvesting energy from the environment as well as the terahertz frequency band channel characteristics. Few protocols have been developed for WNSN which have their own qualities and shortcomings.

It is more advantageous to organize the nanonodes in WNSN into clusters to minimize energy consumption of individual nodes in the network. This is achieved by selecting a subclass of the nanonodes as the nano-cluster head based on their energy. These nano-cluster heads are in charge of the cluster activities and received monitored data from their nano-cluster members. These data are conveyed to the nanocontroller directly or through multihop using another nano-cluster head based on distance [7 8]. Despite the fact that this technique can minimize the energy consumed, its main challenge is the amount of energy consumed by the nano-cluster head. The nano-cluster head will exhaust their energy quicker as they are responsible for forwarding all the data gathered in the cluster. Also, the nano-cluster head along the routing path tends to have substantial task thereby speedily exhausting their energy.

Therefore, this work gives a review of work done to date on WNSN routing protocol, identifies their weaknesses and then suggest the implementation of an energy harvesting aware protocol that employs cluster-based hierarchical architecture by considering two different scenarios (using a back-up cluster head technique and using a wireless energy transfer technique) with a view to ensuring lifetime operation of the nano-node, minimize packet loss and conserving energy.

II. RELATED WORKS

Wireless nanosensor network research has received a lot of attention from the early researchers, they have surveyed and identified the concept, challenging issues, communication and networking models with energy harvesting as the only source of powering the nano-nodes. Most of the existing routing protocols designed for the WSN are not directly applicable to WNSN due to the energy harvesting, terahertz channel peculiarities and limited capability of the nano-node. The focus of this work is information routing among nano-nodes that forms nanosensor networks operating in the terahertz frequency band. As such, some of the pertinent works are reviewed in this section.

Routing is a key role of the network layer of the communication protocol stack and it is defined as the process of establishing paths through one or several relays from a source to a sink (e.g. a gateway device). The routing protocols research in WNSNs is still at an early stage as only a few numbers of routing protocols have been proposed [9]. In recent years, routing protocols for WNSNs has been receiving attention from various researchers. Three routing protocols have been majorly identified:

a) Flooding based protocols

b) Proximity routing protocols

c) Energy harvesting based routing protocols

The simplest of the above-mentioned protocol is the flood-based routing protocol as it's consistent with the nano-node energy and computation power [10]. However, flooding techniques will lead to the excessive transmission and broadcast storm which in turns increased energy consumption. In an attempt to improve the performance of flooding-based routing protocol, proximity routing protocol which controls the number of neighboring nodes was proposed. Some of the reported proximity protocols include CORONA [11 12]. CORONA categorized the nodes in the network into an anchor node and user nodes where the anchor nodes are assumed to have high processing capability than the user node. While CORONA is effective for point to point communication, terahertz channel attenuation characteristics were however not considered. In an effort to solve the problem associated with CORONA, EEMR protocol was proposed [12]. However, nano-nodes failures as a result of energy exhaustion or interruption in the transmission link due to channel environment not solved by the protocol. The last category of the above-mentioned routing protocol designed specifically for self-powered nano-nodes is the energy harvesting based routing protocols. The main goal of the energy harvesting routing protocol is to balance the harvested and the consumed energy by the nano-nodes in the WNSNs to achieve perpetuity. The first routing framework proposed for WNSNs based on energy harvesting considered the tradeoff between harvested and consumed energy and also establish multi-hop routing based on features of terahertz channel [13]. They employed the usage of hierarchical routing architecture with clustering where each nano-node forwards their information to the nano-controller via their cluster head. It was revealed from simulation that the protocol can increase the throughput as well as reduce energy consumption. Nevertheless, this routing protocol has a high computational complexity which may hamper its use in practice. In an effort to integrate the Body area nanonetwork (BANNET) and a macroscale health monitoring system, an energy harvesting routing protocol based on Hierarchical network architecture that regulates communication among nano-nodes was proposed [14]. They proposed two separates energy harvesting aware protocol stack (greedy and optimal approach) which are both made up of MAC and Routing algorithm. However, the developed protocol did not achieve big and meaningful performance gain as in relation to the flooding scheme due to the handshaking mechanism. Reference [15] proposed a wireless nanosensor network model based on On-Off Keying (OOK) protocol and TDMA framework for intrabody disease detection. Based on the fact that the nano patch antennas are graphene-based in a honeycomb crystal lattice, the author assumed a hexagonal cell-based nanosensor which was deployed in a cylindrical shape 3D hexagonal shape. However, they did not consider the energy harvesting process of the nanosensor node. Reference [16] proposed an efficient scheme for data collection in a Body Area Nanonetwork. The proposed scheme which is largely determined by the distance between the nano-nodes and nano-router aimed at improving the work of [14] by taking the transmission path loss into consideration. However, if a nano-node is outside the coverage range of any nano-router, it waits pending the time when a signal can be received by one of them which results to delay. In order to improve the performance of nano-nodes communicating at terahertz frequency, an energy-conserving routing method using a hybrid cluster with centralized scheduling was proposed [7]. NANO-SIM was employed in simulating the ECR scheme and the performance was evaluated in terms of outage probability, outage capacity and energy efficiency. It was reported from the simulation result that the ECR scheme balance the energy consumed in WNSNs and also reduce the data collision due to the multilayer topology and transmission time allocation. However, consideration is not given to failure of cluster head which might results into loss of data packets. However, a reasonable mechanism for updating the cluster head is not provided. Finally, energy balanced routing protocol for intrabody wireless nanosensor network was proposed [8]. Intra cluster transmission between nano-nodes and cluster head is in a cluster is achieved using one hop while the multihop transmission is used between cluster head and the nano controller. However, consideration is not given to failure of cluster head which might results into loss of data packets.

Considering the similar work reviewed, a summary of the drawbacks includes:

a) The use of routing protocol that doesn't consider the energy harvesting of the nano-nodes which renders the protocol unrealistic for nanosensor networks with limited energy as in the work of [15].

b) The use of the protocol with a high computational complexity which prevents their large usage in WNSNs as in the work of [13].

c) The development of protocols not applicable to health monitoring applications as in the work of [10 11].

d) The development of health monitoring protocols that assume communication is initiated from the external body thereby omitting the critical information detected by the nano-nodes implanted inside the body as in the work of [14 16].

e) The development of a protocol that does not consider the drop in the energy level of cluster head below the required energy prior to inter-cluster transmission as in the work of [7 8].

III. DESIGN METHODOLOGY

Due to the problems identified in the existing work, this paper proposed a system which comprises of nano-nodes implanted inside the human body forming a nanosensor network. The nano-nodes which are energy-constrained are capable of communicating with each other and the outside world. The implanted nano nodes forward their available data through a cluster head to the nano-controller which has more energy and computational resources. The nano-controller forwards the data via the nanointerface to the external world via a gateway. Hierarchical clustering approach will be implemented where each node is grouped into a certain cluster and a cluster head is appointed based on available energy and the designed scheme. The nodes in a cluster are referred to a nano-cluster member. Each nano-cluster member communicates directly with the cluster head or through another cluster member based on the required energy to transmit. The cluster head can either communicate directly to the nano-controller or through a neighbouring cluster head using multihop communication. In a situation where the energy level of the nano-cluster head is below the required energy to complete inter-cluster communication, two solutions are proposed to prevent loss of data in the network as depicted in Fig. 1 and Fig. 2. Fig. 1. shows the back-up clustering technique. In this scenario, those cluster head with deficient energy below the energy required to complete inter-cluster transmission will hand over the gathered data in the cluster to the preselected back-up cluster head (BC). Doing so, the system will prevent the loss of gathered data in the cluster and hence improve the reliability of transmitted data. Fig. 2 depict the conceptual diagram of clustering with wireless energy transfer technique. In this scenario, we employ the concept of wireless energy transfer from a more resourceful nanocontroller to energy deficient cluster head. Prior to data transmission, the cluster head with remaining energy below the required energy for data transmission will receive additional energy from the nanocontroller wirelessly. This will prevent the cluster head from losing gathered data in its cluster as a result of low energy. The nodes activity will be categorized into Active, Listening, blocking and sleeping modes in order to effectively manage energy resources. Transmission of data will be based on TDMA where time slot will be allocated to each cluster layer based on request. Data will be classified as either emergency or regular data. To the best of our knowledge, the concept of back-up clustering and wireless energy transfer from a more resourceful nanocontroller has not been considered in the domain of WNSN, hence the novelty of this work.

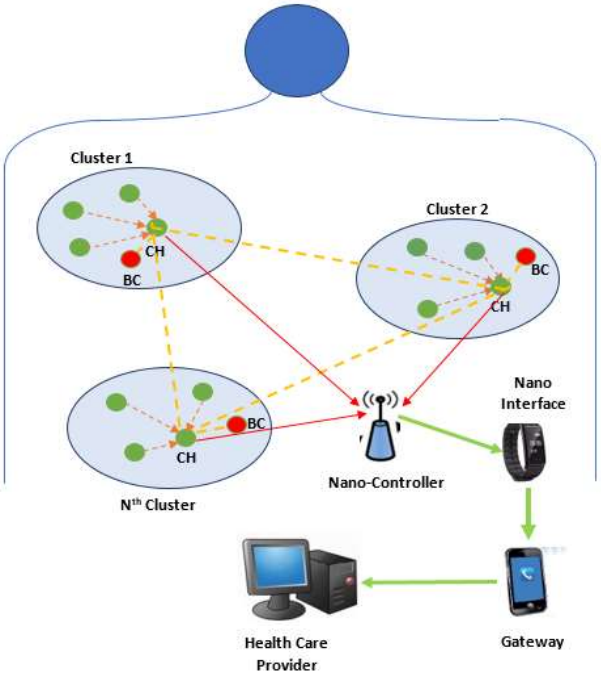
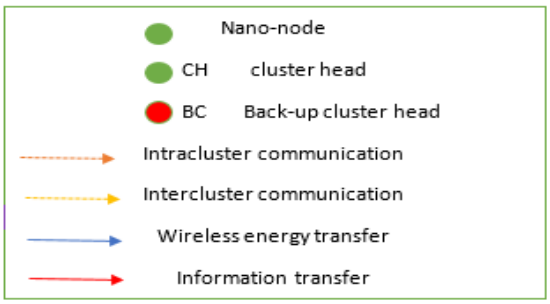


Fig. 1. Conceptual Framework for the proposed work using a back-up cluster head



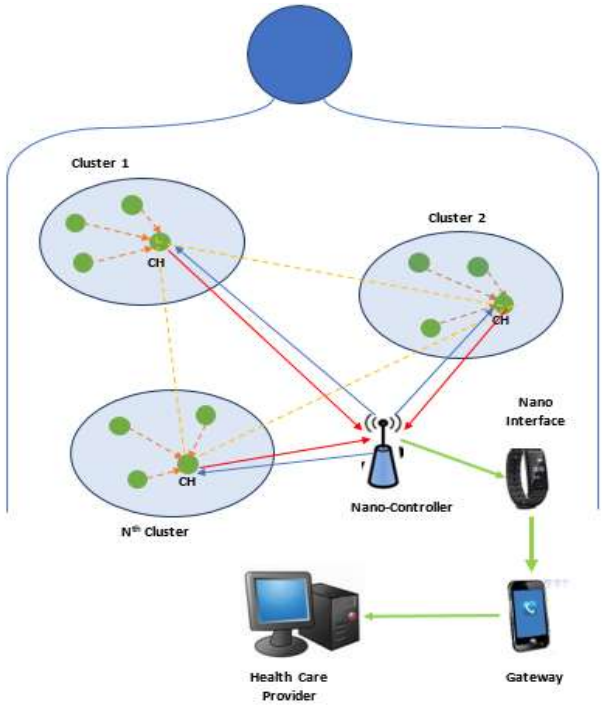


Fig. 2. Conceptual Framework for the proposed work using wireless energy transfer

IV. CONCLUSION

This paper presented the state of the art routing protocol developed for WNSNs. First we discussed the problem and constraint of WNSNs and the unsuitability of directly applying the existing information routing protocol in the WSN to the WNSN. Then we surveyed the existing protocol design for WNSN and identified their drawbacks. We then presented the idea of back-up clustering and wireless energy transfer which is expected to improve the data packet transmission success, minimize energy and improve network lifetime. The current work in progress is the implementation and simulation of the proposed ideas.

REFERENCES

[1] I. F. Akyildiz, and J. M. Jornet, "Electromagnetic wireless nanosensor networks," Nano communication networks, vol. 1 No. 1, pp. 3–19, 2010. doi:10.1016/j.nancom.2010.04.001

[2] G. E. Santagati, and T. Melodia, "Opto-ultrasonic communications for wireless intra-body nanonetworks," Nano Communication Networks, vol. 5 No. 1-2, pp. 3–14, 2014 doi:10.1016/j.nancom.2014.03.001.

[3] F. Dressler, and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," Nano Communication Networks, vol. 3 No. 3, pp. 151–160, 2012. doi:10.1016/j.nancom.2012.08.001.

[4] C. Rutherglen, and P. Burke, "Nanoelectromagnetics: Circuit and Electromagnetic Properties of Carbon Nanotubes", Small, vol. 5 No. 8, pp. 884–906, 2009. doi:10.1002/smll.200800527 .

[5] J. M. Jornet, and I. F. Akyildiz, (2011) "Channel modeling and capacity analysis for electromagnetic wirelessnanonetworks in the terahertz band," Wireless Communications, IEEE Transactions, vol. 10 No. 10, pp. 3211-3221, 2011.

[6] B. Atakan, O. Akan, and S. Balasubramaniam, (2012) "Body area nanonetworks with molecular communications in nanomedicine," IEEE Communications Magazine, vol. 50 No. 1, pp. 28-34, 2012. doi:10.1109/mcom.2012.6122529.

[7] F. Afsana, M. Asif-Ur-Rahman, M. R. Ahmed, M. Mahmud, and M. S. Kaiser, "An Energy Conserving Routing Scheme for Wireless Body Sensor Nanonetwork Communication"', IEEE Access, vol. 6, pp. 9186–9200,2018. doi:10.1109/access.2018.2789437.

[8] J. Xu, Y. Zhang, J. Jiang, and J. Kan, "An Energy Balance Clustering Routing Protocol for Intra-Body Wireless Nanosensor Networks" . Sensors, vol. 19 No. 22, 2019. doi:10.3390/s19224875.

[9] X.-W.Yao, Y.-C.-G. Wu, and W. Huang, "Routing techniques in wireless nanonetworks: A survey,"Nano Communication Networks, vol. 21, 2019. 100250. doi:10.1016/j.nancom.2019.100250.

[10] O. Yalgashev, M. Bakhouya, J. Gaber, and M. A. Manier, "Adaptive Transmission Range Control for Electromagnetic-based Broadcasting in Nanonetworks,"Procedia Computer Science, vol. 52, pp. 1077–1082, 2015. doi:10.1016/j.procs.2015.05.116 .

[11] A. Tsioliaridou, C. Liaskos, S. Ioannidis, and A. Pitsillides, "Corona: A coordinate and routing system for nanonetworks" in NANOCOM 2015: International Conference on Nanoscale Computing and Communication, pp. 1–6. doi:10.1145/2800795.2800809.

[12] J. Xu, R. Zhang, and Z. Wang, "An Energy Efficient Multi-hop Routing Protocol for Terahertz Wireless Nanosensor Networks," Lecture Notes in Computer Science, pp. 367–376, 2016. doi:10.1007/978-3-319-42836-9_33.

[13] M. Pierobon, J. M. Jornet, N. Akkari, S. Almasri, and I. F. Akyildiz, "A routing framework for energy harvesting wireless nanosensor networks in the Terahertz Band,"Wireless Networks, vol. 20 No. 5, pp. 1169–1183, 2013. doi:10.1007/s11276-013-0665-y.

[14] G. Piro, G. Boggia, and L. A. Grieco, "On the design of an energy-harvesting protocol stack for Body Area Nano-NETworks", Nano Communication Networks, vol. 6 No.2, pp. 74–84, 2014 doi:10.1016/j.nancom.2014.10.001.

[15] S. J. Lee, C. A. Jung, K. Choi, and S. Kim, "Design of Wireless NanosensorNetworks for IntrabodyApplication,"International Journal of Distributed Sensor Networks, vol. 11 No 7, 2015.doi:10.1155/2015/176761.

[16] B. Liu, J. Liu, Z. Wu, X. Jiang, "On the Design of an Energy Efficient Data Collection Scheme for Body Area Nano Networks," International Journal of Wireless & Mobile Networks, vol. 9 No. 3, 2017. http://dx.doi.org/10.2139/ssrn.3443439

Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface

Kufre Esenowo Jack
Department of Mechatronics Engineering,
School of Electrical Engineering & Technology, Federal University of Technology Minna,
Minna, Niger State, Nigeria
ORCID ID: 0000-0003-2422-5442
kufre@futminna.edu.ng

Uchenna Godswill Onu
Department of Electrical/Electronic Engineering, School of Engineering Technology, Akanu Ibiam Federal Polytechnic Unwana,
Afikpo, Ebonyi State, Nigeria
uchmangod@gmail.com

Sophia Ededet Akpan
Department of Electrical Maintenance,
Northern Bag Manufacturing Company Limited,
Kano State, Nigeria
Sophia.akpan@rocketmail.c

***Abstract*— This research paper focuses on the design and implementation of an intelligent mosquito monitoring and control system model with android-enabled user interface and bzigo camera system to monitor and repel mosquitoes as a preventive remedy for mosquito bites that cause malaria infection. Several techniques aimed at combating mosquitoes to stop malaria spread ranging from environmental fumigation; the use of mosquito treated net; the use of herbal repellent sticks with low smoking technique; the spray of mosquito insecticide chemical repellents to electronic spray control, have health and environmental concerns. The method adopted for this design includes: microcontroller-based system, bzigo camera system and Android-enabled system. These combined approaches were used to develop a human and environmentally friendly device. The bzigo camera system intelligently scans for mosquitoes within its range of coverage and processes the images of mosquitoes automatically to give a feedback to a microcontroller. The controller receives the image signal and sends a notification to the home owners and also produces a sound frequency of about 38kHz to 45kHz that forces the available mosquitoes into a specified vacuum for the house owner's disposal. This frequency range does not permit the survival of mosquitoes and this operation is monitored using a developed Android-enabled user interface. The design was tested under an indoor space of 12ft x 12ft confinement. The results from this intelligent mosquito repelling system model proves its suitability for the control of mosquitoes and as such seen to be an adequate technique to replace other less human and environmentally friendly approaches.**

Keywords — Android-enabled, Mosquito Repellant, Intelligent system, Bzigo Monitoring, Control Model

I. INTRODUCTION

Engineering principles exist to develop systems that make life easy for mankind. Though, human health deteriorates daily as a result of diseases emanating from the environment. One of these diseases is the mosquitoes-borne menace known as malaria which has now become a major source of attack to global public health [1]**.** Machine learning finds application in monitoring mosquitoes' action and controlling their activities. Mosquito repellents are combined constituents of substances developed to make surfaces unfriendly or deterring to mosquitoes thereby limiting their spread. Mosquito repellents contain some active ingredients that aid their capacity to repel mosquitoes with some other ingredients [2]**.** Advancements in engineering have proven to be the only sustaining strategy for mankind globally; this is due to its inventions, innovations and enhancement of the already existing technologies. Malaria was discovered long ago to be one of the infectious diseases caused by Anopheles mosquitoes. The Anopheles mosquitoes on biting human being introduce the parasite plasmodium into the body that causes malaria. Due to the fact that this infectious disease has proven to be universal, the World Health Organization decided that some ways of controlling, eliminating and eradicating this global menace be formulated [3]. Several of these approaches from scientific research have attempted to control, eradicate and eliminate malaria spread. These methods range from keeping the environment clean, the use of treated net, treated swatter, UV lamps, LED trapping system, burning of dry leaves to application of liquid or dry inflammable repellant. The electronic approach of tackling mosquito spread using the frequency range of 20 kHz to 40 kHz was proposed. In this proposed design, 20 kHz to 40 kHz frequency range is invisible to human but the sound is capable of displacing mosquitoes after an intelligent camera has established the presence of mosquitoes within the experimented area. Mosquitoes are made to sense the sound waves constantly thereby compelling them to move to far distance with the embedded internet of things device[4]**.**

Mosquito bites resulting an infectious disease known as malaria from the associated parasite plasmodium has remained a source of health concern in our society[5][6]. Several efforts have been made by researchers to combat this infectious disease ranging from keeping the environment clean, production of liquid or dry inflammable mosquito repellent and burning of mosquito coils. These means of combating this menace have proven not to be environmentally safe and healthy. The use of insecticides has proven to be one of the ways of combating this epidemic but its effects on human health and environment still makes it unsafe for continued use. Electricity driven mosquitoes repellent promisingly provides the solution to mosquito attack but the unguaranteed steady supply of electricity becomes another setback for a developing economy, hence the need to design and implement an intelligent, android-enabled mosquito monitoring and repelling control system as it will aid the elimination of the malaria disease condition resulting from mosquito bite with minimal power consumption. Plasmodium is transmitted through bites from the female anopheles mosquitoes that serve as its host which in turn causes fever, vomiting within 15 to 20 days of human infection [5]**,** there is need for a design that will completely prevent the transmission of this disease causing organism like this design with minimal health and environmental concerns.

[7]explained that since mosquito disease is severe worldwide and with adverse effects on human health, a low-cost acoustic mosquitoes sensing system is needed. The sounds from their wing

beat are used to identify different mosquito species automatically and to monitor its activities.

The primary objective of this work is to develop an intelligent android-enabled mosquito monitoring and repelling control system model as a preventive remedy to mosquito transmitted malaria disease conditions. This primary task will be achieved with the implementation of the following secondary objectives: to develop an enhanced intelligent mobile microcontroller-based device using piezo electric sensor for mosquito repellent action; to incorporate image processing concept into the mosquito repellent system using bzigo camera; to develop a remote monitoring and control system using Android Applications; to formulate, evaluate and analyze criteria capable of ascertaining the performance of the mosquito repellent system.

The intelligent android-enabled mosquito repelling system would curtail the high cost of fumigating public places such as educational institution, banks and hospital etc and eliminate the associated health and environmental hazards for popular acceptance. With this proposed design, the environment will not witness any form of pollution. The low initial cost, easy installation and cost-free maintenance system are some attributes of the proposed design. These will make the design adventurous over other mosquito monitoring and control approaches. The era of moving round to spread or burn mosquito coils would be over. The system could also be deployed in our places of worship, banks, hospital, prison, homes and industrial zones. The listed places are where humans spend most of their time on daily engagements. This design will not have adverse effects on environment in terms of pollution and it will seek to reduce malaria infection rate through prevention of mosquito bites. The existing method of mosquito monitoring and control has effect on both human and environment, hence this proposed model.

The reason for this study is to develop an intelligent-based, camera-based, android-enabled mosquito monitoring and repelling control system model for health enhancement purpose and explore the means of using insect repelling frequency sound waves to scare them away or direct them to a specific zone for safe elimination with minimal health and environmental concerns

II. LITERATURE REVIEW

Mosquito Monitoring and Control requires global attention, several health agencies both governmental and individual are on the process of eliminating this disease-causing organism.

[8]attributes the rapid increase in public health issues as reported from mosquito-malaria infection to inadequate application of insecticide when trying to control its operation. This is in consideration of many other factors like inadequate sanitation of the environment geared towards removing stagnant water around every habitation. The proposed method uses the efficient ways of controlling mosquitoes by surveillance and detection. [9]proposed a preliminary diagnosis device for mosquito-borne diseases (dengue, chikungunya, and malaria) as a measure for monitoring the Mosquitos disease spread using Raspberry Pi-based system. The system has built-in human machine interface, temperature sensor, blood pressure monitoring device with capability of recording vital disease symptoms check.

The wide and rapid spread of mosquito (Chickugunya Infection) disease required sophisticated monitoring and control system thus, mobile device with global positioning system (GPS) was introduced for Smart malaria Healthcare system and presented a cloud based system which aids data collection through Android device and sensor with edge servers [10]. [11]also confirmed that disease causes risk on human. [12]developed low power system for monitoring and control with wireless system from Radio-frequency identification (RFID).

[13]reviewed several chemicals and their structures as they are used for production of mosquito repellents. Although several achievements were recorded involving continuous advancement and improvement, the research demonstrated chemical influence over mosquito and suggested many other compounds that could be used for repellents production. Despite these research efforts, there were some setbacks on human and environmental safety from these chemical approaches, as attempts to make them human and environmentally safe were not completely achieved. Similarly, [14] posited that Chemical mosquito repellents gained wide acceptance though harmful in comparison with the natural plant-based repellents. Mosquito repellents are considered suitable means for human protection against mosquito attack as it causes malaria because of the pathogens it transmits known as plasmodia [6].

[15]examined mosquito repellent and proposed that it should be used on fabric. With this, textile materials were treated with repellent to protect humans from mosquito bites. The essence of mosquito repellent is to make life within a given environment uncomfortable for mosquitoes. Common ways of eliminating mosquitoes are by applying smoke or burning herbs, extracting oil from the plants, tars, and mud [2].

[16]formulated a repellent stick with a low smoke herbal content for mosquitoes control with several important oils. The ingredients of these oils were combined in different proportions and proved to support burning and smelling which would aid repelling of mosquitoes. The example of one of the formulated oils was Azadiractaindica which has continuous burning and repellency capability. It was discovered that with combined ingredients, this herbal-based and eco-friendly herbs will not have adverse inhalation effect on human but it was not implemented.

Similarly, [17] carried out a research using Azadiractaindica and experimented in two days of six hours for both indoor and outdoor scenario and its mosquito repellent activities were ascertained. Citronella grass oil also gained wide acceptance in mosquito repelling herbal chemical production, this used natural binders in an attempt to eliminate the traditionally available mosquito repellents made of chemicals that were found unsuitable for human health. This was prepared with 100% herbal ingredients and [18] [19]validated essential plant oils that are good mosquito repellents.

[20]evaluated and analyzed the available electronic mosquito repelling system and concluded that the available mosquito repellent devices as at the time of the research failed to reduce human-mosquito bites but the advancement in researches has proffered solution to this problem.

[4]posited that to traditionally eliminate mosquitoes in our environment, the existing approaches like spraying of repellents, mosquito traps and mosquito killer bats were used. Their disadvantages were enormous, ranging from reaction of human skin, pollution to excessive use of the repellents with the attendant hazards. Those systems could not trap and kill the mosquitoes instantly. Another means used to combat mosquito bite was by developing a swatter, swatter is designed with thick plastic and placed such that mosquito net can be wrapped around the bed to prevent it from having contacts with human. Their design proposed that the elimination of mosquitoes can be achieved by trapping and killing. The introduction of the UV Light, mosquito liquidator with the ultrasonic sensor was also demonstrated. With these, an electric fence could be activated in an ON and OFF mode with a microcontroller via cloud to repel mosquitoes.

The electronic approach to pest control has proven that science and technology research is effective, electronic approach considers generating a certain frequency which is not audible to human ear but deterring to mosquitoes. Research shows that the sound frequencies of 10 kHz to 100 kHz make insects feel uncomfortable thereby scaring them away. This continuous audio stress has no adverse effect on humans and the environment. Whereas an audio frequency range of 20 Hz to 20 kHz can be heard by human, frequencies above this range are not audible to human but mosquitoes can hear sound with frequency higher than 20 kHz, and get irritated and forced to leave the radius of the area under the frequency coverage. The Electronic approach posed no harm to human health and the environment thereby proving a better alternative to chemical pesticides and others. Among other

advantages of electronic pest control are: low power consumption of about 1.5watts; affordability for individual and family; portability and compactness; user operational status indicator; simplicity and ease of mass production capabilities [21].

This design will introduce some modifications to improve on the already existing work by using android application for monitoring and control of the device to enhance its smart status for a better user interface, considering it's human and environmental safety attributes and effectiveness in repelling of mosquitoes.

Most recently, further effort aimed at eliminating mosquito attack on human using electronic repelling technique was demonstrated with a solar energy powered device. The design proffers a solution to a prevailing absence of constant electric power supply since electronic repelling systems rely on electric power for their optimal operation. [22] opines that for effective mosquitos' eradication, monitoring and control of their breeding Sites should be ensured. Wireless network and electromechanical technologies was adopted. The stagnant pools was identify and the short message service through Android phone was sent via GPS for the stagnant water to be removed using electromechanical pump-out techniques.

[23] [24]state that critical human threatening disease condition are caused by malaria include dengue fever, yellow fever and west Nile virus infection. The deadly disease can be control using Sterile Insect Technique.

This method was frequency dependent for evening and night mosquito repelling operations. The system incorporated wire meshes such that when mosquitoes come in contact with it, the capacitor discharges violently and creates an electrocuting electric field immediately to kill mosquitoes. With this, it was imperative to have a constant power supply which necessitated a solar-powered device. The researcher improved on the hand held device to produce a solar-powered design [25].

In [25] Arduino system was programmed with calendar update encapsulation. The recorded status of the system makes the relay either high or low to show the device operational mode. Malaria disease is a vector-borne disease and is increasingly becoming problematic mostly for urban dwellers because of indiscriminate waste dumping. The threat posed to human health requires multi-disciplinary approach to combat the spread using Remotely Piloted Aircraft Systems[26].

In another research development, the use of sound in scaring mosquitoes was demonstrated [27], with an inexpensive and scalable system which records and analyzes mosquito sounds, and posited that there is a sound frequency level that is allergic to mosquitoes. [5] developed a low energy consumption device to detect and trap mosquitoes using optical fiber sensor. The device was able to count, capture and detain live mosquitoes entering the trap using renewable energy source. [1] developed a trapping box for the collection of mosquitoes using wood made of Pinus kesiya to reduce threats posed by mosquitoes to public health. Three species of mosquitoes were captured namely: epiroticus, quinquefasciatus and sitiens which were likely to transmit malaria that will affect human health. The device was tested and proved to control the spread of malaria around the experimented zone.

[28] developed a system that traps insect with one or more optical mosquito image recording devices positioned to monitor insects passing through a particular trap inlet. The data were captured and recorded from the light scattered or shadow cast. Their method combined both mosquitoes counting and image capturing. [29] reviewed all the tools used in tracking mosquitoes, the device used in recording mosquito activities also analyzed mosquito flights. Their research opined that as long as mosquitoes exist, malaria disease will continue to affect human health and economic activities if not managed properly. Bzigo is a recent image processing device with embedded artificial intelligent encapsulation combined with laser system and AI system capability. The camera intelligently detects any mosquito that enters the house and points the laser light on it and alerts the owner of the house on the detected mosquito. With the use of computer vision, Bzigo camera can detect mosquitoes as they enter the house within minutes at a distance of about 26 feet. Whenever mosquitoes enter the room, the camera detects them and a laser pointer is automatically directed on the mosquitoes and sends a notification alert via Wi-Fi to the user device [30]. The device has no means of repelling the mosquitoes which this work seeks to incorporate. This design will develop a highly efficient and power conservative mosquito repelling system with incorporated image processing and android applications user interface. In this work, several researches so far reviewed showed that various measures aimed at mosquitoes monitoring ,detection, elimination and control were offered ranging from keeping of the environment clean, evacuation of drainage system around the environment to get rid of stagnant water, burning of natural herb, rubbing of repellents on clothes, use of mosquitoes treated & untreated nets , use of combined chemical for fumigation and spraying of insecticides or pesticides, automatic trapping & killing approach to electronic techniques. The electronic techniques used frequencies that are deterring and allergic to mosquitoes to scare them away without causing harm to humans and environment.

The basis of this work is on the electronic approach with sound frequency technique and its contribution aims to improve on the existing electronic repelling systems and develop a portable, energy saving and rechargeable system. It also incorporates AI camera system for mosquitoes' image processing, and android application for monitoring and control with smart user interface operation.

This research proposed a combined Artificial Intelligent-based system, camera monitoring, sound repelling system, android-enabled user interface mosquito monitoring and control model as a health enhancement remedy. It also creates a reservoir for the traps mosquito to be kept until the room owners come to dispose the accumulated mosquitoes that have been channeled into a waste disposal system designed to trap and hold mosquitoes.

III. METHODOLOGY

A. MATERIALS AND RESOURCES

Software: Proteus, Android studio, Arduino IDE: Arduino Integrated Development Environment, Sublime text, MYSQL, Android Gap and Arduino

Hardware: Arduino Uno, Liquid Crystal Display, GSM Module, Capacitor, Audio Amplifier IC, Voltage Regulator, Light Emitting Diode, Rechargeable Battery, Resistors, Android Phone, Piezoelectric buzzer/Speaker and Bzigo Camera

B. METHODS

i. The System Conceptual Design Model

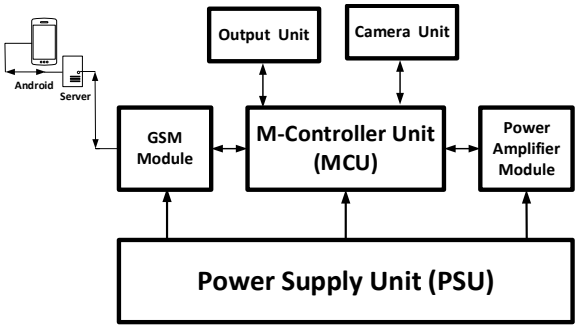


Figure 1: An Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System Architecture

In Figure 1, the conceptual model has the power supply which provides power to the entire system; the power amplifier module which provides the audio amplified sound frequency to scare mosquitoes; the microcontroller unit which coordinates and

initiates the overall monitoring and control actions; GSM module which links the controller action to the android via the server and the output unit. The output unit consists of the light emitting diode to indicate the system ON/OFF status; the Liquid crystal display which gives the physical display of the frequency of the operation and the Sound alarm buzzer which generates sound waves allergic to mosquitoes

ii. ***Software Implementation of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System***

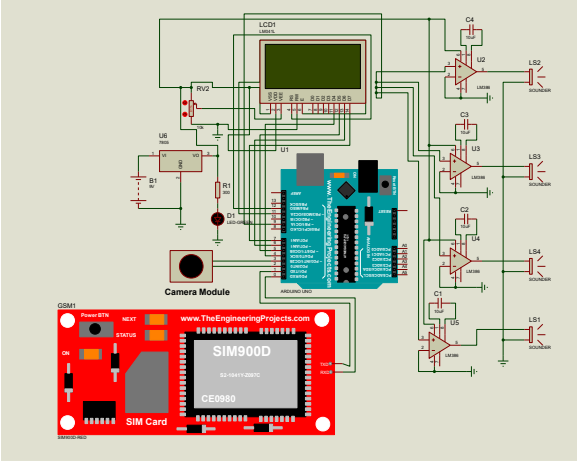


Figure 2: An Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System Circuit

In figure 2, the circuit was simulated with proteus 8.0 and the command code was written in Arduino IDE. The software functionality was ascertained. The design of microcontroller-based device system using piezoelectric sensor was achieved, with the in-built portable rechargeable scheme. The hardware design implementation stage and the remote monitoring and repellent control of Mosquitoes using Android Applications was not implemented during the pre-circuit demonstration.

iii. Hardware Implementation of an Artificial Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

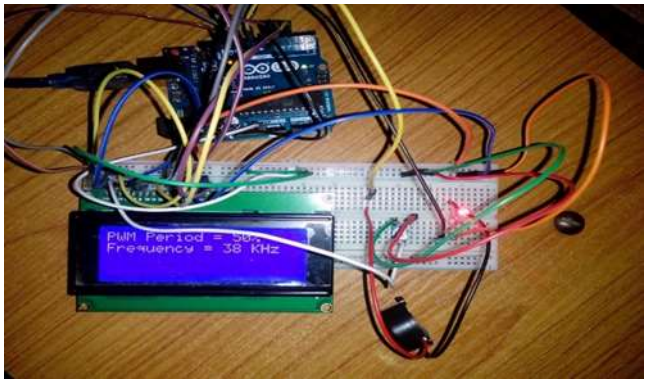


Figure 3: Pre-hardware Validation Test for an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

Figure 3 gives the pre-hardware demonstration test with bread board to ascertain its functionality and to validate the system performances and conformity with design specifications.

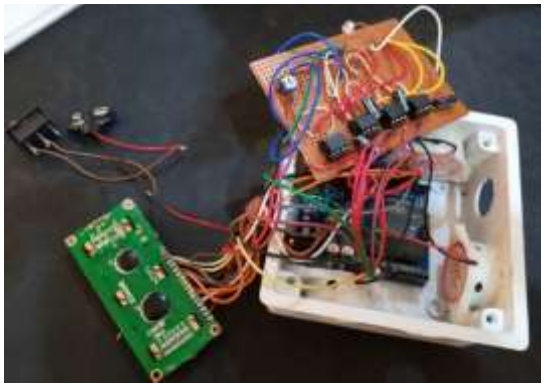


Figure 4: Hardware configuration of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

Figure 4 shows the smart system design configuration without the incorporation of the bzigo camera, the system generates the allergic sound frequency that sends mosquito away from a radius of specified frequency coverage. The bzigo camera system smartly detects when there are mosquitoes in the surrounding and sends the resulting image signal to the controller unit to initiate the repelling action that will scare mosquitoes away. The system will run for 20mintues repelling detected mosquitoes after which it pauses while the environment is being scanned for 10minutes but within the interval, the system can still intelligently come up if there are mosquitoes present.

iv. Flow Chart

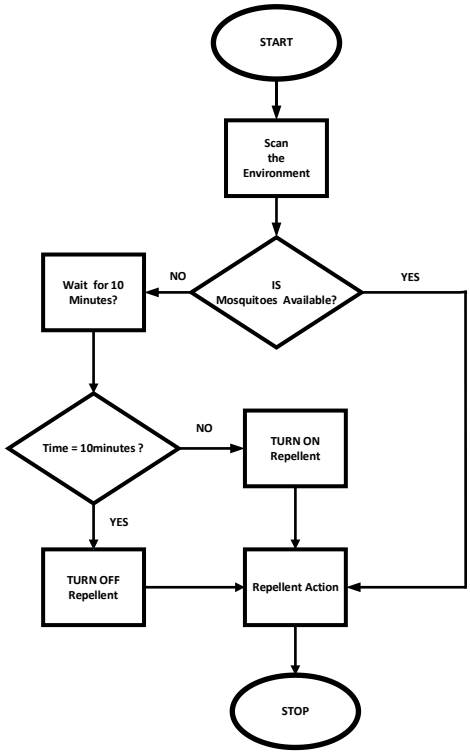


Figure 5: Flowchart of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

v. Android Application design

The android design model used the sublime text to design the signup/sign in page; Graphical user interface for visual observation of the system actions and the database for the documentation were developed using MYSQL. In the sublime text the HTML, CSS and JavaScript code were edited

Figure 6: Android application design for an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

IV. RESULTS, DISCUSSION AND ANALYSIS

A. *The results from the software implementation of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System*

In figure 2, the system was simulated with proteus software, the Arduino uno control was coded with the program code written in Arduino IDE. The embedded program aids the artificial intelligent actions by actuating sound buzzers to produce allergic sound frequency from the operational amplifier (Op-amps) output signal. Figure 4 also provides the soft/hardware preliminarily test platform, where hardware components were connected on a breadboard to ascertain the system functionality. The soft/hardware pre-confirmatory test gives the sound at 38Hz and relates the signal to the android application through the GSM Module.

B. *The results from the hardware implementation of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System*

Figure 6: Hardware implementation of an Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System

Figure 4 shows the hardware implementation of an Intelligent and Android-Enabled user interface mosquitoes monitoring and control system. Figure 6 shows the proposed bzigo camera incorporated system such that when the system smartly detects the presence of mosquitoes in the room at about 1metre distance, the artificial intelligent system initiates the repelling action and after 10minutes will pause while the environment is being scanned. An alert will be sent to the room occupants' phone while mosquitoes will then be driven to reservoir trap for disposal through a connected channel.

C. *The results from the Mobile Application for an Artificial Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System*

Figure 6 shows the signup/in page for the Artificial Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System applications, the new user has to download and install the applications so that when there is an alert from the artificial intelligent system, the message will be displayed for the user to see and on logging in to view his room mosquitoes status from the user machine interface designed on the phone for control purpose. Every room that has this device with its manufacturing part number can monitor and control mosquito activities remotely. With this, there is a database documentary from the android device, the documentary aids the determination of mosquito presence within a certain environment.

V. CONCLUSIONS

An Artificial Intelligent Mosquito Monitoring and Control System Model with Android-enabled User Interface and Bzigo Camera System was developed. These designs add to other known techniques of combating mosquito habitation within a human living environment aimed at stopping malaria spread. Environmental fumigation, use of mosquito treated net; herbal repellent sticks with low smoking technique and the spray of mosquito insecticide chemical repellents which are harmful to human lives and environment will no longer be needed with the advent of this new system. An electronic sprayer for the control of mosquitoes has also not been safe for both environment and humans. This developed Intelligent-based and Android-enabled user interface portable system is a human and environmentally friendly device. The results reveal that the system produces a sound frequency of about 38 kHz to 45kHz which does not permit the existence of mosquitoes within the demonstrated area. The mosquitoes are scared away by the allergic sound frequency from the design after the camera has captured and processed mosquitoes' images to signal the presence of mosquitoes within the experimented area. The artificial intelligent camera now sends a notification via GSM module to the owner's android phone while scaring the mosquito to a specified trap location outside the area of interest for disposal. The design was demonstrated under an indoor space area of 12ft x 12ft confinement. The results from this artificial intelligent and android-enabled user interface mosquito repelling system proved its suitability to replace the conventional human and environmental hazardous approaches. Future research should consider incorporating other systems for further enhancement of this system.

ACKNOWLEDGMENT

We appreciate the Almighty God for his inspiration and guidance which has led to success of this research.

REFERENCE

[1] T. Chaiphongpachara, P. Bunyuen, and K. Khlaeo Chansukh, "Development of a More Effective Mosquito Trapping Box for Vector Control," *Sci. World J.*, vol. 2018, pp. 1–8, 2018.

[2] P. Kantheti and R. D. Kamari, "Use of Mosquito Repellent Devices-Problems and Prospects," *Int. J. Recent Sci. Res.*, vol. 8, no. 1, pp. 15279–15283, 2018.

[3] K. Mendis, A. Rietveld, M. Warsame, A. Bosman, B. Greenwood, and W. H. Wernsdorfer, "From malaria control to eradication: The WHO perspective," *Trop. Med. Int. Heal.*, vol. 14, no. 7, pp. 802–809, 2009.

[4] P. Vijayakumar *et al.*, "IoT based smart mosquito killing

system," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 4, pp. 587–591, 2019.

[5] A. K. Biswas, N. A. Siddique, B. B. Tian, E. Wong, K. A. Caillouet, and Y. Motai, "Design of a fiber-optic sensing mosquito trap," *IEEE Sens. J.*, vol. 13, no. 11, pp. 4423–4431, 2013.

[6] E. L. Moore *et al.*, "An online survey of personal mosquito- repellent strategies," *PeerJ*, vol. 2018, no. 7, pp. 1–25, 2018.

[7] D. Vasconcelos, N. Nunes, M. Ribeiro, C. Prandi, and A. Rogers, "LOCOMOBIS: A low-cost acoustic-based sensing system to monitor and classify mosquitoes," *2019 16th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2019*, pp. 1–6, 2019.

[8] W. H. Organization, *Public Health Significance of Urban Pests*, no. January 2008. 2015.

[9] G. V. Magwili, M. A. E. Latina, F. I. C. Miguel, J. K. P. Ortega, T. K. L. Pastoril, and E. J. D. Tanglao, "Raspberry pi-based medical expert system for pre-diagnosis of mosquito-borne diseases," *2018 IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag. HNICEM 2018*, pp. 1–6, 2019.

[10] S. Rani, S. H. Ahmed, and S. C. Shah, "Smart health: A novel paradigm to control the chickungunya virus," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1306–1311, 2019.

[11] M. Mecoli, V. De Angelis, and S. C. Brailsford, "Modelling the risk of mosquito-borne diseases by system dynamics: The case of human travel between different geographic regions," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, pp. 19–25, 2010.

[12] B. Hur and W. R. Eisenstadt, "Low- power Wireless Climate Monitoring System with RFID Security Access Feature for Mosquito and Pathogen Research," 2014.

[13] G. Paluch, L. Bartholomay, and J. Coats, "Mosquito repellents: A review of chemical structure diversity and olfaction," *Pest Manag. Sci.*, vol. 66, no. 9, pp. 925–935, 2010.

[14] S. Naseem, T. Munir, and M. Faheem Malik, "Mosquito management: A review," *J. Entomol. Zool. Stud.*, vol. 4, no. 5, pp. 73–79, 2016.

[15] A. A. Anuar and N. Yusof, "Methods of imparting mosquito repellent agents and the assessing mosquito repellency on textile," *Fash. Text.*, vol. 3, no. 1, pp. 1–14, 2016.

[16] A. Trivedi, P. Rai, J. Kumar, and C. Ashwin Trivedi, "Formulation of low smoke herbal mosquito repellent sticks by using different essential oils," *~ 173 ~ Pharma Innov. J.*, vol. 7, no. 4, pp. 173–175, 2018.

[17] A. Ranasinghe MSN, "Development of Herbal Mosquito Repellent Formulations," *Int. J. Collab. Res. Intern. Med. Public Heal.*, vol. 8, no. 6, pp. 341–380, 2016.

[18] N. Rani, A. Wany, A. S. Vidyarthi, and D. M. Pandey, "Study of Citronella leaf based herbal mosquito repellents using natural binders," *Curr. Res. Microbiol. Biotechnol.*, vol. 1, no. 3, pp. 98–103, 2013.

[19] B. Kalita, S. Bora, and A. K. Sharma, "Plant Essential Oils As Mosquito Repellent-a Review," *Int. J. Res. Dev. Pharm. Life Sci.*, vol. 3, no. 1, pp. 741–747, 2013.

[20] C. F. S. ANDRADE and V. S. BUENO, "Evaluation of Electronic Mosquito-Repelling Devices Using Aedes albopictus (Skuse) (Diptera: Culicidae)," *Neotrop. Entomol.*, vol. 30, no. 3, pp. 497–499, 2001.

[21] D. K. Tiwari and M. A. Ansari, "Electronic Pest Repellent : A Review," in *2016 International Conference on Innovations in information Embedded and Communication Systems (ICIIECS'16)*, 2016, no. March, pp. 435–439.

[22] P. Anupa Elizabeth, M. S. Mohan, P. P. Samuel, S. R. Pandian, and B. K. Tyagi, "Identification and eradication of mosquito breeding sites using wireless networking and electromechanical technologies," *2014 Int. Conf. Recent Trends Inf. Technol. ICRTIT 2014*, 2014.

[23] L. Alphey *et al.*, "Sterile-Insect Methods for Control of Mosquito-borne Diseases: An Analysis," vol. 10, no. 3, pp. 295–311, 2010.

[24] J. Bouyer, H. Yamada, R. Pereira, K. Bourtzis, and M. J. B. Vreysen, "Phased Conditional Approach for Mosquito Management Using Sterile Insect Technique," *Trends Parasitol.*, vol. 36, no. 4, pp. 325–336, 2020.

[25] D. Sunehra, "Article ID: IJARET_10_02_046 Cite this Article: Dr. Dhiraj Sunehra, Solar Energy Driven Mosquito Repeller System Using Arduino Uno," *Int. J. Adv. Res. Eng. Technol.*, vol. 10, no. 2, pp. 472–481, 2019.

[26] J. Wyngaard, S. S. C. Rund, G. R. Madey, and J. Cleland-huang, "for Mosquito-borne Disease Research and Control," *2018 IEEE/ACM 40th Int. Conf. Softw. Eng. Companion*, pp. 226–227, 2018.

[27] Y. Chen, A. Why, G. Batista, A. Mafra-Neto, and E. Keogh, "Flying Insect Classification with Inexpensive Sensors," *J. Insect Behav.*, vol. 27, no. 5, pp. 657–677, 2014.

[28] J. Wang, S. Zhu, Y. Lin, S. Svanberg, and G. Zhao, "Mosquito counting system based on optical sensing," *Appl. Phys. B Lasers Opt.*, vol. 126, no. 2, pp. 1–10, 2020.

[29] J. Spitzen and W. Takken, "Keeping track of mosquitoes: A review of tools to track, record and analyse mosquito flight," *Parasites and Vectors*, vol. 11, no. 1, pp. 1–11, 2018.

[30] D.Takahshi and W.Kyle,"Bzigo Uses AI and Laser to Locate Mosquitoes in your home", Special Issue: AI and Surveillence.https://hitecher.com/news/go-mosquito-hunting-with-a-bzigo-laser-detector

Saturation and Value-Based Luminance Enhancement Model

B.O Sadiq, M.A. Isa-Bello, O. Ajayi, A.D. Adekale
Computer Engineering Department
Ahmadu Bello University
Zaria, Nigeria
bosadiq@abu.edu.ng,
bintghazall@gmail.com,
aoreofe@abu.edu.ng
adekale@abu.edu.ng

O.S Zakariyya
Electrical and Electronics Engineering Department
University of Ilorin
Kwara, Nigeria
zakariyya.os@unilorin.edu.ng

H. Bello
Electronics and Telecommunications
Ahmadu Bello University
Zaria, Nigeria
koachila@yahoo.com

Abstract— **This paper presents a saturation and value-based Luminance Enhancement Model (LEM) for colored images. The LEM was modified to addresses the issue of noise amplification associated with the use of a Laplacian filter in image enhancement. The images which were originally in RGB format were converted to HSV format to ensure a more stable performance of the model. A mathematical model was developed and applied to the formatted HSV image. The result obtained from the developed model is presented and benchmarked against the existing methods of color enhancement using the HSV color space. Simulations of the developed model were achieved using MATLAB. A Structural Similarity Index (SSIM) and Peak-to-Signal Noise Ratio (PSNR) of 67.9 and 0.8901 respectively were obtained using the developed model. The obtained results showed significant improvement over existing models.**

Keywords—color image, CLAHE, Laplacian Filter, Enhancement

I. INTRODUCTION

Image enhancement techniques as a tool are used to manipulate digital image constituent to make the resulting output improved as compared to the original [1] – [4]. The image can be enhanced in its natural format as in spatial domain techniques or transform to another domain before enhancement as in transform domain techniques [5], [6]. RGB and HSV color model is used in image enhancement. But, the HSV color model is mostly used because of the fact that color manipulations perform better in HSV color space than in RGB color space. Fig. 1. depicts the HSV color space model.

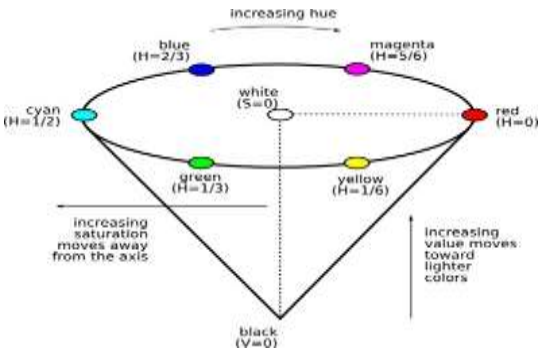


Fig.1: HSV colour Space [1]

Image enhancement is an aspect of image processing research that has caught the attention of researchers due to its areas of applications such as medicine and satellite technology. However, enhancing the images in these domains requires techniques that are dependent on the type of images used. This necessitates the need to develop an improved enhancement technique that can achieve a reasonable result in a wide variety of images [4].

The domains of image enhancement are the spatial and frequency domains. Nonetheless, for real-time applications, spatial domain enhancement has been proven to be efficient and reliable. Therefore, the spatial domain enhancement technique is the focus of this paper. Sobel, Prewitt, Roberts, Canny, Laplacian amongst others are the typically used spatial domain filters. But, the peculiarity of the Laplacian filter is that it can determine sharp changes in pixels values. This makes it mostly the choice of many candidate's researchers as against others. However, the use of the Laplacian filter is limited by noise amplification.

Therefore, the paper proposes the development of saturation and value-based enhancement model that will reduce noise amplification with the use of the Laplacian filter to the barest minimum.

II. RELATED WORKS

Pertinent related works are reviewed as follows: The work of [7] proposed a local based spatial processing technique for color image enhancement. This technique used the luminance component of the image, thereby enhancing the contrast based on neighborhood dependency. The overall tone of the enhanced image is then enhanced using local gamma correction, although their approach displays significant improvement based on colorfulness and proportion of the number of saturated pixels as related with existing techniques like Dualistic sub-image Histogram Equalization (DSIHE), Histogram Equalization (HE) and Brightness preserving Bi-Histogram Equalization (BBHE). But it is only effective for images with non-uniform luminance.

Authors in [8] combined the histogram equalization with the magnitude compression procedure, color stretching process, and saturation maximization for color image enhancement. The approach showed a reduced artifact with improved contrast and colorfulness. However, the details in the image are not effectively enhanced. This was due to the inconsideration of edge preservation in the image.

This was also the case of the work of [9] where the sigmoid function was first used to enhance satellite images, after which the gamma correction employed for intensity preservation and multi-objective particle swarm optimization (PSO) was used to control over-enhancement and artifacts.

The authors in [10] Illuminated each pixel by first estimating and individually determining the optimal value of the RGB channels that will provide Low-light image enhancement. The final map was generated using the illumination map through structure refinement. Though this method has lower lightness order error as compared with HE, Adaptive Histogram Equalization (AHE), GC, and CVC it involves a lot of weighting value and approximation analysis that make it unsuitable for practical application.

A kneen transfer and gamma correction are applied to dark satellite images for enhancement as proposed by [11]. The dark low contrast satellite image acquired as test data were decomposed into four quadrants which are LL, LH, HL, and HH with a view to estimating the singular value matrix. Inverse DWT is applied to these quadrants separately and then combined to obtain the enhanced image. In comparison with conventional methods like gamma correction, BPFDHE, and GHE, the contrast and local details are better improved by the proposed technique. However, it results in an exaggeration of image inherent noise towards the edges which may lead to loss of useful information.

[12] presented an iterative mean filter for image denoising with a view to improving the image quality. The presented model addressed a salt and pepper type of noise that degrades the quality of an image. Fixed-size of the window was used to justify the effectiveness of the algorithm. Using a fixed-size window increases accuracy and processing speed but inadequately removes noise.

A cascade filter was presented by [13] that was capable of removing salt and pepper noise of high-density in colored images. The developed algorithm made use of a clipped median filter based on pixel values for image restoration. Nonetheless, the use of the median filter for saturation and value-based enhancement is not efficient in the RGB space model.

Nonetheless, past research works in image processing have presented an enhancement model as in equation (1) and (2). This equation tunes the Saturation (A) and Value (B) component of an image in the HSV model. This is intending to improve the image quality and reduce the problem of the existing techniques to the barest minimum [14], [15].

$$\rho(\mathrm{g},\mathrm{h}) = \sum \frac{[\mathrm{B}(\mathrm{g},\mathrm{h}) - B_a(\mathrm{g},\mathrm{h})],[\mathrm{A}(\mathrm{g},\mathrm{h}) - A_a(\mathrm{g},\mathrm{h})]}{\sqrt{\sigma_B^2(\mathrm{g},\mathrm{h}),\sigma_A^2(\mathrm{g},\mathrm{h})}} \quad (1)$$

$$B_{enh} = B(\mathrm{g},\mathrm{h}) + K_1[\mathrm{B}(\mathrm{g},\mathrm{h}) - B_a(\mathrm{g},\mathrm{h})] - K_2[\mathrm{A}(\mathrm{g},\mathrm{h}) - A_a(\mathrm{g},\mathrm{h})]X\rho(\mathrm{g},\mathrm{h}) \quad (2)$$

However, this paper seeks to readdress the model developed and presents an improved model with a view to achieving a better-enhanced image.

III. PROPOSED TECHNIQUE

The proposed enhancement model is discussed as follows:

Step I: Image Manipulation

Input: Load RGB Image and convert into HSV and the A and B component will be filtered using the Laplacian filter to give A_a and B_a as presented by the work of [16] and [17]. The A_a and B_a are input to the modified processing block.

Step II: Modified Enhanced Processing Block
The variance and correlation are calculated and this is used to enhance the Laplacian filtered B_a using equations (3) and (4)

$$B_{variance} = \sigma_B^2(\mathrm{g},\mathrm{h}) = \sum[\mathrm{B}(i,j) - B_a]^2 \quad (3)$$

$$A_{variance} = \sigma_A^2(\mathrm{g},\mathrm{h}) = \sum[\mathrm{A}(i,j) - A_a]^2 \quad (4)$$

Both A and B variance serves as the input to the correlation and final enhancement. The equations for correlation and enhancement are presented in equation (5) and (6).

$$\rho(\mathrm{g},\mathrm{h}) = \sum \frac{[\mathrm{B}(\mathrm{g},\mathrm{h}) - \sigma_B^2(\mathrm{g},\mathrm{h})],[\mathrm{A}(\mathrm{g},\mathrm{h}) - \sigma_A^2(\mathrm{g},\mathrm{h})]}{\sqrt{\sigma_B^2(\mathrm{g},\mathrm{h}),\sigma_A^2(\mathrm{g},\mathrm{h})}} \quad (5)$$

$$B_{enh} = B(\mathrm{g},\mathrm{h}) + K_1[\mathrm{B}(\mathrm{g},\mathrm{h}) - \sigma_B^2(\mathrm{g},\mathrm{h})] - K_2[\mathrm{A}(\mathrm{g},\mathrm{h}) - \sigma_A^2(\mathrm{g},\mathrm{h})]X\rho(\mathrm{g},\mathrm{h}) \quad (6)$$

The modification is done in the correlation phase and final B enhancement where the B_a and A_a is replaced with $B_{variance}$ and $A_{variance}$ respectively

Step III: Contrast enhancement:
The output of contrast after subjecting it to the Laplacian filter is enhanced using a fixed value of gamma 0.77 [14].

$$A_{enh} = A^{0.77} \quad (7)$$

Enhanced luminance (B_{enh}) and contrast (A_{enh})is added to Hue and converted to RGB to get the final enhanced image. Table 1 presents the pseudocode for the proposed Luminamance Enhancement Model (LEM).

TABLE 1: PROPOSED LEM ALGORITHM.

Algorithm: Luminance Enhancement

Start
Input: Input Original Color Image
RGB ⟶ HSV: Convert RGB to HSV
Laplacian filter: compute S and V
component of Processing Block:
    Use Equations 3 and 4 to find $B_{variance}$ and $A_{variance}$
    Compute the Correlation and Luminance Enhancement using equations 5 and 6
Colour Enhancement:
    Enhance overall saturation component using equation (7)
end

IV. EXPERIMENTAL RESULT AND ANALYSIS

Standard test images were used to test the developed luminance enhancement model. These test images were retrieved from standard databases [18]. The Structural Similarity Index (SSIM) and Peak Signal-to-Noise Ratio (PSNR) as shown in equations (8) and (9) was used to determine the performance of the luminance enhancement model.

$$SSIM = \frac{(2M_0M_i + C_1)(2CV_{0i} + C_2)}{(M_0^2 + M_i^2 + C_1)(SD_0^2 + SD_i^2 + C_2)} \quad (8)$$

Where,

M_oM_i : is the mean of the input and output image

CV_{oi} : is the cross co-variance for both images

SD_0 : is the standard deviation of the output image

SD_i is the standard deviation of the input image

$$PSNR = 10\log_{10}\left[\frac{255^2}{MSE}\right] \quad (9)$$

Where MSE is given by [12]

$$MSE = \frac{\sum_{r,b}(I_0(r,b) - I_p(r,b))^2}{rb} \quad (10)$$

Where,

r and b are the number row and column in the image respectively

$I_0(r, b)$ is the output image

$I_p(r, b)$ is the input image.

The test images are presented in Fig. 2 (a-h)

(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

Fig.2 Test Images

V. PERFORMANCE ANALYSIS

The performance of the Luminance Enhancement Model was determined using the standard test images of Fig. 2 (a-h) which are of poor quality using PSNR and SSIM as presented in Table 1. From the generated results and as presented in Fig. 3 (a-h), it is evident that the LEM outperformed the existing models that used the HSV color space. However, the plate number in output in Fig. 3 (d) had cracked characters which imply that the model cannot perform effectively on images with numbers. But, nonetheless, the general image was adequately enhanced.

Table 2: PSNR and SSIM comparison of the proposed algorithm and Laplacian-CLAHE

VALIDATION OF LEM.

No	*Test Image*	*LEM*		*[14][15]*	
		PSNR	*SSIM*	*PSNR*	*SSIM*
1	butterfly	66.5140	0.8901	28.3227	0.6636
2	Clinmill	72.1548	0.8811	29.5946	0.6311
3	flower	84.8484	0.9174	29.6242	0.5466
4	voit	57.4388	0.9383	28.3812	0.7245
5	Tulips	57.6491	0.8414	27.5110	0.4976
6	peppers	62.4335	0.9011	29.9763	0.7261
7	Barnfall	76.2424	0.8337	29.6223	0.5219
8	bodie	66.1341	0.8886	30.7823	0.5677

Table 2 presented the comparison of LEM with the Laplacian-CLAHE enhancement model. To further ascertain the efficiency of LEM it was compared with other enhancement models by various researchers on an average PSNR of 67.9. While Gang Song et al [19] achieved PSNR of 32.3 and Hanumantharaju et al [15] achieved a PSNR of 32.5

VI. VISUAL ANALYSIS

Since the paper implemented a luminance enhancement model, the efficiency of the model was tested on the standard dataset presented in Fig. 2 (a-h). The images were fed directly as input to the model and visual output generated enhancement images using LEM are presented in Fig. 3 (a-h)

(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

VII. CONCLUSION

This paper proposes the development of a saturation and value-based enhancement model that will reduce noise amplification with the use of the Laplacian filter to the barest minimum. Most of the enhancement models are based on the RGB color space. However, color manipulations are not adequately achieved in this space. Thus, leading to difficulty in image enhancement. As such, based on the HSV color model, an improved luminance enhancement model is presented in this paper. The result obtained showed that the proposed LEM performed effectively on most of the images except for the image that has number plate were the characters in the plate was cracked. Further work will consider the use of metaheuristics to optimize the filter as well as improving the LEM to support character enhancement.

REFERENCES

[1] I. T. Young, J. J. Gerbrands, and L. J. van Vliet, *Fundamentals of Image Processing*, 2.3. Netherlands: Delft University of Technology, Mekelweg 5, 2628 CD Delft, Netherlands, 2007.

[2] K. R. Castleman, *Digital Image Processing*. Prentice Hall Professional Technical Reference ©1979, 1979.

[3] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd Editio., no. September. Pearson Prentice Hall Pearson Education, Inc. Upper Saddle River, New Jersey 07458, 2008.

[4] A. C. Bovik, *The Essential Guide to Image Processing*. Academic Press, Inc. Orlando, FL, USA ©2009, 2009.

[5] Bashir Olaniyi Sadiq, Emmanuel Okechukwu Ochia, Olayinka Sikiru Zakariyya, Abdulazeez Femi Salami. On the Accuracy of Edge Detectors in Number Plate Extractor. *Baltic Journal of Modern Computing,* 7(1), 19-30, 2019.

[6] B. O. Sadiq, S.M Sani, S. Garba. Edge Detection: A Collection of Pixel Based Approach for Coloured Imaged. *International Journal of Computer and Its Applications (IJCA),* 113(5), pp. 29-32, 2015.

[7] B. O. Sadiq, S.M Sani, S. Garba. An Approach to Improving Edge Detection for Facial and Remotely Sensed Images Using Vector Order Statistics. *International Journal of Multimedia and Its Application (IJMA),* 7(1), pp.29-32, 2015.

[8] C. Y. Wong *et al.*, "Histogram equalization and optimal profile compression-based approach for color image enhancement," *ElsevierJ. Vis. Commun. Image Recognit.*, vol. 38, pp. 802–813, 2016.

[9] R. Malik, R. Dhir, and S. K. Mittal, "Remote sensing and Landsat image enhancement using multiobjective PSO based local detail enhancement," *J. Ambient Intell. Humaniz. Comput.*, 2018.

[10] X. Guo, Y. Li, and H. Ling, "LIME: Low-Light Image Enhancement via Illumination Map Estimation," *IEEE Trans. Image Process.*, vol. 26, no. 2, pp. 982–993, 2016.

[11] A. K. Bhandari, A. Kumar, G. K. Singh, and V. Soni, "Dark satellite image enhancement using knee transfer function and gamma correction based on DWT–SVD," *Springer Multidimentional Syst. Signal Process*, 2015.

[12] Uğur Erkan, Dang Ngoc Hoang Thanh, Le Minh Hieu, Serdar Enginoğlu. An Iterative Mean Filter for Image Denoising. *IEEE Access,* pp. 167848- 167859, November 2019

[13] B. Karthik, T. Krishna Kumar, S. P. Vijayaragavan, M. Sriram. Removal of high-density salt and pepper noise in color image through modified cascaded filter. *Springer Journal of Ambient Intelligence and Humanized Computing*, pp.1-8, August 2020

[14] S. Bhairannawar, A. Patil, A. Janmane, and M. Huilgol, "Color image enhancement using Laplacian filter and contrast limited adaptive histogram equalization," *2017 Innov. Power Adv. Comput. Technol. i- PACT 2017*, vol. 2017–Janua, pp. 1–5, 2017.

[15] M. C Hanumantharaju, M. Ravishankar, D. R. Rameshbabu. Adaptive Color Image Enhancement Based Geometric Mean Filter. *International Conference of Communication, Computing & Security,* pp.*403*-408, 2011.

[16] S.S. Bedi and RatiKhandelwal, "Various Image Enhancement Techniques -A Critical Review", International Journal of Advanced Research in Computer and Communication Engineering, pp.1605-1609, March 2013.

[17] J.A, Ojo, I.D Solomon, Adeniran S.A, "Contrast Enhancement Algorithm for Colour Images", 2015 Science and Information Conference (SAI), pp. 555-559, July 2015.

[18] Dileep MD, A. Sreenivasa Murthy, "A Comparison between different Colour Image Contrast Enhancement Algorithms", International Conference on Emerging Trends in Electrical and Computer Technology, pp. 708-712, March 2011.

[19] Gang Song and Xiang-Lei Qiao, "Color Imagne Enhancement based on Luminance and Saturation Components", Proceedings of International Congress on Image and Signal Processing, 2008.

Optimizing ICT Resources to Mitigate Contagion:A Case Study of COVID-19 Pandemic

James Kunle Olorundare,
Technical Standards and Network Integrity,
Nigerian Communications Commission,
Abuja, Nigeria
Email:olorundarek@ncc.gov.ng

Adebimpe Olubunmi Olorundare,
Information Technology Department,
National Open University of Nigeria,
Abuja, Nigeria.
Email:bolorundare@gmail.*com*

Abstract— ***COVID-19 is ravaging many countries and there are unprecedented challenges in managing the pandemic. Basically, two strategies are being adopted; Traditional Health System and Telehealth which include telemedicine, remote monitoring of patient, Use of Artificial Intelligence (AI) etc. This paper discusses how the communications and computing resources are being used in the telehealth sector to respond to COVID -19. It expands the impact of telehealth on the general approach of pandemic management and how this is rapidly flattening the curve of COVID-19 pandemic as seen in the country experiences of China and South Korea discussed. The research validated the quantitative survey conducted vis-à-vis the experiences of countries discussed and provided recommendations to fill the gap noticed in mitigating pandemic by optimizing ICT resources and infrastructures.***

Keywords— Mobile technology, Information and Communications Technology (ICT), Telehealth (ehealth or e-health), Mobile App, Artificial Intelligence (AI), Coronavirus Disease (COVID-19). Pandemic

I. INTRODUCTION

ICT infrastructure can be used to improve our healthcare system through the deployment of electronic health system on Information and Communication Technology platform as it is now being used during the COVID-19 pandemic either directly as in telehealth or indirectly as in such applications like telecommuting, e-commerce etc. Never before has ICT infrastructures been so critical to our society day- to-day activities. Routines such as general safety to mitigate COVID-19, health management, commercial activities etc are few examples of how communications networks and other IT infrastructures are adding values to our health sector. With the pressure on the health system. The ICT resources are being optimized for higher efficiency in order to fast track the mitigation of COVID-19.

The issue of social distancing and stay-at-home to prevent the spread of COVID-19 are now being facilitated by the use of ICT infrastructures. A survey conducted to find out how ICT resources can facilitate the suppression of COVID -19 was conducted and analyzed. The result discussed below showed that ICT tools are very key in combatting COVID-19 pandemic. And hence the need to optimize the ICT resources for utmost performance. The objective of the paper is to show how ICT resources can be used to mitigate COVID-19. The motivation stemmed from the need to find alternative way to suppress COVID-19 as the traditional medical infrastructures are being overstretched all over the world. The scope of the paper is quite global since COVID-19 is a global pandemic and the survey conducted cut across many continents.

The paper from this point is arranged as follows: Literature review which is followed by methodology and data analysis followed by country experiences of selected countries based on unique scenarios in which specific strategies of ICT resources benefits are analyzed. These include, Telecommuting, E-commerce, Telehealth and others. Recommendations are made in section V which is followed by conclusion and future research work in section VI.

II. LITERATURE REVIEW

The COVID-19 pandemic has spread to many countries on the surface of the earth and the traditional health system of the world is being tested to its full capacity. There is a strong need to reduce the stress on the traditional health system. One of the promising techniques is the use of Information and Communication Technology to boost the performance of the health systems of many countries in terms of electronic health system or eHealth. eHealth is the deployment and application of Information and Communication Technology (ICT) for health and to optimize the health system. The eHealth can be said to be capacity expansion of the already existing traditional health system by the applications and optimization of ICT infrastructures. However, many countries have not really looked at how ICT resources can be optimized for mitigation in pandemic situation like COVID-19. And this is the gap the research intends to fill since COVID-19 pandemic is novel.

"Optimizing ICT resources to mitigate contagion: A case study of COVID-19 Pandemic" is the theme of this paper which came up as a result of COVID-19 pandemic currently ravaging the world (year 2020) and the need to get rid of the pandemic. The traditional health system cannot handle this pandemic alone because of the contagious nature of the pandemic. Hence, the need to employ the ICT resources. However, the ICT resources are being used for so many applications including ehealth. In order to get better result

from using ICT resources to mitigate COVID-19 pandemic, it is important that the resources are optimized for increased efficiency. Contagion is "a disease that can be spread by people touching each other" [1].

The objectives of ehealth in each country is to promote and strengthen the use of ICT in health development from field applications to hospital procedure applications which can also include inter-state or interregional hospital connectivity and usage [2]. E-Health (it is the same as ehealth) is a new healthcare strategy which is still a developing practice that can only be achieved through the use of electronic processes and communication technologies [3]. E-health cannot be implemented without ICT resources. Hence, the baseline of applying ehealth is availability of ICT resources. And this can be excellent resources during pandemic and the question this research would answer is how ICT resources can be optimized to mitigate COVID-19 pandemic.

There exists an appreciable development in health Information Technology especially with respect to sharing of information due to the seamless presence of the Internet which makes it easy and also broadband technology has brought the use of telemedicine which makes it possible for experts to be able to attend to patient in another location. This is a borderless service based on the use of Information and Communications Technologies [4]. Telemedicine would be an excellent tool to be harnessed against CORVID-19 pandemic which is already taking its toll on the medical practitioners because of many infected people to attend to in the hospital. Hence the need to optimize ICT resources as alternative mitigating techniques.

Digital divide between the developed and the developing countries of the world is visible. This can be seen in the distribution of benefits from ICT that created global imbalance. For instance, United States of America and China account for 75% of all patents related to blockchain technologies, 50% of global spending on IoT, 75% of the cloud computing market in addition to that, about 90% of the market capitalization value of the world's 70 largest digital platforms. This implies that there is huge digital divides in the world and half of the world population is still offline. This can be seen in the availability of communications infrastructures like broadband facilities and this digital divide also translate into the availability of telemedicine facilities and other technologies that can be used in the treatment of COVID-19 [5]. Regardless, ICT resources are needed to compliment traditional health system to combat COVID-19. How to optimize the ICT resources for this purpose will be discussed.

In a pandemic situation like COVID-19, eHealth in general, and telemedicine in particular can be a vital resource to remote regions of emerging and developing countries but it is often challenging to establish because of inadequate ICT infrastructure[5] For instance, in this COVID-19 pandemic Nigeria is trying to set up more laboratories to test samples and, availability of enough reagent is also a challenge in Nigeria in the early days of the pandemic. The difficult financial situation in many African states implies that the majority of the African countries are poorly treated medically. In many developing countries, it is not only about insufficient facilities and trained manpower, but lack of accessibility to eHealth because of inadequate broadband facilities and access to the Internet access in unserved villages [6]. This is a serious challenge in time of COVID pandemic. There is need to devise strategy to optimize the available ICT resources. Developed countries are also grappling with coping with the pandemic because of the rate of infection and it is only feasible to rely on optimizing communications and telecommunications infrastructure to flatten the effect of COVID -19. This is what this paper intends to establish and proffer harmonized strategic solutions.

Self-monitoring is the use of sensors or tools which are readily available to the general public to track and record personal data. The sensors are usually wearable devices and the tools are digitally available through mobile device applications. From a survey conducted and reported by Olorundare et al, majority of Nigerians would really want self-monitoring system which is a good development in time of pandemic like the COVID-19. This implies that if health application is deployed using IoT monitoring systems, it will be embraced and this will help to reduce the rate of infection and in a short time, the rate of infection will be flatten through self-distancing and stay at home while those under quarantine can still be monitored without further exposing the health workers managing the sick. This is one of the advantages of self-monitoring system based on ehealth [7].

Telecoms operators and other ICT service providers are recognizing that their customers will rely on ICT services during stay-at-home in order to flatten the rate of spread; self-isolation for those that have contacted COVID-19 and unconfirmed cases still being tested and quarantine for those with confirmed COVID-19 cases. The overarching objectives are for working at home, personal or family entertainment and maintaining social connections with others. Also, for accurate information broadcast to all.

Operators in countries like France, Australia, Saudi Arabia, Bahrain, Russia and Belgium for the purpose of illustration have started working on an increasing or removal of data caps, or even free unlimited Internet especially for fixed subscribers [8]. The importance of this is for their citizens that are subscribers to those operators services to be seamlessly connected so that they can communicate in time of emergency for medical crisis or for them to be able to do away with boredom in terms of entertainments or to be able to do electronic transaction for the purpose of receiving or transferring money or to buy essentials online like facemask, food, groceries etc. This paper intends to itemize strategies on how ICT resources can be optimized for the purpose of mitigating COVID-19 pandemic.

III. METHODOLOGY AND DATA ANALYSIS

i. Research Methodology

Secondary data are the already existing data collected by the investigators and this was collected and reviewed under the literature review in Section 2 above. It shows the relevant research works to the theme being researched the existing gap and to advance this work, the researchers conducted primary research using Quantitative Survey technique which was responded to within a week because it was conducted in the middle of COVID-19 pandemic April 2020. The Primary data collection source for this research was collected through a survey at [9].

ii. Survey Questions, Infographics and Analysis

1. A survey of 10 key research questions was carried out in April 2020 and there were 100 responses in less than a week based on the trendy nature of the survey. Out of 100 respondents 87 respondents are from Nigeria and other parts of the world also responded except Australia with no response because of the random selection of respondents. The pie chart below fig.1. represents the proportional distribution of the respondents.

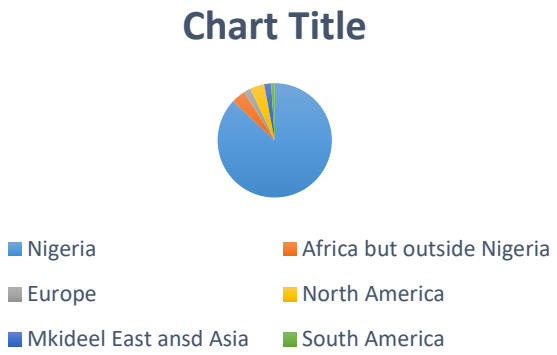


Fig. 1: A Pie Chart showing distribution of 100 respondents.

2. What is your educational level? The Bar Chart in Fig.2 below depicts the education level distribution of the respondents. It shows that 99% of the respondents have at least University degree which shows that they can understand the survey being answered correctly. This implies that the survey is valid and the result can be relied on because the respondents understand the survey.

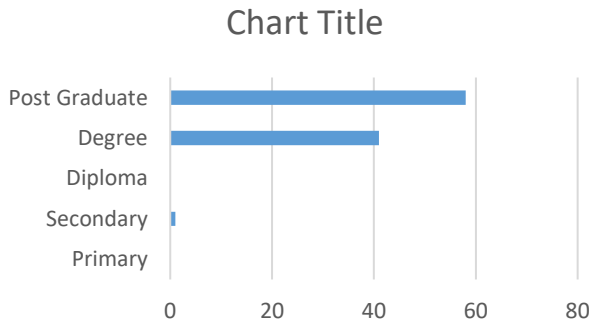


Fig. 2: A Bar Chart showing the level of education for the respondents

3. Do you know about COVID-19 pandemic? This is a question to confirm if the respondents have fundamental knowledge of the survey. 97 out of 100 respondents know about the COVID-19 Pandemic which shows that the survey can be relied on and the responses are valid.

4. Do you know about Information and Communications Technologies, and their applications? This deals with how to what extent the respondents are familiar with Information and Communication Technology and what it can be used for. The results showed that majority of the respondents have good knowledge of ICT as shown in Bar Char in Figure 3 below.

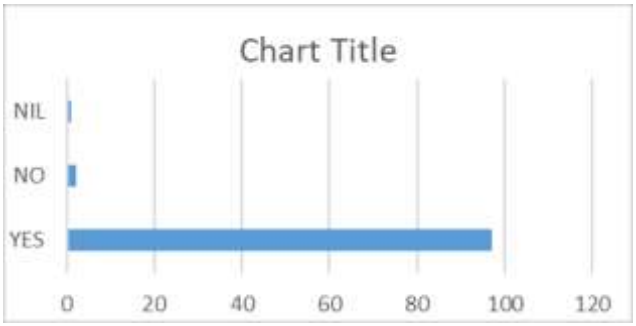


Fig. 3: Bar Chart showing the answer to knowledge of ICT.

5. Do you know that Robotics, Artificial Intelligence and other emerging technologies can be used to reduce the exposure of medical practitioners to COVID-19 contagion? 86% of the respondents answered in affirmative while 13% answered no and one respondent skipped. With this results majority of the respondents know that Robotics or Artificial Intelligence can be used in one way or the other to help in combatting COVID-19 contagion. The use cases in Section 4 below established and confirmed the knowledge of the majority of the respondent in this key research question.

6. Can e-commerce (online store where you can buy food and other essentials) help to maintain, stay-at-home order, quarantine, isolation, during COVID-19 contagion? 97 % of the respondents answered in affirmative and 2% answered in Negative and1% did not answer, This is valid and based on what is obtainable during the COVID-19 contagion, the answer confirmed that e-commerce is one of the ICT channels that can facilitate effective isolation, stay-at-home order which can help to combat contagion like COVID-19. The illustration in section 4 on China and South Korea experiences can also point to the validity of the survey.

7. Can national emergency number information center, mobile network SMS broadcast, national agencies social media information dissemination help in educating the citizenry and broadcasting correct information on COVID-19 hence, reduced misinformation in the public space? From the table below (Table 1), 89% responded in affirmative to the question showing that majority are on the side that ICT tools like emergency number information center; Short Message Service (SMS) broadcast by Mobile Network Operator to give current and accurate information; Social Media pages wall and twitter handles of national agencies giving timely and accurate information can help in as much as one of these facilities can be accessed either in well-served or underserved area. However, unserved areas exist but the number of totally unserved places could be minimal and that can be explained from variance in answer like both,

"Yes to a certain extent" and "No" can also come up in such areas as answers. Looking at the distribution of the answers, the frequency of "yes" shows that the above ICT media/channels would help a great deal if deployed.

S/N	RESPONSE	FREQUENCY
1	NO	3
2	YES	89
3	BOTH	1
4	NO ANSWER	6
5	YES, CERTAIN EXTENT	1

Table 1: Table showing distribution of answer to Question 7 above

8. Can ICT applications such as Internet of Things, Robotics, Artificial Intelligence, Telecommunications Networks, Drones (UAV) applications help in reducing rate of COVID-19 infection propagation? Fig. 4 below shows the distribution of answers given by respondents. The descending order showed that ICT applications like IoT, Artificial Intelligence, Drones etc can help in reducing COVID-19 infection propagation through different applications. The illustration in Section 4 below is a validation of the majority answer to the survey and using pareto chart for grouping the frequency: "A lot" can be added to "A great deal" and "moderate" that is at the center of pareto chart, can be neutral and "Non at all", "No answer" and "a little" can be grouped on the negative. This gives a very large percentage of affirmative as shown in pareto chart Figure 4 below. The importance of pareto chart is to group answers in a progressive order and that has been established.

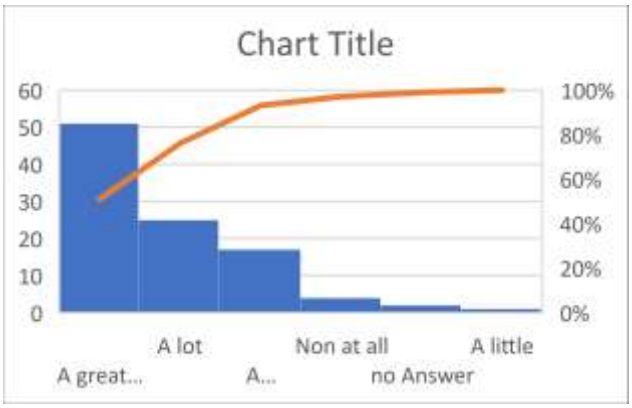


Fig. 4: A Pareto Chart showing the distribution of responses in descending order of frequency

9. If we work from home based on Stay-at-Home order, can that help to reduce rate of COVID-19 infection propagation? Fig. 5 below is a pie chart showing that 96% of the respondents agreed with the fact that working from home is part of the solution to reduce COVID-19 infection propagation. To work from home, there is need for robust Internet system which will connect us with our colleagues and other staff from the same office for proper organization and job process flow. Also, the use of mobile phone which is also part of the ICT tools is very key to being able to work from home effectively. This implies that the use of telecommunications networks, Internet and other ICT tools like laptops, desktop computers which are connected on the Internet either from direct access, Virtual Private Networks, intranet, extranet or any other type of connection is an integral part of working from home. Hence, this will help to combat COVID-19 contagion going by the large percentage of affirmative answers to "working from home" as recorded in the survey. Fig. 5 below shows the answer to this survey question.

Fig. 5: A Pie Chart showing that majority of respondents agreed with Working from home as a solution to COVID-19 infection Propagation

10. In your own word, how do you think ICT resources can be optimized to reduce COVID-19 infection propagation rate?

There are 88 free comments made and up to 70% agreed through different media that the following can help:

i. ICT infrastructures
ii. Internet of Things applications and smart systems
iii. Artificial intelligence applications
iv. E-commerce and telecommuting
v. Mobile Telephony
vi. Telemedicine
vii. Broadband facilities
viii. Drones
ix. Policies on Electronic activities like E-commerce, Telecommuting etc

All these point to the fact that optimization of ICT tools and infrastructures can help to combat pandemic like COVID-19 contagion directly or indirectly and the illustration of country experience below also established this valid point.

IV. COUNTRY EXPERIENCE TO ILLUSTRATE OPTIMISATION OF ICT RESOURCES:

4.1 China COVID -19

The Chinese government used strategy of Quick Responses together with Intense and Rapid Contact Tracing. In addition to surveillance of potential contacts and Isolation. But the COVID-19 pandemic rate of infection was high and e-Health based on ICT infrastructures were applied as explained below [10]. This is a validation of the quantitative survey analyzed in section III above.

A. The country implemented large-scale contact tracing in the early 2000s during the SARS epidemic. China learnt from SARS of 2002-2003 by setting up large-scale surveillance system which can implement contact tracing by identifying and tracking people who may have been in contact with an infected person. The system is "idiot-proof"

and if a tracer makes a mistake on questionnaire or forms, the screen would flash a yellow color alert on the screen [10].

B. China used technology that aims to trace every single COVID-19 case.

The Emergency centers in china is used to track the virus using huge screen to display the critical cluster of the virus for proper surveillance, monitoring and to arrest the situation. This is in addition to Chinese social media including Weibo (a microblogging website and app which compares to twitter and Instagram) , Tencent (specializes in social networking, music, web-portals, e-commerce, mobile games and other internet services) and WeChat (a multi-purpose messaging social media and mobile payment app) were used to broadcast and share current and accurate information [10]. This validated and established Question 7 of the survey conducted and analyzed in section III above.

C. The country postponed non-urgent medical care and moved many doctor's visits online.
The Chinese model include prioritization of critical health issues. And the non-critical ones are given less priority and moved online. These include most of the normal physical routine to be able to keep regular services going, prescriptions in an orderly manner. And this gave room for concentration on COVID-19. It helps to also solve the problem of overcrowded medical systems which is affecting most of the countries with COVID-19 [10]. It also helped to reduce the exposure of the medical practitioners to COVID-19. It is also a validation of Question 5 in the analyzed survey in section III above.

D. Online Shopping
In China, practical barriers to staying put in order to prevent spreading or contracting the illness were largely eliminated using the online system like buying fresh food online, groceries and other essentials. This help in suppressing the spread and to also maintain the social distance by staying at home. This is also good for isolation cases and quarantine.
This also helped in reducing panic buying and supplies because e-commerce helps in bringing the essentials to customer’s doorstep steadily [10].

E. Telecommuting

In the past, many people did not want to discuss this but due to COVID-19 pandemic and the need to stay out of office many people in industries who did not want to implement it are now advocating for it and also working from home. Industries such as banking, aerospace engineering industry to the teaching profession in America. Telecommuting extends to spending time with friends and family on video calls as well in order to prevent boredom and sense of isolation [11]. Telecommuting can increase productivity; boost morale and it can be less stressful. These are some of the benefits of telecommuting among others.

One of the effective strategies to suppress the spread of COVID-19 is working from home while people are isolating or in quarantine. Working from home is made possible through the use of ICT resources connected through the Internet and associated technologies like Internet of Things which can use a monitoring module connected to the internet to monitor if the work is being done or not. Video conferencing can also be done for executive meeting and departmental routine meeting. For schedules that can be done from home this was implemented. The flipside of this is that there are some schedules that may not be online like logistics and that may have to be dealt with in a different way. COVID-19 has shown the need to work from home when it is practicable as shown from the China COVID-19 experience. Other part of the world has started using a similar strategy to suppress the spread of COVID-19 [12] [13]. This is a validation of the result got from Question 9 of the survey in section III above.

4.2 South Korea: Use of ICT tools to suppress COVID-19
A. Fast-developed testing kit: Combatting COVID-19 goes beyond the use of traditional medicine. Innovations and other initiatives beyond social distancing, need to be employed to rapidly flatten the curve. To Flatten the curve, South Korea has used Artificial Intelligence to develop test kits within a very short time of 3 weeks and South Korea has a testing capacity of 15,000 per day on average. This has helped to flatten and bring down the curve rate of infection [14]. This validates the results of Question 8 of the survey in section III.

B. Smart quarantine information system: This is a system that allows the monitoring of incoming passengers from epidemic countries and this information is shared with relevant agencies (Ministry of Foreign Affairs, Health Insurance Review & Assessment Service, telecommunication companies and the Korea Centers for Disease Control and Prevention - KCDC) in Korea. The passengers are monitored within the incubation period of the disease the system is an ICT platform which uses roaming data of oversea arrival [15].

C. Mobile phone technology data for contact tracing and Mobile App for Information Sharing: Several mobile apps have been developed in a very short time which can show where to buy mask, another one can direct a patient to the closest testing center [14]. There are other one that give public critical information and so many applications. These help to combat COVID -19 and to slow down the rate of infection which was initially rapid

D. AI for improving diagnosis efficiency and patient classification: The South Korea has developed a Chest X-Ray AI Image Support Decision Tool. This helps to categorize the cases of COVID-19 into Mild, moderate, severe and very severe, this is a risk mitigation strategy which helps intreating each case based on the category. The system is based on an algorithm for identifying abnormal findings on chest x-rays. The systems can examine the lungs within just three seconds [14]. This further validates question 8 results from section III survey.

E. Daegu: Making use of a smart city hub: Daegu was the epicenter of COVID-19 in South Korea but it is now being

transformed into a Smart City and the Smart Hub in the city has been used during the epidemiological investigation to create route tracing application being used to develop new medicine[14].

V. RECOMENDATIONS

From the foregoing, the following recommendations are hereby made:

- ICT Pandemic Management System: Based on the foregoing, it is recommended that, there is need to set up ICT Pandemic Management System (ICT PMS) which will be used during Pandemic situation like the COVID-19 by each country. This will include the strategy to work online and to monitor staff by manager and at the same time to make them feel under office environments but not making the staff feel uncomfortable. Applications that can handle such activities are already developed and being advanced based on lesson learnt from COVID-19. The app would also help workers to overcome boredom since they can see other staff working through their webcams on the screen face slate. This is an all-inclusive solution that can even help managers to help to monitor duration of staff work.

  It is expected that this will include Business Continuity Management ISO22301 that can be used to define management system policy for all climes/countries and this should be expanded to include how countries can combat pandemic such as COVID-19 by including robust policy on Artificial Intelligence to combat future occurrence. This can be a policy document processed through the Act of Parliament with unique definitions for each country as deemed fit. This will accelerate the optimization of ICT resources to combat contagion.

- Emergency number: Setting up of national emergency number should be prioritized for countries that have not set up such facilities for the purpose of communications for victim or infected people to be able to communicate with the right channel like ambulance service, direction to close test center, direction to controlled market to buy Personal Protection Equipment (PPE), how to get drone services and what it can deliver, Disease Control Agency etc. this should be all inclusive robust platforms. This is a point to note for developing countries to implement a robust emergency platform. This validates the result of the survey in section III as established in country experience analyzed in section IV.
- The use of Artificial Intelligence, Augmented Reality and smart systems for monitoring people for the purpose of tracking them in terms of movement should be set up by all countries so that tracking and tracing contacts would be easier. This can be implemented through Smart Hub, IoT, Big Data Analytics applications. Instead of the manual tracing which may not yield the desired results in case of larger samples like the COVID-19 in some countries that have been seriously affected. The country experience model above which can help to locate concentration of highly infected area integrated with "idiot -proof" system can be advanced by further applications of internet of things to integrate more monitoring systems. It is a known fact that for novel diseases and contagion it takes time to study the full epidemiology, to sequence the genome and to produce drugs and vaccine within the period of contagion before medical breakthrough, Artificial Intelligence can also be deployed to suppress and combat the contagion. South Korea and China illustration demonstrated this and validated questions 5, 7, 8 and 10 of the survey analyzed in section III above.
- For effective optimization of ICT resources, it is recommended that framework or policy on telehealth should also be considered as a standalone policy. This will define the minimum resources require to establish a telehealth for a particular country. The definition of what is expected in the telehealth services can also be included. It is expected that the minimum resources required for implementation like broadband standards be included. This should define the hardware requirements as it were.
- Work should commence on the implementations of the above recommendations as a way of preventing or combatting future contagion.

VI. CONCLUSION AND FUTURE RESEARCH WORK

The COVID-19 pandemic rate of infection is high and it is a fact that the traditional health system capacity needs to be boosted using the ICT resources in terms of electronic health system running on the ICT resources. This investigation has successfully proved that. The country experiences of South Kore and China have shown that without optimizing available ICT resources to do more in emergency situation like the COVID-19 pandemic, it will be difficult to slow down the rate of infection. Use of Artificial Intelligence, Robotics, emergency numbers for different applications and increase use of those ICT infrastructures and resources have assisted in mitigating COVID-19 in the illustrated examples. This has validated the results of the research and therefore given empirical evidence to the feasibility of the recommendations.

Future research work shall be: "Regulation and Standardization of Digital Technologies Used in Facilitating the Mitigation of a pandemic disease".

REFERENCES

[1] A. S. Hornby, D. Lea and J. Bradbery, Oxford advanced learner's dictionary of current English, Oxford University Press, 10th edition ed. 2020.

[2] World Health Organization, “EHealth at WHO”, ehealth Unit Geneva, Switzerland. [Source: online]. Available :https://www.who.int/ehealth/about/en/ , [Accessed:12th April, 2020]
[3] D. Mea, Vincenzo, "What is e-Health (2): The death of telemedicine?". Journal of Medical Internet Research. 3 (2): e22. [doi:10.2196/jmir.3.2.e22. PMC 1761900. PMID 11720964., 2001]
[4] O. S. Daudi and M. Mughwira, Application of ICT in strengthening health information systems in developing countries in the wake of globalization, ACTS [African Centre for Technology Studies, pp 194–198., 2004] Source: online] Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2688333/ [Accessed:12th April, 2020].
[5] United Nations Conference on Trade and Development, Digital Economy Report 2019 Value Creation and Capture: Implications for Developing Countries, [United Nations Publications, Geneva., 2019]
[6] G. Bethscheider, (2015). Barney, Randall (ed.). "Satellite is vital for a unified, global, E-Health system. An SES Techcom Services Perspective". World Teleport Association. [Source: online]. Available: https://www.worldteleport.org/news/249029/Satellite-Is-Vital-For-A-Unified-Global-e-Health-System...-An-SES-Techcom-Services-Perspective-.htm [Accessed:12th April, 2020].
[7] O. J. Kunle, O. A. Olubunmi and S. Sani, Internet of things prospect in Nigeria: Challenges and solutions, IEEE 3rd International Conference on Electro-Technology for National Development [NIGERCON, Owerri, pp. 736-745. 2017]
[8] International Telecommunications Union, (2020) Telecoms, Coronavirus and keeping the networks running: Opinion Available: online] Source: https://news.itu.int/telecoms-coronavirus-and-keeping-the-networks-running-time-for-leadership/ [2020] [Accessed: 12th April, 2020].
[9] SurveyMonkey, [Source: online] Available: https://www.surveymonkey.com/r/V3YDQLH under the SurveyMonkey application. [Accessed: April, 2020].
[10] H. Brueck, 11 extreme measures China took to contain the coronavirus show the rest of the world is unprepared for COVID-19. [Source: online] Available: https://www.pulse.com.gh/bi/tech/11-extreme-measures-china-took-to-contain-the-coronavirus-show-the-rest-of-the-world/he13wmg [2020] [Accessed: 7th April, 2020]
[11] B. Morgan, Is COVID-19 Forcing Your Digital Transformation? 12 Steps To Move Faster, Forbes. 2020.[Source: online] Available:https://www.forbes.com/sites/blakemorgan/2020/04/05/is-covid-19-forcing-your-digital-transformation-12-steps-to-move-faster/#56f55df3617b [Accessed: 12th April, 2020].
[12] S. Banjo, L. Yap, C. Murphy and V. Chan, The Coronavirus Outbreak Has Become the World’s Largest Work-From-Home Experiment. Time. 2020. [Source: online] Available: https://time.com/5776660/coronavirus-work-from-home/ [Accessed: 12th April, 2020]
[13] A. Holmes, Employees at home are being photographed every 5 minutes by an always-on video service to ensure they're actually working — and the service is seeing a rapid expansion since the coronavirus outbreak, Business Insider by Pulse. 2020 [Source: online] Available: https://www.pulse.com.gh/bi/tech/employees-at-home-are-being-photographed-every-5-minutes-by-an-always-on-video/9bdc24p [Accessed: 10th April, 2020].
[14] International Telecommunications Union, COVID-19: How Korea is using innovative technology and AI to flatten the curve 2020. [Source: online]. Available: https://news.itu.int/covid-19-how-korea-is-using-innovative-technology-and-ai-to-flatten-the-curve/ [Accessed: 7th April, 2020].
[15] Osong, Health Technology Administration Complex, Smart quarantine information system project, KCDC, Korea. 2019. [Source: online]. Available: http://www.cdc.go.kr/contents.es?mid=a30301180000 [Accessed:15th April, 2020].

A Bruner EIS-Based Learning Management System for Teaching Algebra: A Pilot Study

Jessica Chinezie Benson-Iyare, Ekuma James Nkorabon, Felix A. Sani, Gbenga R. Akeredolu
Department of Computer Science
Federal Polytechnic, Idah
Kogi State, Nigeria
jessben100@gmail.com,
Ekuma_ejn@yahoo.com,
felixsani@yahoo.com,
akmasgbenga2@gmail.com

Joseph Chinalu Osagu
Founding Partner
Scribes Empire and Mathematics Clinic
Ekiti State, Nigeria
scribesempire@mathematicsclinic.com

Judith Chineye Azikiwe
Department of Psychology
Federal University, Oye
Ekiti State, Nigeria
juddydear@yahoo.com

Abstract*— Research works have shown that students have negative attitudes toward learning algebra. These negative attitudes are due to the inability of the teachers to use an appropriate teaching approach that will encourage students' active participation in the learning process. One of the ways to capture their interests to learn algebra is to use the different teaching modes which are reflected in Bruner's EIS theory. This study developed a Learning Management System (LMS) for Nigerian secondary school students. This was done using WordPress. The LMS was used to teach the basics of algebra using the three modes of knowledge representation as stipulated by Bruner. Questions designed based on the Technology Acceptance Model (TAM) relating to perceived usefulness (PU) and perceived ease of use (PEOU) were asked to obtain students' opinions on the LMS. From the results, 71% of the students found the LMS useful for learning; 86% affirmed that they could easily interact with the LMS and 85% submitted that they will easily become skillful at using the LMS. The results of the data analysis are an indicator of their satisfaction with the Bruner EIS-Based LMS. The study provides support for teaching and learning functions by spurring the interests of students in the learning of algebra.

Keywords—Learning Management System (LMS), Bruner's EIS theory, Enactive, Iconic, Symbolic, Technology Acceptance Model (TAM), Algebra, WordPress, Nigerian Secondary School Students.

I. INTRODUCTION

Algebra is an integral part of mathematics and holds a pivotal role in numerous fields of study. As important as algebra is to building students' algebraic problem-solving skills, most students have negative attitudes towards learning it. Reference [1] in their study discovered that Nigerian secondary school students do not have positive attitudes towards learning algebra. They posited that the students' negative attitudes towards solving algebraic problems are due to heavy reliance on teachers on every concept they learn and difficulty in connecting past experiences with present situations. They further suggested that the teachers' inability to use the appropriate teaching approach that will encourage students' active participation in solving problems themselves also contributes to the negative attitudes. The studies of [2]-[4] submit that most students find algebra very difficult to understand due to the following reasons (i) the students' perception that algebra is very difficult, uninteresting, and is founded on symbolic manipulations that are meaningless and irrelevant to day to day living and (ii) the students' misconception of the use of algebraic symbols.

Several schools have attempted integrating technology into their teaching system. One such attempt is the use of the learning management system (LMS). References [5], [6] defined a Learning Management System as an online learning technology for creating, managing, and delivering course materials. In present-day learning, this web-based information system typically plays a major role in providing an instructor/teacher with tools for the administration, documentation, tracking, reporting, delivery of e-learning education courses or training programs, and performance assessment. The other key features are video conferencing to provide synchronous learning; threaded discussion and discussion forums to aid asynchronous learning.

In this study, the authors are interested in finding a solution to students' negative attitudes towards learning algebra through a virtual learning environment. This interest triggered the development of an LMS for learning the basics of algebra (expressions, equations, variables, coefficients, and literals). An LMS describes the incorporation of computer systems and web technologies into instruction provision, management of resources, and tracks the achievement of both students and institutions. It helps the instructors to deliver material to the students, administer the test and other assignments, track student progress, and manage record-keeping regardless of time or place provided Internet access and appropriate technologies are available [7]-[9]. The utilization of LMS for students can support learning and save resources such as time and money [10]-[14].

This research was funded by Institution-Based Research-Tertiary Education Trust Fund, Nigeria under the grant number TETFUND/DESS/POLY/IDAH/RP/VOL.1.

Furthermore, LMS is normally used to supplement and complement the traditional teaching method i.e. the face-to-face conventional way of imparting knowledge to students. LMS has been used widely in citadels of learning and much of the research about it has been focused on technology or studies adoption [15], but very few on learning theories to back the curriculum design for the courses being offered. To overcome students' negative attitudes towards learning algebra, this study developed a Bruner EIS-based LMS for Nigerian secondary school students to help to spur their interests in learning algebra. To this end, the study tried to find out whether, with the use of Bruner EIS-based LMS, students would become more interested in algebra.

II. LITERATURE REVIEW

A. Overcoming the Difficulties in Learning Algebra

Several authors have looked at ways to overcome the difficulties students face in learning algebra. The study of [16] investigated the challenges faced by some Zambian secondary school students in learning algebraic linear equations. The study concluded that the students' failure to correctly solve linear equations is attributed to their inadequate pre-requisite knowledge. The authors suggested that students should first be equipped with the necessary background knowledge upon which new knowledge can be built. Reference [17] determined the difficulties of the algebraic thinking ability of a group of secondary school students and proffered the Math-Talk Learning Community concept as a way to improve the students' algebraic thinking ability. In the study of [4], a diagnostic teaching approach was employed as a possible solution to students' difficulties and misconceptions on several aspects of algebra.

B. Studies on Learning Management Systems

The traditional form of classroom teaching has recently been enhanced for effective learning using LMS [18]. A study on factors influencing LMS usage by teachers and students conducted by [19] identified six factors (students, teachers, technology, resources, pedagogy, and curriculum) that influence the use of LMS in education. The authors combined the six factors to develop a model which was called Holistic Information Communication Technology Adoption Model (HICTAM) to be incorporated into the curriculum to increase the efficiency and effectiveness of the teaching-learning processes. The study of [20] posited that required tools be built into LMS to enhance ease of educational task performance. The study of [21] investigated learning via mobile applications by comparing students' LMS usage before and after its introduction. The major achievement **of this study** is the provision of examples for developers of mobile learning platforms for tertiary institutions.

Some studies have looked into the effect of blended learning in higher institutions using LMS. The research conducted by [22] was carried out among students of the Technological Educational Institution in Ionian Island, Greece. The researchers utilized the Open eClass platform to improve lecture materials. They found out that despite worries on students' truancy and non-participation in physical classes when exposed to online educational materials including videos, students did not reduce their presence in classes; rather it served an additional means in assisting them to learn more.

Reference [23] study shows that students' ideas and attitudes toward learning and education contribute to their perception of the usefulness of LMS. In Nigeria, there is a paucity of studies on the adoption of LMS in educational institutions. One of the very recent studies on LMS was conducted by [24]. The work investigated LMS adoption sampling students from four universities in Nigeria. Results from the study revealed that the study variables determine the student's intention to use LMS which in turn determines LMS actual usage.

This present study fosters incorporating Bruner's EIS constructivism learning theory into an LMS as a way to enforce meaningful learning in the teaching of algebra and also provides a solution to students' negative attitudes towards the learning of algebra.

III. THEORETICAL FRAMEWORK

A. Learning Theories

Learning design should be based on learning theories because they help the teacher make more informed decisions around the design, development, and delivery of learning. Learning theories are combinations of principles, rules, and techniques that have been formed through speculation, research, and hypothetical testing on how knowledge acquisition occurs. This study embraces the constructivism learning theory emphasized in Bruner Jerome's EIS theory which presents three modes of representations [25]. Constructivism is a learning theory that concerns the process of how humans come to know new knowledge based on their previous knowledge and experiences from the things around them [26]. The role of teachers/instructors in this process is to facilitate the construction of knowledge and ensure students make sense of the knowledge acquired.

B. Bruner Jerome's EIS Theory

Jerome Seymour Bruner was a cognitive psychologist who believed that education is about discovery and making the learner independent. He created a theory of development based upon the idea that the goal of education should be intellectual development. His focus was on children as he studied the way they learn and came to the agreement that children are born as ready active learners [27].

Bruner suggested that students may experience, or represent tasks in three modes: *Enactive* representation (action-based) which refers to learning through actions, *Iconic* representation (image-based) which refers to the learner's use of pictures or models, and *Symbolic* representation (language-based) which refers to the development of the ability to think in abstract terms. Each mode is a way in which information or knowledge is stored and encoded in the memory. The modes of representation are not delineated into stages but are integrated and loosely sequential [28]. Bruner's EIS theory suggests that it is efficacious to follow a progression from enactive to iconic to symbolic representation when faced with new materials. He believed that the learning theory

can be applied to any student of any age and can be used to teach any subject provided the learning instructions are organized appropriately [28]. His work further suggests that tests or punishments do not spur the learner to learn. One learns best when one finds the acquired knowledge appealing so, organizing appropriately the learning materials will spur the learner's interest.

IV. A 3-Tier Architecture of the Learning Management System

This study developed a learning management system in which a three-layered conceptual framework was used.

A. Presentation Layer

In this tier the user interface had been built to display data to the student or accept input from the user. It contains controls like textboxes, dropdown lists, grid views, labels, etc. The graphical user interface is used for the presentation layer to enable users to operate the LMS by moving a mouse pointer or other pointing devices onto Windows, icons, or buttons. Users can learn online by logging on to the website. The LMS can support using desktop computers and mobile devices such as smartphones.

B. Business Layer

This tier serves as an intermediary for data exchange between the presentation layer and the data access layer. This layer includes the following modules:

1) Teaching management agent: This agent is responsible for the presentation of learning materials.

2) Quiz/test/examination agent: This agent is responsible for the quizzes/tests/examinations that are taken after completing the course.

3) Question & answer agent: This agent is responsible for the discussions that the students initiate to ask the teacher some questions about what he/she has learned and also to receive answers from the instructor/teacher.

4) Discussion forum agent: This agent is responsible for the discussion boards opened by each student.

C. Data Layer

This tier stores information. The layer contains the following databases:

1) Content database: This database stores basic teaching materials which include images, texts, and videos.

2) User database: This database stores users' logging information such as their personal information, to verify whether they have the right to view the course content and learn. It also maintains records related to students' quiz processes, and discussion boards opened by each user.

V. The Learning Management System Design

Fig. 1 is the Use Case diagram for the learning management system. The Use Case diagram represents the users' interactions with the system. It shows the relationship between the users, also known as the actors, and the different use cases, usually represented by either circles or ellipses, in which the users are involved.

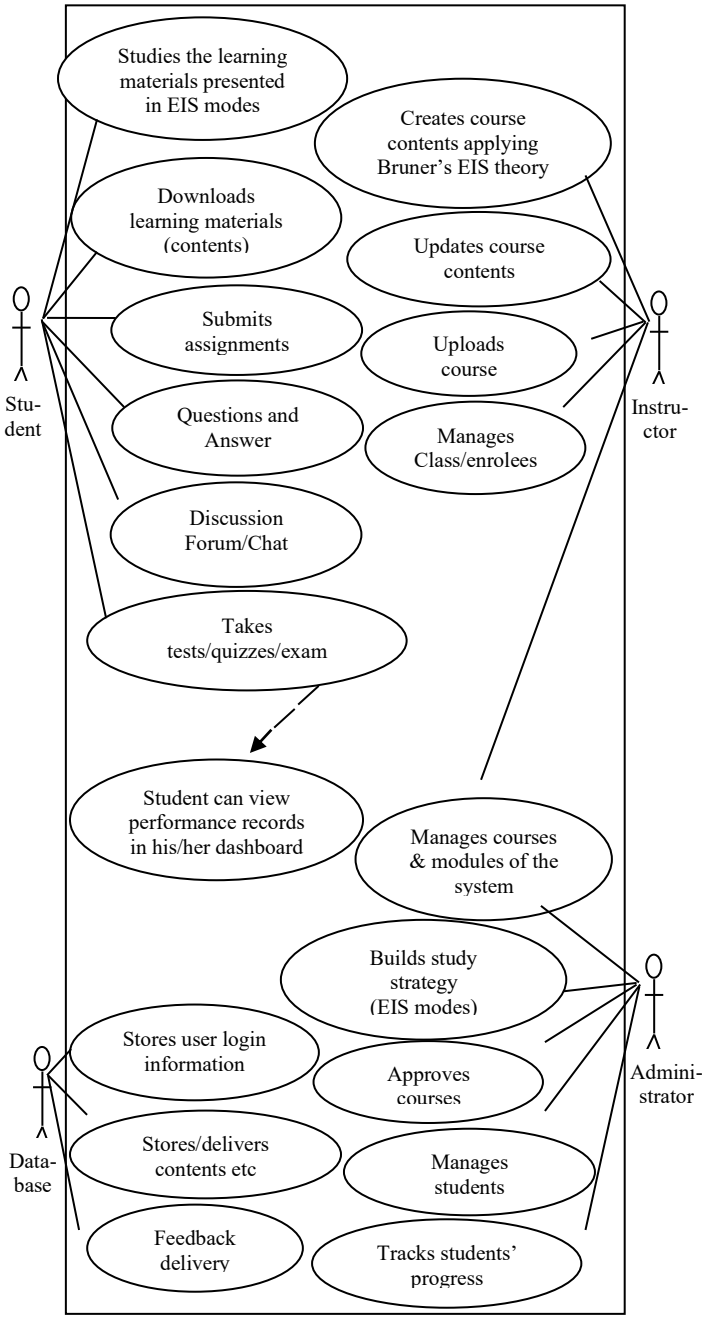


Fig. 1. Design of the Bruner EIS-Based Learning Management System using Use Case Diagram

Instructor, student, administrator and database are identified as the main actors in the Use Case diagram in Fig. 1. The instructor generates events, courses or lessons. The student accesses and interacts with a specific event and participates in the lessons. The administrator manages the whole environment. The architecture supports both contact learning and distance learning modes. The student can create an account or login in to his/her account, enroll in a course, take lessons at his/her own pace till completion, take quiz or examination, and view his/her performance on his/her dashboard. The student can further engage the instructor (who may also be an administrator) in a question and answer section to clarify doubts on the course taught. The discussion forum is an avenue for the student to engage other students on the platform by exchanging ideas on the course learned. The performance record is stored and maybe used for counseling them on the course studied.

VI. SYSTEM DEVELOPMENT

The LMS was developed using WordPress - a content management system (CMS). A CMS is software specifically built for web content that provides website authoring, collaboration, and administration tools that help users create and manage website contents. WordPress is open source publishing software that can be installed locally on a web server and viewed on a proprietary website or hosted in the cloud and viewed on the WordPress website. It was coded with PHP (Hypertext Preprocessor) and uses MySQL (**My Structured Query Language**) database engine. It is used with a combination of themes, plugins and page builders to create and launch LMSs which were programmed with HTML (Hyper Text Markup Language), CSS (Cascading Style Sheets), PHP, JavaScript, and Ajax languages. Themes define the interface for the LMS. The plugin extends the functionalities of WordPress by combining a wide range of features to present a class setting without having the students come into a physical classroom. It allows one to create classes, share coursework, enroll students, and evaluate the students with quizzes and dashboard in the shortest possible time. Using WordPress to develop the LMS was a good choice due to the reduced development time it avails its users.

Some of the basic requirements of the LMS are explained below:

- ***Course builder*** with tools for uploading different file types like videos, Portable Document Format (pdfs), links and other contents.
- ***Course progress information*** is used to show to the students how well they are performing.
- ***Student enrolment and management*** enables the instructor or administrator to see how many people are undertaking the courses.
- ***Quizzes and tests*** for students to evaluate how much they have absorbed the material. Quizzes can be used as a way to determine who is qualified for a class.
- ***Chats and forums integrations*** for users to generate student profiles and interact with other students and teachers.
- ***Homework options*** allow the students to submit homework for grading.

VII. COURSE DESIGN-THE APPLICATION OF BRUNER'S EIS THEORY IN THE LMS

Bruner had influenced education greatly; his EIS theory has been most noticeable in mathematical education. The theory is useful in teaching mathematics which is primarily conceptual, as it begins with a concrete representation and progresses to a more abstract one. Bruner's learning theory has direct implications on the teaching practices.

The course lessons were organized according to enactive, iconic, and symbolic modes specified in Bruner's theory and are presented in this section.

A. Enactive Representation of Knowledge

This is the first mode of knowledge representation and involves hands-on method of learning. Bruner believed that learning should begin with an action for instance, touching, feeling and manipulating. In mathematics education, manipulative are the concrete objects or anything tangible with which the actions are performed. In classroom learning, examples of manipulative used in this mode are algebra tiles, paper, coins, and scales. This mode has been represented in the LMS through *written information* and directly involving the students by asking them to *perform some actions* based on the knowledge acquired on what they have been shown. The use of scale in the enactive stage is a great way to "hook" students, who may not be particularly interested in the topic taught. (See Fig. 2).

Fig. 2. Screenshot of the LMS showing lessons represented in Enactive mode (Source of learning material: Adapted from https://www.wyzant.com/ resources/lessons/math/algebra/equation-basics)

B. Iconic Representation of Knowledge

This is the second mode of knowledge representation and involves using images or other visuals to represent the concrete situation enacted in the first stage. Bruner believed that learning should scaffold from action-based to image-based. In classroom learning, images are drawn on boards or on papers. This allows the students to picture the concrete situations in their heads in the form of visual illustrations. This mode has been represented in the LMS with *videos* demonstrating the knowledge through diagrams, charts, graphs, and colors. (See Fig. 3).

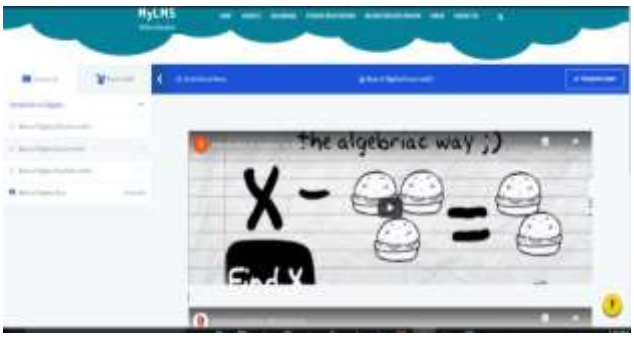


Fig. 3. Screenshot of the LMS showing lessons represented in Iconic mode (Source of video: Adopted from https://www.youtube.com/watch?v=z0OIXIZKfo0)

C. Symbolic Representation of Knowledge

This is the third mode of knowledge representation and involves using words and symbols to represent the images from the second stage. Bruner believed that learning should scaffold from image-based to language-based. With the use of words and symbols, the student can organize information in his/her mind by relating concepts together. The symbolic representation is likely to be useful for learning something new in a familiar topic. Furthermore, by having all students go through each of the modes, it builds a foundation for which the students can fall back on if they forget or as they encounter increasingly difficult problems. This mode has been represented in the LMS through *videos* putting the whole knowledge together as would be done in the conventional teaching. (See Fig. 4).

Fig. 4. Screenshot of the LMS showing lessons represented in Symbolic mode (Source of video: Adopted from https://www.youtube.com/watch?v=NybHckSEQBI)

VIII. Data Collection Method

The participants for this study were chosen based on a convenience sampling technique. This technique was chosen for two reasons: 1) The Higher National Diploma (HND) final year students of the Federal Polytechnic, Idah were readily available for us to use as they were concluding their project works. 2) The said students had already passed through the secondary school level. It is our belief that they can easily access if the LMS will be good for secondary school students and if they will use it. The study adopted a quantitative approach to examine students' level of acceptance of the LMS based on the two main factors – perceived usefulness and perceived ease of use. Questionnaires were administered to the 7 Computer Science students of The Federal Polytechnic, Idah, Nigeria, who volunteered to use the LMS to learn "The Basics of Algebra". All the 7 respondents completed and returned the questionnaire. Questions designed based on Technology Acceptance Model (TAM) which relates to perceived usefulness and perceived ease of use were asked in the questionnaire. All the questions were rated on a five-point Likert scale ranging from "strongly agree" to "strongly disagree". Cronbach's alpha on the full scale is 0.75 which demonstrates a reliable internal consistency of the questionnaire.

IX. Data Analysis and Results

The data from the questionnaire were analyzed as presented in Table I. The results showing the level of satisfaction is given in Table II.

X. Discussion

A. Perceived Usefulness

Perceived usefulness is the degree to which a person believes that using a particular system would enhance his or her job performance [22]. All the students in the study found the LMS helpful in understanding algebraic basics more quickly and also agreed that the LMS increased their learning abilities. 71% of the students found the system useful for learning. (See Table II).

B. Perceived Ease of Use

Perceived ease of use is the degree to which a person believes that using a particular system would be free from effort [22]. All the students in the study submitted that they will use the LMS again to learn other topics in algebra and would recommend the system to other students. 86% affirmed that they could easily interact and understand the LMS and further found the system flexible to interact with. Furthermore, 85% of the students submitted that it will be easy for them to become skilful at using the system. (See Table II).

The sample size was small but it was enough to gain some insights into the students' perception and usage of the LMS. The success and adoption of a LMS in any institution starts by its acceptance. Findings from this study suggest that with the adoption of Bruner EIS-based LMS, students would become more interested in learning algebra.

TABLE I. TECHNOLOGY ACCEPTANCE MODEL QUESTIONS SHOWING THE FIVE-POINT LIKERT SCALE RANGING FROM "STRONGLY AGREE" TO "STRONGLY DISAGREE", THE FREQUENCY OF THEIR RESPONSES AND THEIR PERCENTAGES

Students' Responses to Questions	TAM Questions and their Responses					
	Questions	*Strongly Agree f(%)*[a]	*Agree f(%)*[a]	*Neutral f(%)*[a]	*Disagree f(%)*[a]	*Strongly Disagree f(%)*[a]
	Scale for Perceived Usefulness (PU)					
PU 1	Using the LMS enables me to understand algebraic basics more quickly.	4 (57)	3 (43)	0	0	0
PU 2	Using the LMS increases my learning ability.	4 (57)	3 (43)	0	0	0
PU 3	I find the LMS useful for learning.	4 (57)	1 (14)	2 (29)	0	0
	Scale of Perceived Ease Of Use (PEOU)					
PEOU 1	Interaction with the LMS is easy and understandable.	4 (57)	2 (29)	0	1 (14)	0
PEOU 2	I find the LMS flexible to interact with.	4 (57)	2 (29)	1 (14)	0	0
PEOU 3	It would be easy for me to become skillful at using the LMS.	5 (71)	1 (14)	1 (14)	0	0
PEOU 4	I would use this LMS again to learn other topics in algebra.	4 (57)	3 (43)	0	0	0
PEOU 5	I would recommend the LMS to other students.	4 (57)	3 (43)	0	0	0

[a.] Percentages were rounded up to the nearest whole numbers.

TABLE II. RESULTS SHOWING THE LEVEL OF SATISFACTION

Level of Satisfaction	TAM questions and Satisfaction Level in Percentage	
	Questions	*Level of satisfaction f(%)*[a]
	Scale for Perceived Usefulness (PU)	
PU1	Using the LMS enables me to understand algebraic basics more quickly.	7 (100)
PU2	Using the LMS increases my learning ability.	7 (100)
PU3	I find the LMS useful for learning.	5(71)
	Scale of Perceived Ease Of Use (PEOU)	
PEOU 1	Interaction with the LMS is easy and understandable.	6 (86)
PEOU 2	I find the LMS flexible to interact with.	6 (86)
PEOU 3	It would be easy for me to become skillful at using the LMS.	6 (85)
PEOU 4	I would use this LMS again to learn other topics in algebra.	7(100)
PEOU 5	I would recommend the LMS to other students.	7 (100)

[a.] Percentages were rounded up to the nearest whole numbers.

XI. CONCLUSION AND SUGGESTIONS FOR FURTHER STUDIES

This study presents a solution to overcome students' negative attitudes toward learning algebra. To achieve this, it developed an LMS for learning the basics of algebra by representing the learning materials in three ways: enactive representation (E), iconic representation (I), and symbolic representation (S) as suggested by Bruner. The use of scale in the enactive mode is a great way to "hook" students to be interested in the topic taught. The iconic mode allows the students to picture the concrete situations in their heads in the form of visual illustrations. The use of words and symbols in the symbolic mode allows a student to organize information in the mind by relating concepts together. This study submits that by having all students go through each of the modes, it builds a foundation for which the students can fall back on if they forget or as they encounter increasingly difficult problems.

The whole essence of utilizing Bruner's EIS theory in the teaching of algebra is to allow teachers/instructors to be able to involve all the students in the learning process. This approach of learning provides the necessary background knowledge upon which new knowledge can be built. More so, the chat and forum features were integrated into the LMS as a way to improve the students' understanding of the concept being taught through community learning.

Although the sample size used for this study is too small to generalize the findings, the students' responses show some degrees of their acceptance of the LMS and also suggest their willingness to use the LMS to their advantage. Notwithstanding, further studies would cover larger sample

sizes and stringent measures that will ensure that the students learn with the system would be put in place. Future studies would also empirically validate this present study by evaluating the LMS to test for significance on students' learning ability.

Conclusively, the study found out that the use of Bruner EIS-based LMS would make Nigerian secondary students more interested in learning algebra. This study would be a major endeavor in promoting effective teaching and learning processes by motivating students to learn algebra. Specifically, this study would serve as a future reference for curriculum creators. The contributions of this study are not exclusive to only secondary school students but would be valuable to all students at all levels of education.

XII. Recommendations

It was evident from the findings that students' acceptance of the LMS is a precursor to its adoption. Hence, it is recommended as follows that:

1) Nigerian government should approve and adopt this method for teaching mathematics, not just algebra in our schools.

2) Mathematics curriculum creators and instructors/teachers should be well equipped in the application of the Bruner's EIS theory to the mathematics curriculum.

3) Nigerian government should expedite actions to provide the necessary infrastructural facilities to enable the use of LMS such as computer systems, broadband networks, and improved electricity supply.

4) Instructors/teachers should promote the use of LMS by complementing it with conventional teaching and learning processes.

Acknowledgment

The authors thank the owner of https://www.wyzant.com and the YouTubers from whose site and channels the texts and videos that constituted the learning materials used for the study were extracted.

References

[17] E. Julius, A. H. Abdullah, and N. Suhairom, "Attitude of students towards solving problems in algebra: A review of Nigeria secondary schools," IOSR Journal of Research & Method in Education (IOSR-JRME), vol. 8, pp. 26-31, January-February 2018.

[18] L. Sugiarti and H. Retnawati, "Analysis of student difficulties on algebra problem solving in junior high school," in Journal of Physics: Conference Series Yogyakarta, Indonesia, 2019.

[19] J. L. Booth, K. M. McGinn, C. A., Barbieri and L. K. Young, "Misconceptions and Learning Algebra," in And the Rest is Just Algebra, Springer. October 2017, pp. 63-78.

[20] T. C. F. Chow, "Students' difficulties, conceptions and attitudes towards learning algebra: an intervention study to improve teaching and learning," Ph.D. Thesis, Dept. of Mathematics, Curtin University, Malaysia, October 2011.

[21] D. Turnbull, C. Ritesh, and L. Jo, "Learning management systems: An overview," In *Encyclopedia of Education and Information Technologies*, edited by A. Tatnall. Cham: Springer Nature. 2019.

[22] R. Sabharwal, M. R. Hossain, R. Chugh, and M. Wells, "Learning management systems in the workplace: A literature review," Paper presented at the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 387–393. Wollongong, December 4–7, 2018.

[23] R. Kraleva, M. Sabani, and V. Kralev, "An analysis of some learning management systems," International Journal on Advanced Science Engineering Information Technology, vol. 9, pp. 1190-1198, 2019.

[24] I. A. Almrashdeh, N. Sahari, N. A. M. Zin, and M. Alsmadi, "Distance learning management system requirements from student's perspective," Journal of Theoretical and Applied Information Technology, vol. 24, pp.17-27, 2011.

[25] A. S. Alzouman, N. A. Alhazzani, and H. A. Alwaili, "The effectiveness of learning management systems (LMS) in developing the education and upbringing process," Information and Knowledge Management. vol. 7, pp. 21-27, 2017.

[26] W. N. T. Wan Hussin, J. Harun, and N. A. Shukor, "Problem based learning to enhance students' critical thinking skill via online tools," Asian Social Science, vol. 15, pp.14-23, 2018.

[27] K. Changwong, A. Sukkamart, and B. Sisan, "Critical thinking skill development: Analysis of a new learning management model for Thai high schools," Journal of International Studies, vol. 11, pp. 37-48, 2018.

[28] N. J. Kim, "Enhancing students' higher order thinking skills through computer-based scaffolding in problem-based learning," All Graduate Theses and Dissertations. 5488, 2017.

[29] R. G. Saade, D. Morin, and J. D. E. Thomas, "Critical thinking in e-learning environments," Computers in Human Behaviour, vol. 28, pp. 1608-1617, 2012.

[30] J. P. Hernandez-Ramos, F. Martinez-Abad, F. Garcia-Penalvo, M. E. Herrera-Garcia, and M. Rodriguez-Conde, "Teachers' attitude regarding the use of ICT. A factor reliability and validity study," Computers in Human Behaviour, vol. 31, pp. 509-516, 2014.

[31] T. J. McGill and J. E. Klobas, "A task-technology fit view of learning management system impact," Computers & Education, vol. 52, pp. 496-508, 2009.

[32] K. Samuel, H. M. Mulenga, and M. Angel, "An investigation into challenges faced by secondary school teachers and pupils in algebraic linear equations: A case of mufulira district, zambia," Journal of Education and Practice, vol.7, pp. 99-106, 2016.

[33] D. M. Nurhayati, T. Herman, and S. Suhendra, "Analysis of secondary school students' algebraic thinking and math-talk learning community to help students learn," International Conference on Mathematics and Science Education (ICMScE) IOP Conf. Series: Journal of Physics: Conf. Series 895, pp. 1-7, 2017.

[34] L. E. Chaw and C. M.Tang, "What makes learning management system effective for learning," Journal of Education Information System, vol. 47, pp. 152-169, December 2018.

[35] H. Fung and A. Yuen, "Factors affecting students' and teachers' use of lms – towards a holistic framework," in Hybrid Learning, S.K.S. Cheung, J. Fong, L. F. Kwok, K. Li, and R. Kwan, Eds. International Conference on Hybrid Learning. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, vol. 7411, 2012.

[36] R. Medina-Flores and R. Morales-Gamboa, "Usability Evaluation by Experts of a Learning Management System," in *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje,* vol. 10, pp. 197-203, November 2015.

[37] P. Hung, J. Lam, C. Wong and T. Chan, "A Study on Using Learning Management System with Mobile App," *International Symposium on Educational Technology (ISET),* Wuhan, 2015, pp. 168-172.

[38] Y. Hirata, Y. Hirata, "Learning Management System: Japanese Student Perceptions and Expectations," in Li K.C., Wang F.L., Yuen K.S., Cheung S.K.S., Kwan R. (eds) Engaging Learners Through Emerging Technologies. Communications in Computer and Information Science, Springer, Berlin, Heidelberg, vol. 302, 2012.

[39] K. Kabassi, I. Dragonas, Ntouzevits, A. et al., Evaluating a learning management system for blended learning in Greek higher education. SpringerPlus, vol. 5, pp. 1-12, February 2016.

[40] M. N. Yakubu, S. I. Dasuki, A. M. Abubakar, and M. M. O. Kah, "Determinants of learning management systems adoption in Nigeria: A hybrid SEM and artificial neural network approach," Education and Information Technology, February 2020.

[41] K. M. Tegegne, "The Influence of E-Learning on the Academic Performance of Mathematics Students in Fundamental Concepts of Algebra Course: The Case in Jimma University," Ethiop. J. Educ. & Sc., vol.9, 2014.

[42] S. O. Bada, 'Constructivism learning theory: a paradigm for teaching and learning," IOSR Journal of Research & Method in Education (IOSR-JRME), vol. 5, pp. 66-70, November-December 2015.

[43] M. A. Sani, "The Contributions of Jerome Bruner's Constructivist Approach to Education," Indian Journal of Research, vol. 6, pp. 1, 2017.

[44] J. S. Bruner, The Process of Education. (Revised Ed.) Harvard University Press, 1960.

[45] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," Management Information Systems Quarterly, vol. 13, pp. 319-340, 1989.

Basics of Algebra, No date. Accessed on: Nov. 2, 2019. [Online]. Available: https://www.wyzant.com/ resources/lessons/math/algebra/equation-basics.

Introduction to Algebra for kids, May 31, 2016. Accessed on: Nov. 2, 2019. [Video file]. Available: https://www.youtube.com/watch?v=z0OIXIZKfo0.

Algebra Basics: What is Algebra?, May 22, 2015. Accessed on: Nov. 2, 2019. [Video file]. Available: https://www.youtube.com/watch?v=NybHckSEQBI.

Leveraging Edge Analysis for Internet of Things Based Accident Information system

Longinus Sunday Ezema, Akande Akinyinka Olukunle,
Nnaemeka Chiemezie Onuekwusi, Ehinomen Atimati
Department of Electrical and Electronic Engineering
Federal University of Technology, Oweeri (FUTO)
Imo State, Nigeria
longinus.ezema@futo.edu.ng, akandeoluk@gmail.com,
nnaemekaonuekwusi@yahoo.com, mailehinomen@gmail.com

Joy Nnenna Eneh
Department of Electronic Engineering
University of Nigeria Nsukka (UNN)
Enugu State, Nigeria
enehjoy@yahoo.com

Abstract – The rate of road accidents and the number of casualties recorded in recent years in Nigeria are alarming. Many of these accidents happen in isolated areas and ditches making it difficult to rescue the victims in a quick and effective manner, to save lives. In this paper, a design and simulation of an IoT based accident information system is developed to detect the vehicle accidents and send the location information of the accident area via Short Message Service (SMS) to the ambulance service/Emergency Management Service (EMS) for quick and effective response to the accident victim. The system was developed mainly with a vibration sensor which detects the accident and a Global Positioning System (GSM) module for the determination of the coordinates of the vehicle in real-time and the communication between the web server and hardware device is established via GSM module. The system when simulated provided the accurate detection of accidents as well as their locations and was also able to communicate wirelessly the location coordinate to the EMS.

Keywords- Arduino Uno, GSM Module, GPS Module, IoT, Information System, Vehicle Accident

I. INTRODUCTION

It is documented that the cities are increasingly so crowded in terms of inhabitants, visitors and vehicles. This has led to boost in traffic, which has resulted to increase in road accidents. The 2018 World Health Organization (WHO) Global Status Report (GSR) on road safety stated that 1.35 million deaths are recorded yearly while 50 million people get injured from road accidents [1]. Same report ranked road accident as the eighth primary cause of death (up from 9th in its preceding information of 2015). Furthermore, the Association for Safe International Road Travel (ASIRT) already predicted that it is likely going to increase to the fifth major cause of casualties in the near future, unless there are drastic changes. ASIRT estimated that countries expended about 2% on their yearly budget on road accidents [2].

Recently, there has been a global appreciation in the annual number of road accident deaths, even in developed countries that have good roads and safety measures [2]. However, it is still the case that the greatest burden of fatalities and injuries owing to road accidents lies in low- and middle-income countries and this account for about 90% [3][4]. For example, in Pakistan, 15 people (on average) lose their lives daily road accidents. The Pakistan Bureau of Statistics already propagated that 9582 accidents have caused 4036 deaths, demonstrating that in every two road accidents, there are more than one death on average [1]. In Nigeria, the trend analysis of fatal road accident shows that between Jan. 2006 and May 2014 about 15,090 people lost their lives in 3,075 road accident incidents. The highest record within this period was obtained in 2013 when 2061 deaths were recorded with 2.8% increase from 2012 records [5]. The trend seems to be increasing with a total of 5181 deaths recorded in 2018 according to the Federal Road Safety Commission [6]. Currently in Nigeria, road accident ranks as the third most cause of death [4]. A decade (2011 – 2020) goal of United Nation (UN) is to even out and lessen the ever growing trend in road accident fatalities thereby saving an estimated 5 million lives in that period [7]. Such fatality rate begs for an urgent improvement in road safety especially in the less developed countries.

The IoT as an emerging technology and with the 5G technologies promises the advancement of intelligent traffic management systems. IoT is a network of physical devices such as vehicles and other items which are embedded with electronics, software, sensors, actuators and network connectivity which help in the connectivity of data [8]. It refers to a rapidly growing network of connected objects which can collect and exchange data by using embedded sensors. It is used in monitoring events and changes in structural conditions such as risk and scheduling, repair and maintenance activities in an efficient manner.

The IoT is an important piece of present world. So many people have burning desire to stay connected on the internet. This communications comes in the form of interactions of human and machine [9]. It has already become an essential part of smart transport applications, smart cities, smart homes and smart industrial applications[10–12], and has so much impacted on the academia, industry, government, and society [13]. It is only via IoT that the physical world can be connected to the web as shown in Fig 1. The IoT is more than just internet connected consumer gadgets. Very soon IT organizations will have to create a framework to support IoT [14].

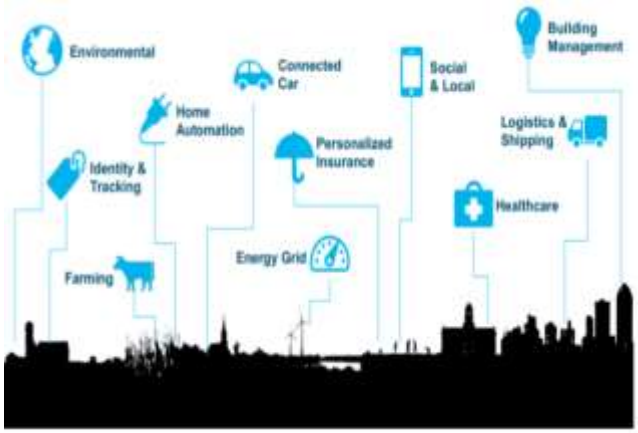


Fig 1: IoT Edge Connection [14]

Vehicle accidents in developing countries are enormous due to numerous unmotorable roads and unchecked recklessness of drivers. Many of which result in fatalities and more worrisome is the fact that some of the deaths could have been savaged if appropriate response team were contacted. Some of these vehicles tumble into ditches/vallies leaving no trace for road users to notice the incident and assist the victims or report to safety team.

The road accident detection, location and reporting system developed in this paper leverages IoT to ensure that accident victims especially unconscious ones automatically get the help they need by reporting the accident and location to safety response team.

II. REVIEW OF LITERATURE

In [15], an accident detection system was built using a tilt sensor for sensing when the car turns, a heartbeat sensor to sense the abnormality in the driver's heartbeat and an android application was built to interface with the system using a bluetooth module (HC-06). The system works in such a way that when the accident occurs, the bluetooth module will send a message to the android application and the application gets the current location of the car using the phone's GPS location and then forwards the message to a nearby hospital. However, the limitations of the work are: the location in the android phone might not be on and not every driver has an android phone thereby defeating the purpose. The system has no alarm to alert the road users and does not give occupants the opportunity to stop alerting the safety response team for rescue should it be minor accident. The tilt sensor cannot detect head-on collision and the bluetooth connectivity can easily be interrupted.

In [16], [17] and [18], the authors made use of a vibration sensor, a GPS module, a GSM module and a buzzer. When an accident occurs, the vibration sensor senses it and alerts the system. The buzzer activates and begins to sound while the GSM module takes the current coordinate of the car and sends a message to emergency services. Nevertheless the buzzer system can only be stopped if the vehicle battery is removed which might be unsafe at that moment. A stop button should have been included in the system to enable the driver to stop the system from contacting the emergency service team if unnecessary.

The idea used in [19] is a very good one and will save a lot of cost. Instead of using a GSM module and a GPS module, an android application was created which accesses the GPS of the phone and the GSM of the phone cutting out both hardware components. The limitation in this work is: a stop button should have been included in the system to enable the driver to stop the system from contacting the emergency service team if unnecessary. The system mandates the driver to be an android phone user for the system to work. The mode of connection between the android phone and vibration sensors was not mentioned.

This work ensured that the above limitations are well covered by the design of an IoT based vehicle accident information system using GSM and GPS technology. It includes an alarm system that allows the vehicle occupants to stop the alarm within one minute set time period if the Emergence Service Response (ESR) is not needed else the system will send the accident notification and location to ESR. The system uses vibration sensors installed at various sides of the vehicle to detect an impact on the vehicle.

III. MATERIALS AND METHODOLOGY

A. Materials

The following hardware and software components were employed in the realization of the system: Arduino Uno, TinyGPS Library for Arduino, Arduino Library for Proteus, GPS Module Library for Proteus, GSM Module Library for Proteus, Vibration Sensor Library for Proteus, LCD Library for Proteus, 801S Vibration Sensor, SIM800L GSM Module, NEO-6 Ublox GPS Module, 2 x stop buttons, buzzer, resistor and Liquid Crystal Display (LCD).

B. Methods

The leveraging edge analysis of internet of things based accident information system is designed as an embedded system. Embedded systems are hardware and hardware systems developed into appliances that are not necessarily recognized as computerized devices, but embedded systems do control the functionalities of these devices [20]. The system block diagram and the system circuit diagram are shown in Fig 2 and Fig 3 respectively. The block diagram gives a general operational flow of the system. The Arduino is the central brain box of the system which coordinates the operations of most components.

The vibration sensor 801S works with logic levels (0 or 1) with an operating voltage range of 3v to 9v and is connected to the input pin of the Arduino with a reset button in between. The 801S sensor was chosen because of its adjustable sensitivity features and ruggedly made for this type of project. Sensor configuration: Logic 1 (high) ranges from Vcc of 7v to 9v while logic 0 (low) ranges from Vcc of 3v to 6v.The sensor is configured to detect an accident by sending logic 1 to the Arduino at operating range of Vcc of 7v to 9v.

The GPS module is integrated with the Arduino to provide the local coordinates – the latitude and longitude of the vehicle in real time. The GPS determines the coordinates every 10ms and transmits to the input pin of the Arduino. The 20X4 LCD display and GSM module are connected to the Arduino output pins. The Arduino uno microcontroller when activated by the vibration sensor transmits accident information and vehicle location to a remote server/phone of Emergency Management System (EMS) with the aid of GSM module. In between the GSM and the Arduino is a stop button to ensure the EMS is not communicated if their assistance is not needed. The system behavior can be best summarized in the flow chat in Fig. 4

The GPS module continues to communicate with the GPS satellites in space and uses the time of arrival of signals from the satellite to triangulate the vehicle position. The vehicle position is in turn fed into the Arduino by the GPS module. The Arduino then waits for the vibration sensor to sense impact beyond the threshold. When high impact is received, the vibration sensor tells the Arduino and the Arduino turns on the buzzer by sending logic "HIGH" to it, gets the current data of the GPS module, extracts the longitude and latitude coordinates and puts them in a message and sends to the GSM module. The coordinates of the vehicle can also be displayed on google map to enable the EMS team track the accident scene. The GSM module receives the message from the Arduino, searches for the emergency number the user has stored and sends the message to that number. The buzzer is meant to alert passersby that an accident has just occurred. The system also gives the occupants the option of stopping communications with EMS if their services are not required.

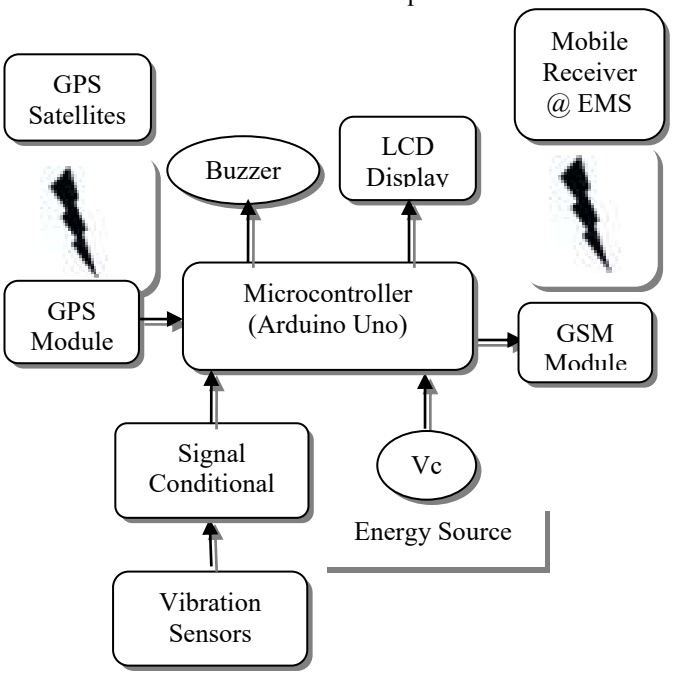


Fig 2: Block Diagram of the System

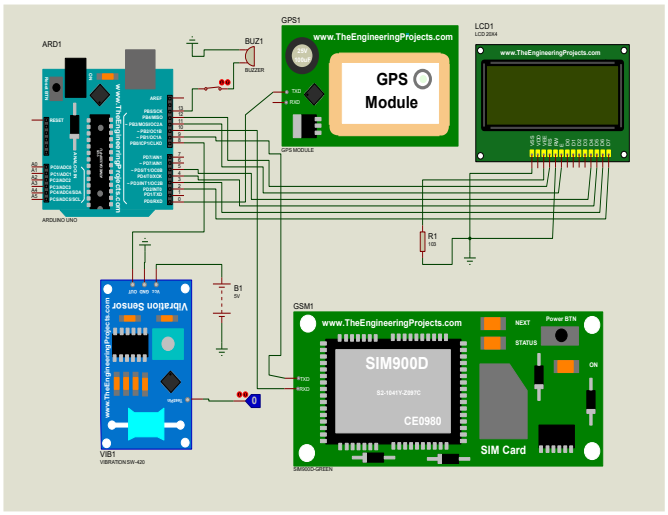


Fig. 3: The system circuit diagram

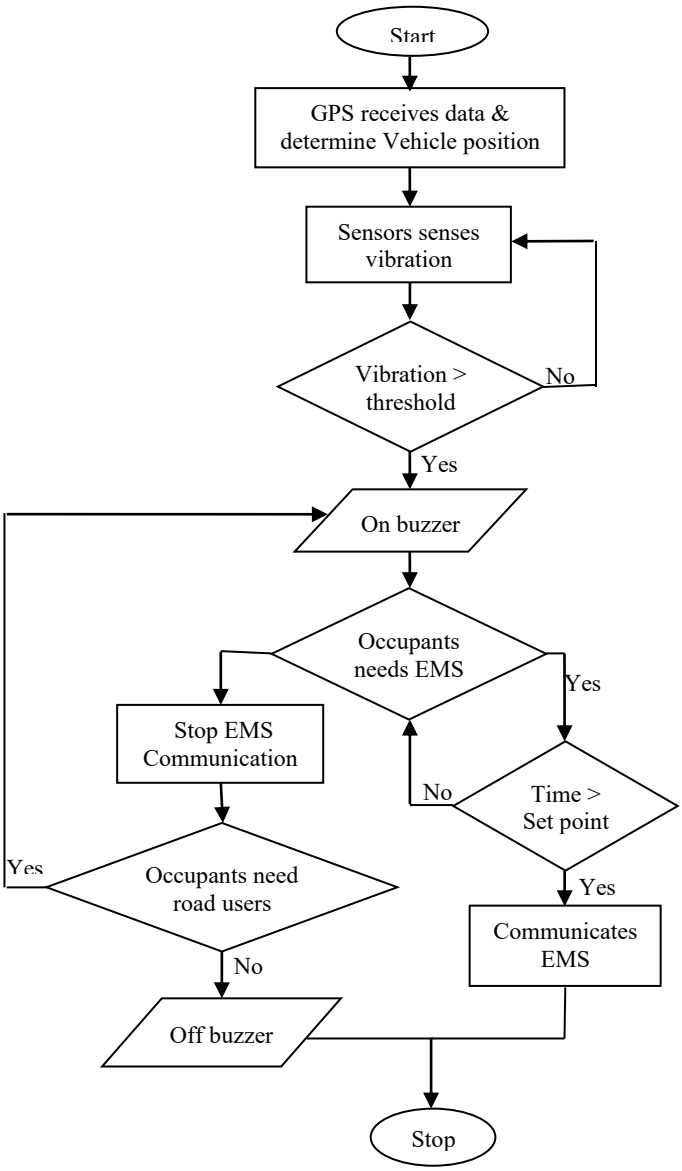


Fig. 4 The system flow chart

IV. RESULT ANALYSIS

The project is built in units and each unit was simulated and confirmed ok before the system integration and simulation test. A simple circuit comprising of the vibration sensor, an LED and an Arduino was developed to see how the vibration sensor functions. The simulation circuits of the vibration sensor in Fig 5 & 6 show the sensor sending logic 1 and logic 0 signals to the Arduino when the impact voltage is 7v and 6v respectively.

The system design performed as expected on completion as depicted in Fig 7. The system is designed to be on at all times, with a message popping up on the LCD to indicate that the system is in active state. At this point, the GPS module is receiving data but does not display it because no accident has occurred (logic 0 state). However, the moment an accident occurs with an impact voltage of 7v and above (logic 1 state) the buzzer begins to sound and the SIM module automatically collects the data from the GPS module via the Arduino, puts it in a text message and outputs the message on the LCD.

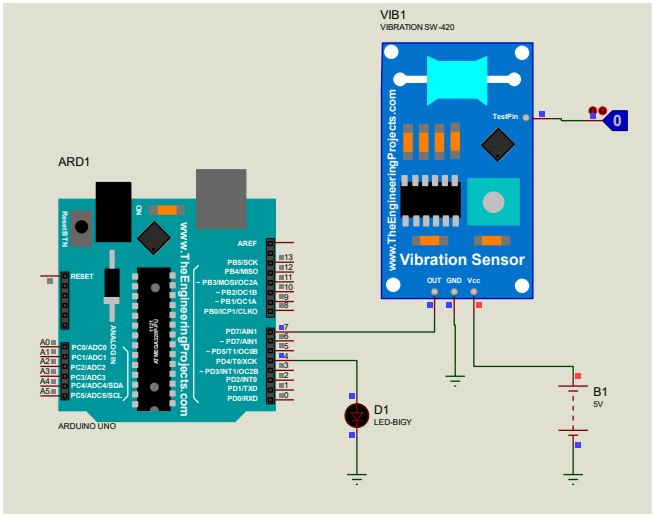


Fig 5: Schematic for vibration sensor testing on logic 0

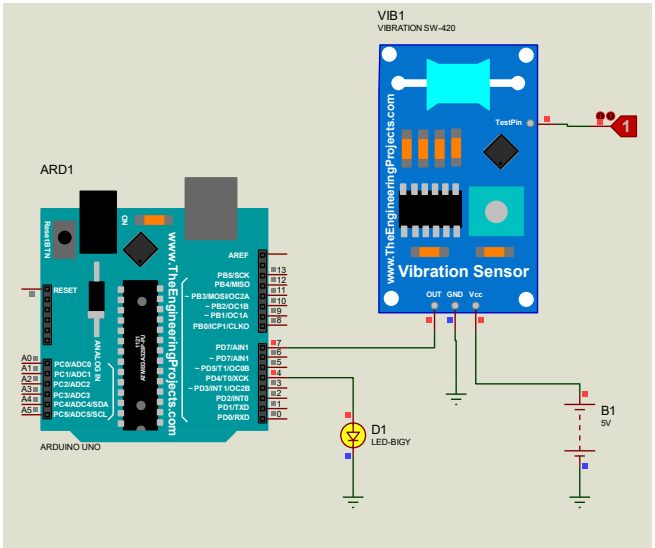


Fig 6: Schematic for vibration sensor testing on logic 1

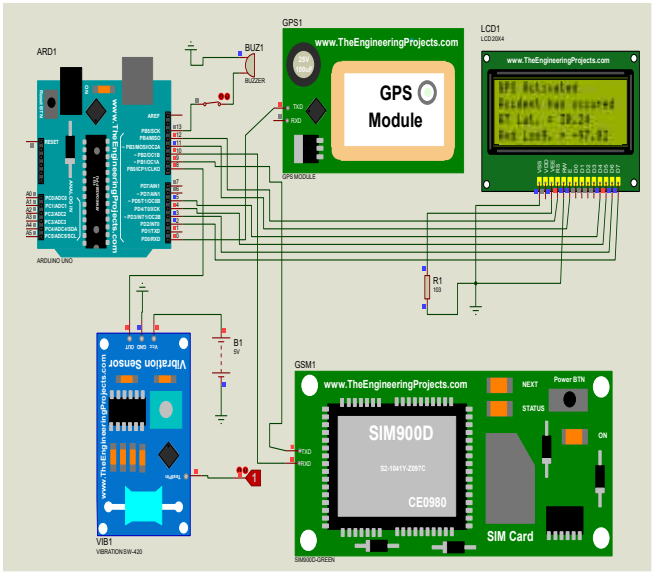


Fig. 7: System circuit simulation

V. CONCLUSION

The accident information system was designed to leverage on IoT technologies. The system continues to monitor the voltage level corresponding to the impact/vibration of the sensor effectively for necessary response. The GPS module calculates the coordinate-longitude and latitude of the vehicle in real-time and sends to the Arduino. The system dictates accidents when the Arduino senses voltage of 7v and above. The system has long distance communication facility which transmits text message using the GSM module to EMS on instruction from the Arduino when logic 1 is received and after 1munite must have elapsed without the driver hitting the stop button. The message which contains the coordinates of the vehicle involved in an accident is displayed on the EMS gadget with Google map for quick and effective response to the accident victims. The developed system meets the United Nations global goal of evening out and reducing the fatality rate in road accidents in this decade. Therefore, it is recommended for every driver especially those in the developing countries like Nigeria.

REFERENCES

[1] World Health Organization. *Global Status Report on Road Safety;* World Health Organization: Geneva, Switzerland, 2018.

[2] A. Khan, F. Bibi, M. Dilshad, S. Ahmed, Z. Ullah, H. Ali. "Accident Detection and Smart Rescue System using Android Smartphone with Real-Time Location Tracking". *Int. J. Adv. Comput. Sci. Appl.* 2018, 9, 341–355.

[3] L. Jackson and R. Cracknell. *Road Accident Casualties in Britain and the World;* House of Commons Library: London, UK, 2018.

[4] N.O. Onyemaechi and U.R Ofoma, "The Public Health Threat of Road Traffic Accidents in Nigeria: A call to Action", *Annals of Medical and Health Sciences Research*. Vol. 6, No. 4, 2016

[5] V. N. Ukoji, "Trends and Patterns of Fatal Road Accidents in Nigeria," *IFRA Nigeria Working Papers Series*, No. 35, 2014.

[6] Federal Road Safety Commission (FRSC). "5181dies in road accident in 2018 says FRSC" The Nation Newspaper, 8th September, 2019.

[7] WHO. Global Plan for the Decade of Action for Road Safety 2011 – 2020, Geneva: WHO; 2010.

[8] V. S. Reddy, L. P. Sree, V. N. Kumar, "Design and Development of accelerometer based System for driver safety", *International Journal of Science, Engineering and Technology Research (IJSETR)*, Volume 3, Issue 12, December 2014.

[9] L. Sanchez, J. Galache, V. Gutierrez, J. Hernández-Muñoz, J. Bernat, A. Gluhak, T. Garcia. "SmartSantander: The meeting point between Future Internet research and experimentation and the smart cities". In *Proceedings of the Future Network & Mobile Summit, Warsaw, Poland*, 15–17 June 2011; pp. 1–8.

[10] I. Din, M. Guizani, B. Kim, S. Hassan, M. Khan, "Trust Management Techniques for the Internet of Things: A Survey". *IEEE Access* 2018, 1, 1–27.

[11] M. Keertikumar, M. Shubham, R. Banakar, "Evolution of IoT in smart vehicles: An overview". In *Proceedings of the International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, India, 8–10 October 2016; pp. 804–809.

[12] O. Khan, M. Shah, I. Din, B. Kim, H. Khattak, J. Rodrigues, H. Farman, B. Jan. "Leveraging Named Data Networking for Fragmented Networks in Smart Metropolitan Cities". *IEEE Access* 2018, 6, 75899–75911.

[13] J. L. Hernandez-Ramos, M. V. Moreno, J. B. Bernabe, D. G. Carrillo, A. F. Skarmeta. "SAFIR: Secure access framework for IoT-enabled services on smart buildings". *J. Comput. Syst. Sci.* 2015, 81, 1452–1463.

[14] A. Saymum, R. Mid. Al-Mamun. "IoT based vehicle accident detection and rescue information system". Department of Computer Science and Engineering (CSE), East West University, Dhaka, Bangladesh, August 2017.

[15] N. Kattukkaran, A. George and M. Haridas, "Intelligent Accident Detection and Alert System for Emergency Medical Assistance", presented at the 2017 International Conference on Computer Communication and Informatics (ICCCI – 2017), Coimbatore, India, 2017.

[16] R. Ramkumar, S. Dinesh, S. Naveen Kumar, G. Prathiipa, *"Smart Alert System for Vehicles"*, Journal for Electronics and Communication Engineering, pp 32-39, 2016.

[17] A. Ajith Kumar, V. Jaganivasan, T. Sathish, S. Mohanram, *"Accident Detection and Alerting System Using GPS and GSM",* International Journal of Pure and Applied Mathematics, Vol. 19, Issue 15, pp 885-891, 2018.

[18] R. Sridhar, A. Sri Vignesh Prasanth, M. Pranesh, S. Gowtham and S.K. Thangarasu, "SMS Based Automatic Vehicle Accident Information System", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 3, Issue 2, 2014

[19] N. Patil Ashish, Y. Abhilash, "Accident Detection System Using Android Application", *International Advanced Research Journal in Science, Engineering and Technology*, Vol. 4, Issue 4, pp 118-120, January 2017.

[20] B.H. Sputh, O. Faust, and A. R. Allen, "A versatile hardware-software platform for in-stui monitoring system" In CPA, 2007, pp.299-311

An Optimization of Multi-Connected Roundabouts' Road Traffic Flows Using Adaptive Neuro-Fuzzy Inference System on Coordinated Traffic Control System

Babangida Zachariah, Philip O. Odion, Isah R. Saidu
Computer Science Department, Nigerian Defence Academy
Kaduna, Nigeria
babangidazachariah@gmail.com, poodion@nda.edu.ng,
rambo@nda.edu.ng

Patience N. Yabuwat
Computer Science Department,
College of Education, Gidan Waya
Kaduna, Nigeria
patienceyabuwat@gmail.com

***Abstract*—Traffic congestion is one of the prevailing challenges of modern cities. The negative impacts on educational, economical, health, and social activities are too numerous and great to mention or quantify with absolute accuracy. Efforts to deal with traffic congestions through construction and expansion of new and existing road networks have not yielded the desired result due to the associated cost. The introduction of static (or fixed-timed) and some basic dynamic controllers at isolated point of interest are ineffective and costly. Therefore, this research employed Adaptive Neuro-Fuzzy Inference System, ANFIS-based controller to perform optimized traffic control at nine (9) roundabouts of Kaduna metropolis in a coordinated manner. The results obtained from the simulated scenarios showed that ANFIS-based controller outperformed the 30s and 25s static traffic controllers by 65.97% and 62.32% respectively. An investigation into the choice of ANFIS membership type and number is recommended to determine if better results may be obtained for the considered road infrastructure.**

Keywords—Optimization, Multi-connected, Traffic Congestions, Adaptive Neuro-Fuzzy Inference System, Traffic Control Systems, Roundabouts

I. INTRODUCTION

Social, health and economic impact of traffic congestions remains a major concern for both developed and developing nations. Efforts are directed towards the development and implementation of inexpensive, but effective methods of managing and minimizing traffic congestions. Automated Traffic Control Systems (ATCS) is most economical methods for traffic congestions management against the manual traffic management approach as well as the expansion of road infrastructures in terms of number and capacity [1]–[4].

Automated traffic control systems may be static (fixed-timed), actuated or dynamic. The Static Traffic Control Systems (STCS) and Actuated Traffic Control Systems have several disadvantages that makes them unsuitable for implementation in the continuously dynamic traffic densities experienced at different locations and times on the road networks with conflicting right-of-ways. Dynamic Traffic Control Systems (DTCS) are effective real-time traffic control approaches, which consider the dynamism of traffic densities and other parameters. Therefore, DTCS are often implemented on road infrastructures with conflicting right-of-ways such as ordinary intersections or roundabouts [5]–[8].

Roundabouts are special intersections that are circular and have the advantages of higher motorists' safety and minimize traffic delays compared to their counterpart, the ordinary intersections, where two or more roads crossover themselves. Roundabouts (as well as ordinary intersections) may be signalized or un-signalized. Signalized roundabouts have ATCS installed to manage the traffic flows at the roundabouts, whereas the un-signalized roundabouts allow the motorist to negotiate right-of-ways using ordinary driving (or traffic) rules. The un-signalized roundabouts expose motorists and pedestrians to a higher risk of accidents as patience-less, inexperienced or unknowledgeable drivers have the tendencies of causing confusions that could lead to accidents. Therefore, the implementation of DTCS at Signalized roundabouts further enhances the performance of the roundabouts in terms of safety and minimized delays [9]–[11].

Signalized intersections (both roundabouts and ordinary intersections) are often controlled independently of others; in which case they are referred to as isolated intersections. This isolated control usually suffices as the most cost-effective option when the intersection is isolated in real life. That is, it is too far away from another intersection. However, in the case of multiple connected intersections that are close to each other, a coordinated control is usually not only cost-effective but often yields better performance [5], [8], [12]–[14].

Isolated ordinary intersections or roundabouts have had STCS and DTCS controllers implemented, which have yielded positive results compared to those that served as benchmarks. However, there is always a need for improvements as the solutions are soon overstretched by the increasing number of vehicles on the roads [15]. Tools such as particle swamp optimization, fluid dynamics models, artificial neural networks, fuzzy logic, adaptive neuro-fuzzy inference systems, etc. have been used in optimizing the efficiency and effectiveness of various controllers used in different fields such power systems, road safety management tools, isolated and coordinated traffic control systems, etc. [4], [7], [11], [16].

Therefore, this paper considers a case of multi-connected roundabouts having STCS controllers, and attempt to propose an optimized coordinated DTCS controller, which will allow the exploration of coordinated traffic controls for the general good and benefits of road users. The dynamism, as well as optimized phase duration determination, is achieve using ANFIS model.

II. Problem Statement

Kaduna North and Kaduna South Local Government Areas of Kaduna State are two major local governments that make up the Kaduna metropolis. They may be referred to as the economic and social hub of the state following that most Government Ministries, Departments and Agencies as well as major markets, private businesses and schools (both Secondary and Tertiary institutions). The other two Local Government Areas that adjoin to make the metropolis are Chikun and Igabi Local Governments. The implication is that most populace of Kaduna State often have to need to access the Town (as it is often called) for various educational, social and economic activities. For this study, it is from here referred to the Central Area.

In ideal traffic conditions, access to the Central Area is without unnecessary delays. However, this not the case as long traffic queues are often observed on the roads that lead to the Central Area. This is especially true considering the road network from around Queen of Apostles Catholic Church, Kakuri through to Kaduna-Zaria road. The high traffic congestions experienced on this road infrastructure is a result of the fact that ever-increasing population of the Kaduna metropolis live outside of the Central Area but are mostly engaged in educational, social or economic activities taking place in the Central Area. The usual unpleasant effects of traffic congestions are the experience of the motorist, pedestrians and inhabitants along with the said road infrastructure [7], [10].

The continuous efforts to contend the cumulative sum of vehicles in the State has led to the construction and expansion of the said road infrastructure as well as others. These efforts have led to the introduction of Nine (9) roundabouts along with the said road infrastructure due to the advantages of roundabouts over the ordinary intersection. These roundabouts are either signalized or un-signalized. The signalized roundabouts have STCSs implemented for traffic flow management. All of these efforts are yet to yield the desired expectations of ideal traffic conditions. Traffic congestion persists in the Central Area of the metropolis and requires better solutions to minimize the negative effects that come with it. Therefore, this research proposes coordinated traffic control systems for the Nine (9) roundabouts and develops an ANFIS model to implement a dynamic traffic control system at the roundabouts. This is an attempt to advance the level of effective traffic management along with the considered road infrastructure, which if not done may further increase the level of negative effects already experience in the region [15].

III. Literature Review

In [17], the theoretical concepts of coordinated control of traffic control systems was presented leading to the design of coordinated traffic control of multiple intersections considering cities of China. In an attempt to design the coordinated traffic control, vehicular average speed, fleet, and traffic turns were considered as the influencing factors. The model of the coordinated traffic control system was simulated in Verkehr In Stadten SIMulationmodel (VISSIM) and the results showed that the delays, average parking time and several vehicles passing the intersections for the coordinated traffic control system showed significant improvement over the existing system.

In [18], a mathematical model for a coordinated traffic control system for multiple intersections. Two-way arterial roads were considered for coordination based on bandwidth approach. Network decomposition techniques were used to minimize the computational complexity of the system. The developed model was simulated in VISSIM and the results were assessed for effectiveness and efficiency in terms of vehicular travel times, delays, stops and queues. The results obtained were considered effective and efficient.

In [19], coordinated traffic control for multiple intersections was developed based on bandwidth progression techniques and different models of pedestrian delays. The coordinated traffic control model considered different traffic conditions of vehicles and pedestrians using bilevel programming problems. The developed algorithm was tested on the VISSIM simulation platform. The analysis of the results revealed that a trade-off between efficiencies of large intersections and progression band; and that delays associated with pedestrians can be minimized.

In [20], the limitation of non-coordinated traffic controllers is acknowledged and a network of local controllers managing the traffic flows of various intersections are built and integrated such that coordination can be achieved by another controller. The local controllers are built as pre-timed signals controls whose signals plans are assessed and coordinated with those of other controllers in the network. The analysis of the system showed promising results leading to a positive conclusion that such hierarchical approach for traffic control coordination may be built and deployed.

In [21], an adaptive traffic control system is developed based on machine learning techniques. Machine learning techniques such as a k-nearest neighbour, decision tree, Bayesian classification, support vector machine and extreme learning algorithms were considered. The proposed system was based on a decision tree algorithm was numerically analyzed for nine ordinary intersections and the results proved the efficiency of the approach.

In [22], the deep reinforcement learning approach is adopted to manage large vehicular traffic networks in cities. The continuous identification of critical nodes of the network using data-driven approaches, while the traffic signal is controlled using deep reinforcement learning leads to the optimality of the traffic management of the network. The developed technique was simulated and the results were outperformed those of the baseline methods.

These researches have considered simple and complex networks of ordinary intersections but none considered the case of roundabouts. Following the advantages of roundabouts over ordinary intersections, a case of coordinated traffic control of multiple roundabouts may yield better results. Therefore, this research sought to use an adaptive neuro-fuzzy inference system approach to manage traffic flows of nine roundabouts that are unique to

themselves in terms of designs and number of inbound and outbound traffic flows.

IV. Materials and Methods

For this research, the simulation approach is adopted. The road network, vehicular traffic flows, traffic control systems and sensors for detection, counting and tracking of waiting times are all simulated. Therefore, this section presents the materials and methods used in carrying out this research.

A. *OpenStreetMap*

OpenStreetMap (OSM) is a community project that provides editable map data of the world [23]. It was used in this research to capture the map of the road infrastructure. This is to ensure that the geometric designs of the road network are accurate. The map shown in Figure 1 is a simplified view of the nine roundabouts considered in this research. The roundabouts are labelled with red colour.

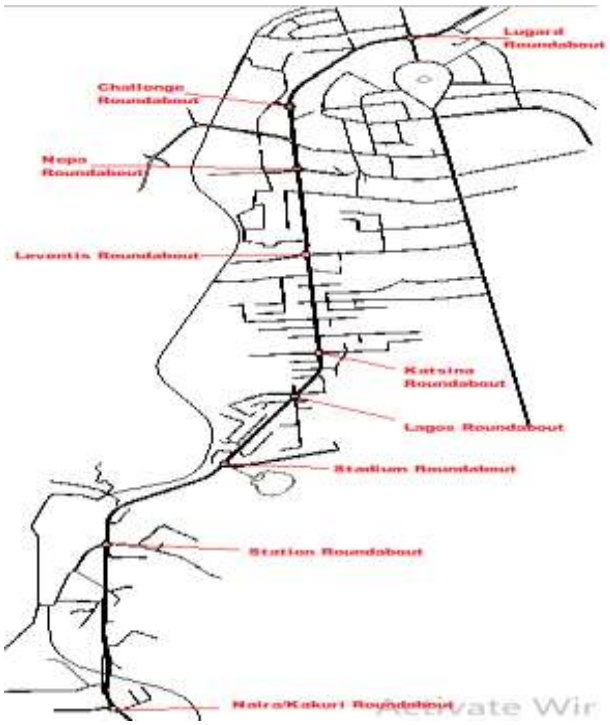


Figure 1: Map Showing Considered Roundabouts

B. *Simulation of Urban Mobility*

Simulation of Urban Mobility (SUMO) is an open project that allows the development of realistic traffic scenarios. SUMO is a suitable tool that is gaining popularity since it allows for the manipulation and control of its objects from suitable Application Programming Interfaces such as Traffic Control Interface for MATLAB (TraCI4MATLAB), Traffic Control Interface for Java (TraCI4J), and others [24], [25]. For this research, the acquired OSM object, traffic light control systems, vehicular traffic flows and the sensors for detection of traffic volumes were implemented in SUMO.

C. *MATLAB and TraCI4MATLAB*

Matrix Laboratory (MATLAB) was used in the design of ANFIS models and execution of TraCI4MATLAB API to interface ANFIS to SUMO and control the traffic lights control systems of the roundabouts.

The Five Gaus2 Membership Function type ANFIS model had two inputs and a single output as shown in Figure 2. It was trained with Six Hundred and Thirty-Six (636) data elements randomly generated and tuned by expert advice. The training and retraining of the model conceded to an error of 0.0050423. That is, it had an accuracy of 95.5%. The generated twenty-five (25) fuzzy rules produced the surface plot shown in Figure 3.

The inputs were traffic queue lengths and waiting times. The queue lengths and waiting times of vehicles waiting to utilize the roundabouts are fundamentals parameters that influence driving behaviours of a motorist, which has implications on the traffic conditions. Thus, queue lengths and waiting times, which the sensors supply at the end of every cycle and fed as input to the ANFIS model, which determines the suitable phase duration for the next cycle. Phase duration, as determined by and the output of the ANFIS model is used to set the length of the green wave of the traffic light for a given flow at the roundabouts. The tuning of ANFIS parameters was done using the Hybrid Learning Method, which employs Least-Squares and Gradient Descent Learning algorithms.

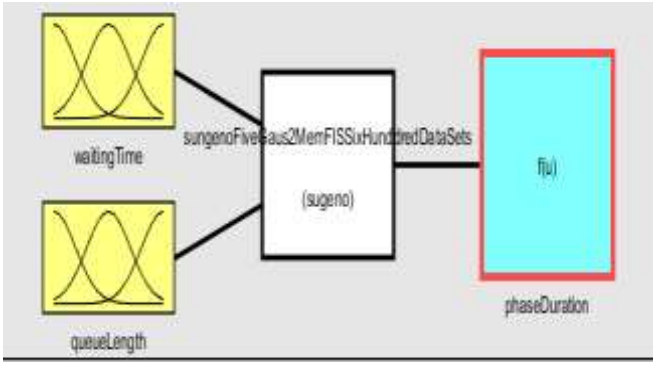


Figure 2: The Designed ANFIS Model

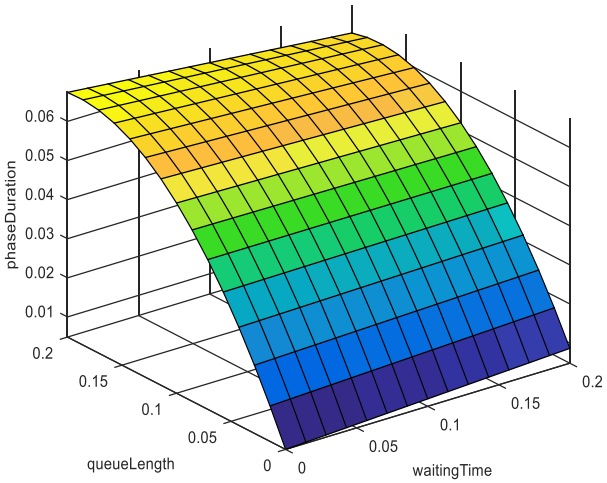


Figure 3: The ANFIS Model Surface Plot

Most STCS in Nigeria often use either 25s or 30s green phase duration. Some of the traffic lights control systems on the roundabouts considered in this research use 25s green

wave duration while some use the 30s green wave duration. Therefore, both the 25s and 30s systems were developed and tested in this research.

V. Simulations and Results Discussions

This research developed simulation models of STCS and DTCS. The DTCS was the ANFIS model described in section 3. The models were subjected to the same traffic volumes and their performances in terms of average waiting time (or delays) at the nine roundabouts was assessed. The traffic volumes were set at seventy (70), three hundred and fifty (350) and one thousand, four hundred 1400 vehicles per hour for all major roads of the considered road infrastructure. This represented Under-Saturated Traffic

Condition (USTC), Saturated Traffic Condition (STC) and Over-Saturated Traffic Condition (OSTC) respectively. This section presents the simulation models results.
Two STCS simulation models having 25s and 30s green wave phase allocation for the different traffic flows at the roundabouts were modeled and the results of each of those models were compared to that of the ANFIS-based DTCS as shown in TABLE I.

From TABLE I, the results of twenty-five seconds (25s) STCS was compared with those of thirty seconds (the 30s) STCS. The 25s STCS outperformed the 30s STCS when traffic volumes were considered to be USTC and OSTC both in terms of the average waiting time and number of collisions. However, when traffic volumes were set to be saturated, the 30s STCS outperformed the 25s STCS in both cases too.

In terms of maximum queue lengths of waiting for vehicles at the considered roundabouts, it is clear from Figure 4.1A and Figure 4.1B that the maximum queue length for a 30s STCS controller was fourteen (14) vehicles on the North-Southern flows and seven (7) vehicles on West-Eastern flows when traffic volumes were set to under-saturated flows. For the STC shown in Figure 4.2A and Figure 4.2B, comparing the 25s STCS controller to 30s STCS controller showed that the 25s STCS controller had shorter queue (maximum number of the vehicle that waited) at the roundabouts in the West-Eastern flows. However, for the OSTC shown in Figure 4.3A and Figure 4.3B, the 30s STCS controller had the shorter queues in the West-Eastern flows compared to the 25s STCS.

From TABLE I, comparing the results of ANFIS-based DTCS controller to the 30s and 25s STCS controllers showed that the ANFIS-based DTCS outperformed both the 30s and 25s STCS controllers in terms of average waiting times in the USTC, STC and OSTC. ANFIS-based DTCS outperformed 30s and 25s STCS by 84.90% and 82.88% in the USTC; 55.36% and 56.64% in the STC; 66.57% and 61.24% in the OSTC respectively. However, the STCSs no vehicular crash in the case of USTC while the ANFIS-based DTCS had one (1). However, the STCSs had crash cases in the case of STC and OSTC while the ANFIS-based controller had none.
In terms of a maximum number of vehicles that waited at the roundabouts in when ANFIS-based DTCS controller was used, the maximum number of vehicles was only nine (9) against the twelve (12) and fourteen (14) when the 30s and 25s STCS controllers were used in the USTC as shown in Figure 4.1A-Figure 4.1C. In the case of STC, the maximum number vehicles that waited at the roundabouts was fifty (50) vehicles against the ninety (90) vehicles in the North-Southern flows and twenty-five (25) against thirty-five (35) vehicles in the West-Eastern flows as shown in Figure 4.2A-Figure 4.2C. Finally, in the case of OSTC, the maximum number of vehicles that waited at the roundabouts in the West-Eastern flows was thirty (30) vehicles against fifty (50) and forty-three (43) vehicles in the case of 25s and 30s STCS controllers as shown in Figure 4.3A-Figure 4.3C.

Therefore, the general performances of the controllers as shown in TABLE I shows the overall average waiting times of for 30s STCS controller was 13.64s, 25s STCS controller was 12.32s and DTCS controller was 4.64s. This implies that the 25s STCS outperformed the 30s STCS by 9.68% while the ANFIS-based DTCS controller outperformed 30s STCS controller by 65.97% and 25s STCS controller by 62.32%. This shows the capability and the potential of the DTCS over the STCS.

TABLE III. COMPARATIVE RESULTS OF SIMULATED MODELS

		Simulated Models					
		30s STCS	*25s STCS*	*% Perfor. (25s Against 30s STCS)*	*DTCS*	*% Perfor. (DTCS Against 30s STCS)*	*% Perfor. (DTCS Against 25s STCS)*
Under-Saturation	***AWT***	4.45	3.92	11.79	0.67	84.90	82.88
	NC	0	0	-	1	-	-
Saturation	***AWT***	9.47	9.75	-2.96	4.23	55.36	56.64
	NC	0	1	-	0	-	100.00
Over-Saturation	***AWT***	27.00	23.29	13.77	9.03	66.57	61.24
	NC	4	1	75.00	0	100.00	100.00
Average Performances		13.64	12.32	9.68	4.64	65.97	62.32

[b.] AWT: Average Waiting Time

[c.] NC: Number of Collisions

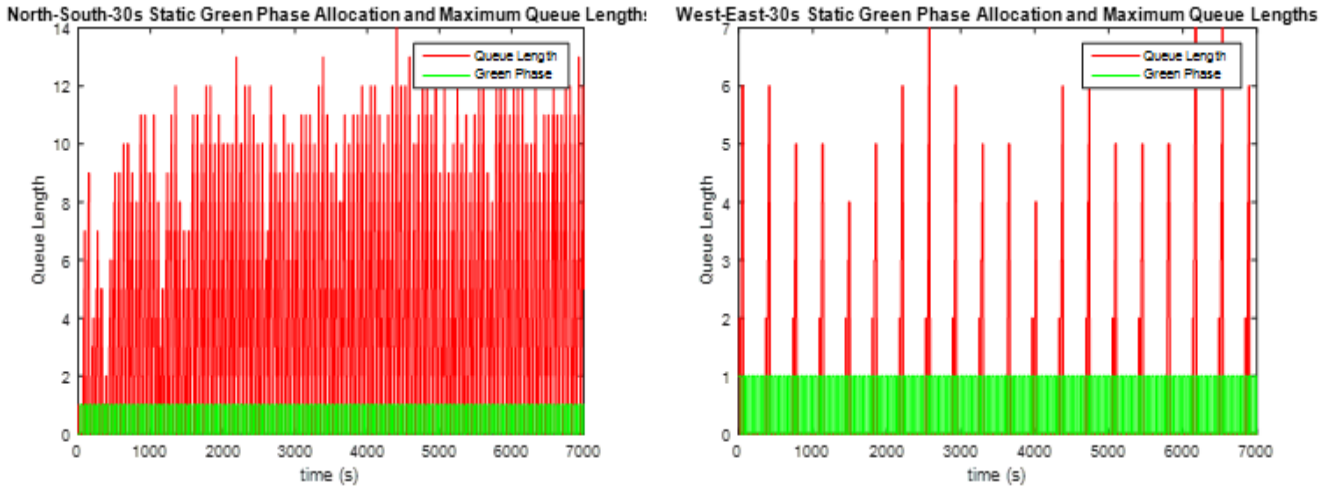


Figure 4.1A: Maximum Queue Lengths for USTC with 30s STCS Controller

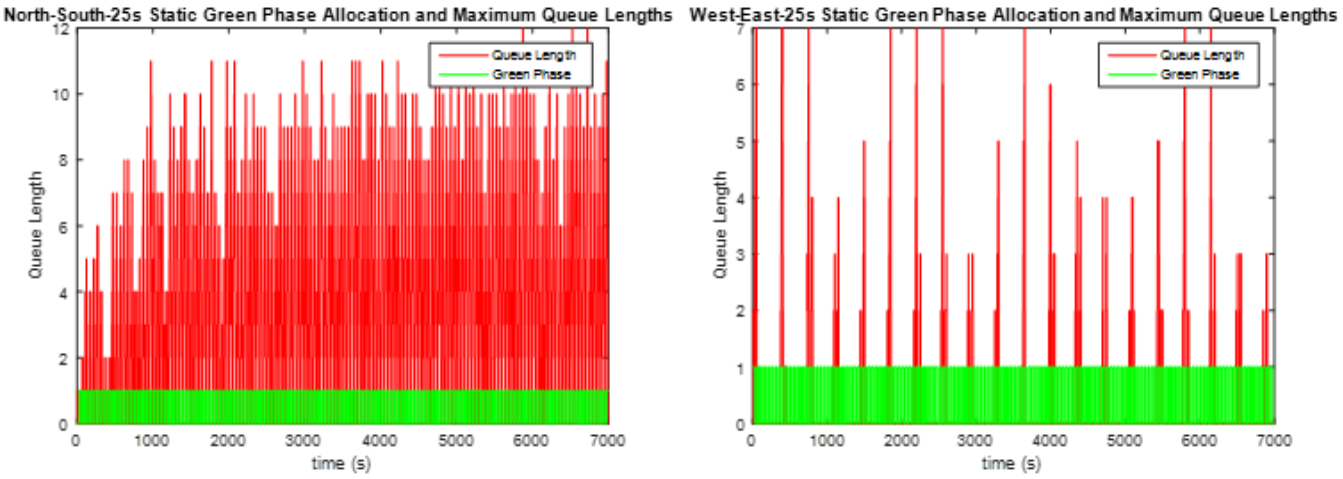


Figure 4.1B: Maximum Queue Lengths for USTC with 25s STCS Controller

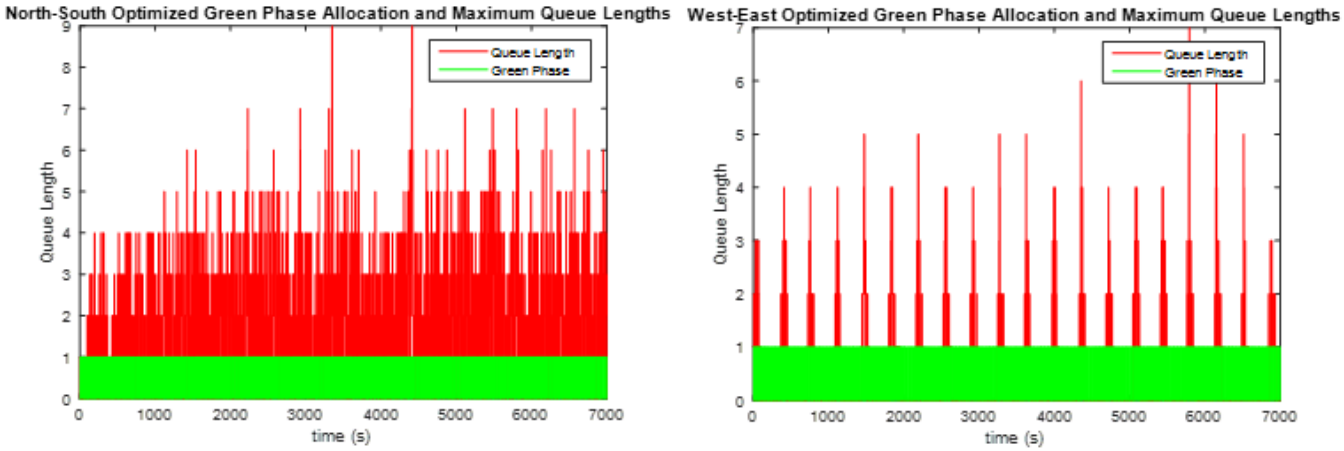


Figure 4.1C: Maximum Queue Lengths for USTC with DTCS Controller

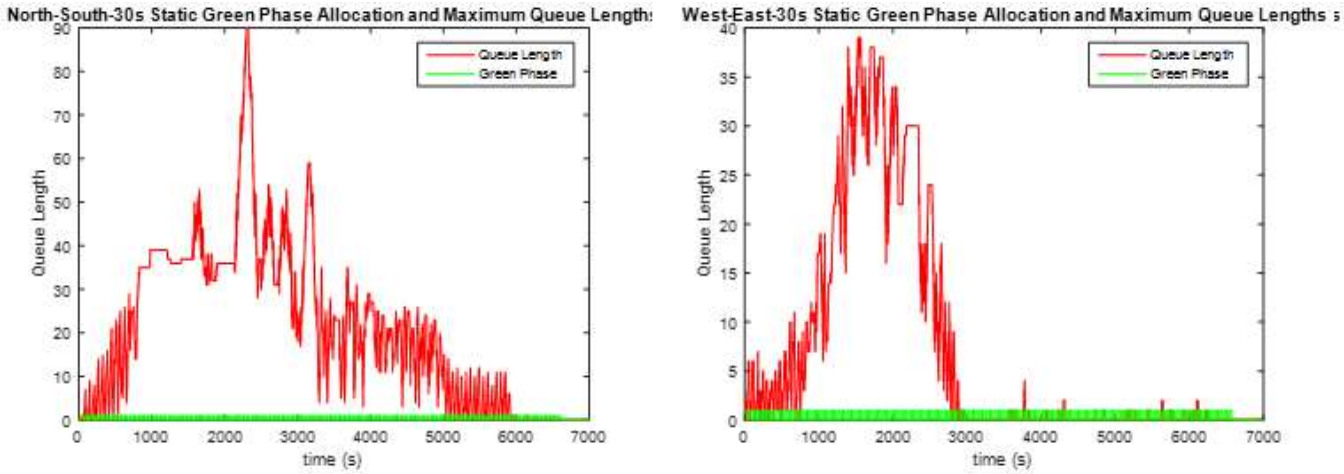


Figure 4.2A: Maximum Queue Lengths for STC with 30s STCS Controller

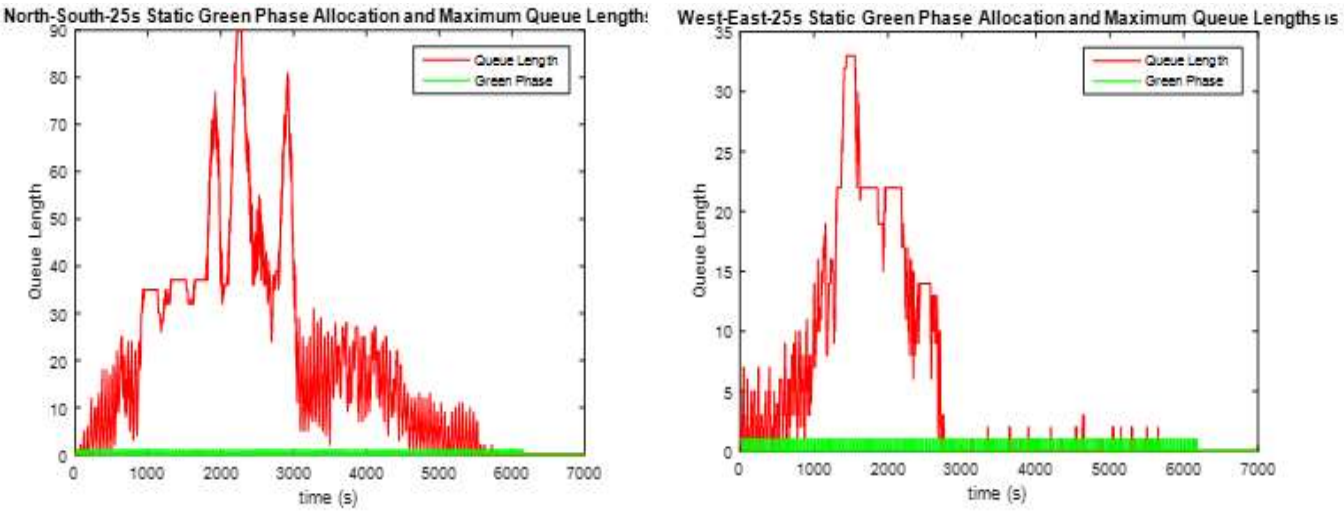


Figure 4.2B: Maximum Queue Lengths for STC with 25s STCS Controller

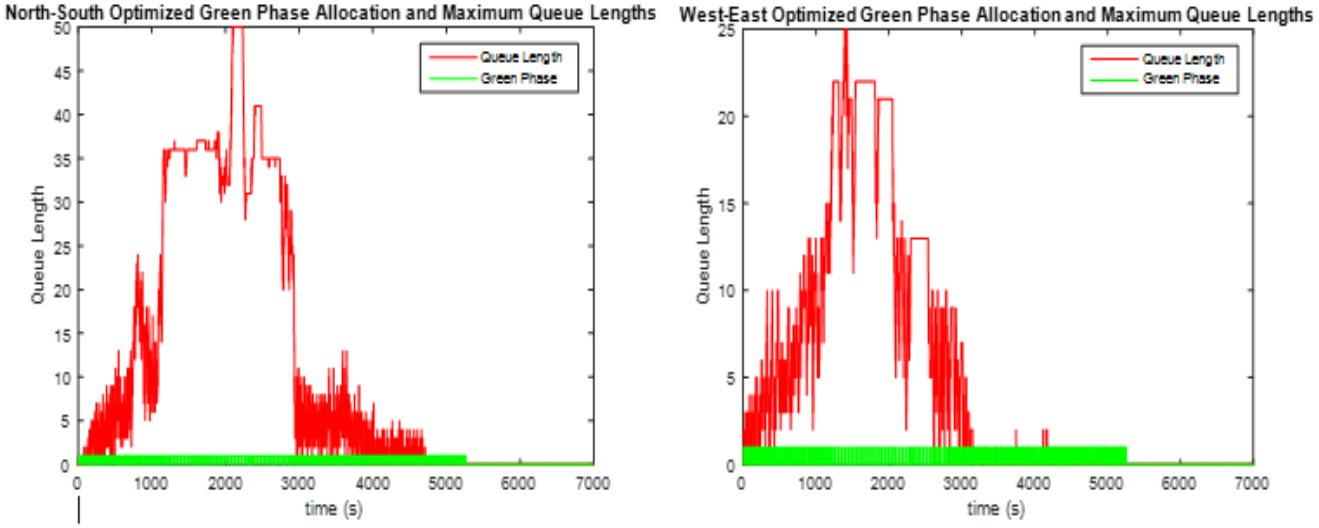


Figure 4.2C: Maximum Queue Lengths for STC with DTCS Controller

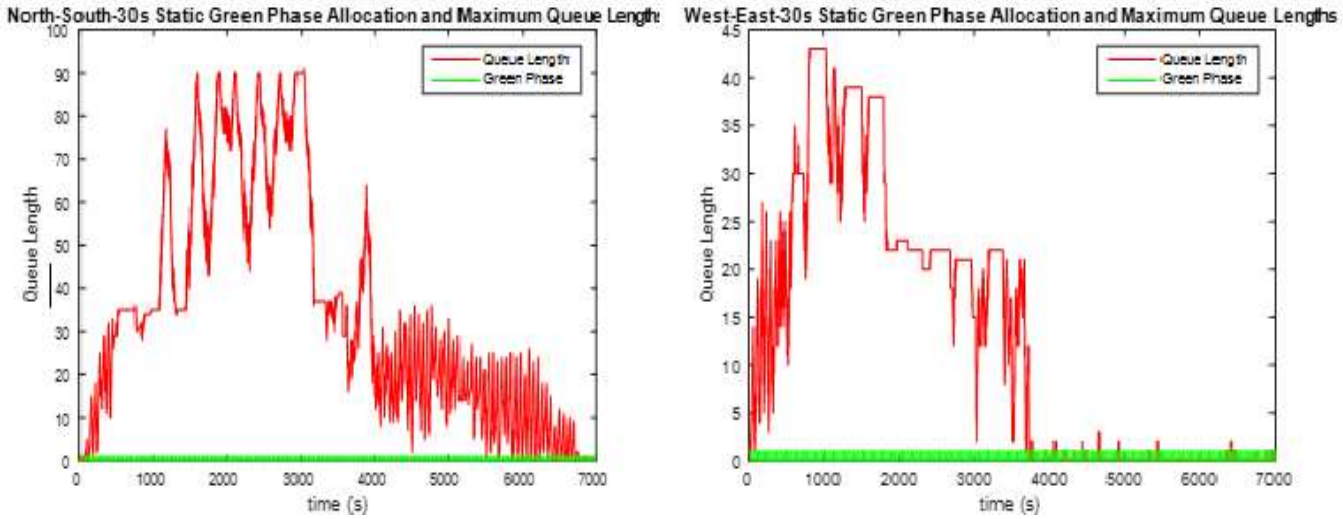


Figure 4.3A: Maximum Queue Lengths for OSTC with 30s STCS Controller

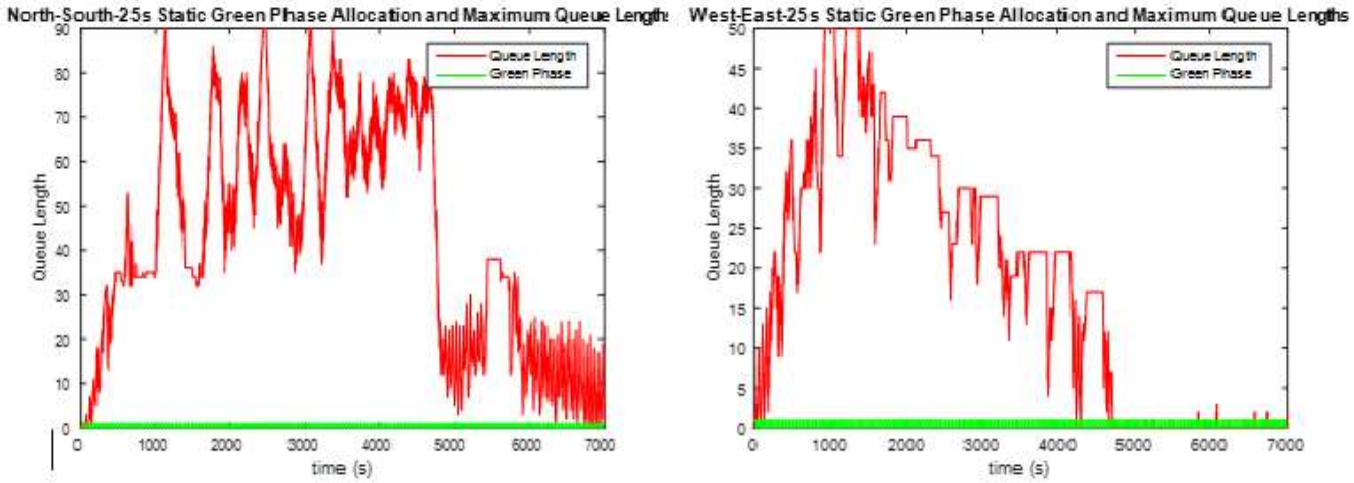
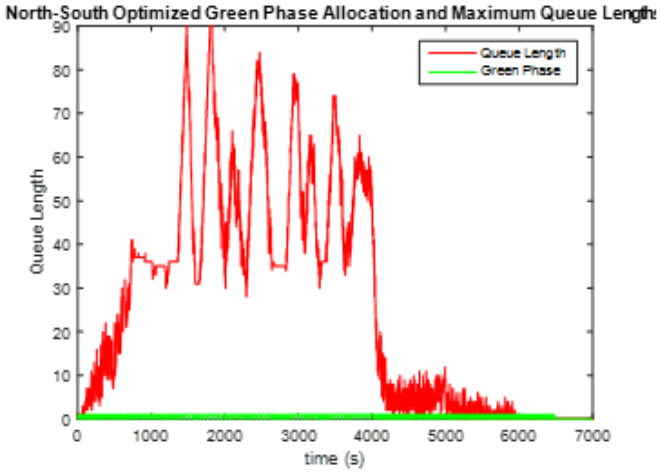


Figure 4.3B: Maximum Queue Lengths for OSTC with 25s STCS Controller



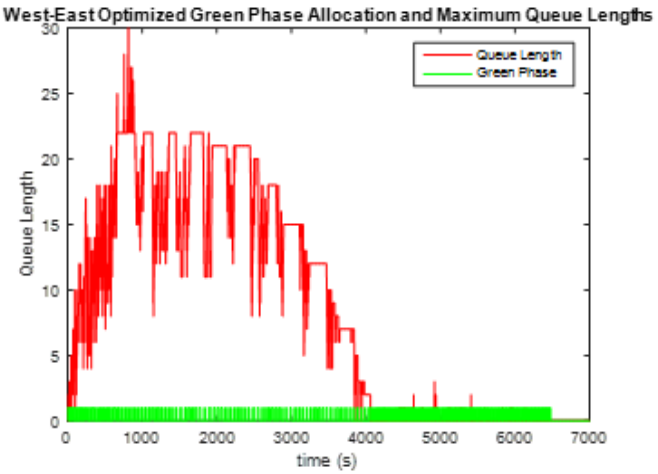


Figure 4.3C: Maximum Queue Lengths for OSTC with DTCS Controller

VI. CONCLUSION

Since traffic congestions, serious negative implications on the educational, health, social and economic status of every economy, the need to find workable solutions to minimize these effects remains a necessity. This research employed Adaptive Neuro-Fuzzy Inference System in a coordinated manner to solve the traffic problems around nine roundabouts in Kaduna metropolis of Kaduna State, Nigeria. From obtained results, ANFIS-based DTCS outperformed the STCS irrespective of the green phase duration used. However, a closer consideration of the individual results shows that the performance, whether statics or dynamic largely depends on the traffic conditions such as traffic volumes, vehicular allowable speeds, geometric parameters of the road infrastructure under consideration. This research cannot claim to have solved the problem of traffic congestion in its entirety. Therefore, a lot needs to be done to advance the effectiveness of the results of traffic controllers with extensive consideration of the various necessary parameters. Besides, the choice of number and type of membership functions has significant impact on the controller. This presents another opportunity to develop another ANFIS model for traffic control on the considered road infrastructure.

REFERENCES

[1] M. E. Fouladvand, Z. Sadjadi, and M. R. Shaebani, "Characteristics of Vehicular Traffic Flow at a Roundabout," *arXiv*, 2008.

[2] R. S. Tomar and S. Verma, "Vehicular Communication for Enhancing Safety in Transportation System," *IUP J. Syst. Manag.*, vol. 9, no. 2, pp. 1–9, 2009.

[3] M. Inţă, "Improving performance of roundabout intersections by optimizing traffic-flow speed," *MATEC Web Conf.*, vol. 121, pp. 1–8, 2017.

[4] B. Zachariah, P. O. Odion, and R. I. Saidu, "Roundabouts Modeling and Vehicular Traffic Control Techniques : A Survey," *IUP J. Inf. Technol.*, vol. XVI, no. 1, pp. 1–17, 2020.

[5] L. Jun, X. Liangjie, F. Juan, W. Ming, and L. Zhaokan, "Considering the Pedestrian Crossing Coordinated Control on Multi-Leg Roundabouts," *IEEE - Int. Conf. Intell. Comput. Technol. Autom. Considering*, no. 50778141, pp. 1023–1026, 2010.

[6] M. Jha and S. Shukla, "Design Of Fuzzy Logic Traffic Controller For Isolated Intersections With Emergency Vehicle Priority System Using MATLAB Simulation," *Control Instrum. Syst. Conf. ariXiv*, 2014.

[7] B. Zachariah, P. Ayuba, and L. P. Damuut, "Optimization of Traffic Light Control System of An Intersection Using Fuzzy Inference System," *Sci. World J.*, vol. 12, no. 4, pp. 27–33, 2017.

[8] C. Zhao, Y. Chang, and P. Zhang, "Coordinated Control Model of Main-Signal and Pre-Signal for Intersections with Dynamic Waiting Lanes," *MDPI Sustain.*, vol. 10, pp. 1–14, 2018.

[9] E. Damaskou and F. Kehagia, "Quality of service (QOS) of Urban Roundabouts : a Literature Review," *Int. J. Transp. Syst.*, vol. 2, pp. 37–45, 2017.

[10] P. Ayuba, B. Zachariah, and L. P. Damuut, "Modification Of Fuzzy Logic Rule Base In The Optimization of Traffic Light Control System," *Sci. World J.*, vol. 13, no. 2, pp. 6–11, 2018.

[11] S. Kazima and J. Musabyimana, "Road Environment Situation Detection Based on 2D LIDAR Sensor," *Int. J. Mechatronics, Electr. Comput. Technol.*, vol. 9, no. 31, pp. 4060–4069, 2019.

[12] P. Tallapragada and J. Cortes, "Coordinated intersection traffic management," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 233–239, 2015.

[13] A. Vlasov, "Features of Calculation of Traffic Light Control Modes in the Conditions of Intensive Road Traffic," *ElsevierTransportation Res. Procedia*, vol. 20, pp. 676–682, 2017.

[14] A. Abdulhafedh, "How to Design Traffic Signals at Multiple Coordinated Intersections," *Int. J. Autom. Control Intell. Syst.*, vol. 4, no. 3, pp. 29–35, 2018.

[15] F. T. Achi, "The Effects Of Traffic Congestion On Travel Time In Kaduna," Ahmadu Bello University Zaria, 2016.

[16] H. Farshi, "Design and Analysis of Hybrid PSO-GA-FA Technique for Load Frequency Control of Two-Area Power System," *Int. J. Mechatronics, Electr. Comput. Technol.*, vol. 9, no. 33, pp. 4287–4301, 2019.

[17] X. Guo, H. Sun, and X. Wang, "The design of traffic signal coordinated control," in *AIP Conference Proceedings:Materials Science, Energy Technology, and Power Engineering*, 2017, vol. 1839, no. 020137.

[18] B. Ye, W. Wu, and W. Mao, "A Method for Signal Coordination in Large-Scale Urban Road Networks," *Math. Probl. Eng.*, vol. 2015, 2015.

[19] D. Li, Y. Song, and Q. Chen, "Bilevel Programming for Traffic Signal Coordinated Control considering Pedestrian Crossing," *Hindawi J. Adv. Transp.*, vol. 2020, 2020.

[20] F. Kurniawan, O. Dinaryanto, and M. Irawati, "Pre-Timed and Coordinated Traffic Controller Systems Based on AVR Microcontroller," *TELKOMNIKA*, vol. 12, no. 4, pp. 787–794, 2014.

[21] A. Sadollah, K. Gao, Y. Zhang, Y. Zhang, and R. Su, "Management of traffic congestion in adaptive traffic signals using a novel classification-based approach," *Eng. Optim.*, pp. 1–20, 2018.

[22] M. Xu, J. Wu, L. Huang, R. Zhou, T. Wang, and D. Hu, "Network-wide traffic signal control based on the discovery of critical nodes and deep reinforcement learning," *J. Intell. Transp. Syst.*, pp. 1–10, 2019.

[23] D. Sinton, "OSM: The Simple Map That Became a Global Movement," *The Direction Mag*, 2016. [Online]. Available: https://www.directionsmag.com/article/163. [Accessed: 18-Jun-2020].

[24] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz,

"SUMO – Simulation of Urban MObility: An Overview," *Third Int. Conf. Adv. Syst. Simul.*, pp. 55–60, 2011.

[25] D. Krajzewicz *et al.*, "Simulation of modern Traffic Lights Control Systems using the open source Traffic Simulation SUMO," *SUMO Conf.*, 2015.

SHORT MESSAGE SERVICE (SMS) SPAM DETECTION AND CLASSIFICATION USING NAÏVE BAYES.

Christine Bukola Asaju, Ekuma James Nkorabon
Department of Computer Science,
Federal Polytechnic Idah,
Idah, Kogi State, Nigeria.
chrisamaju02@gmail.com, ekuma_ejn@yahoo.com

Richard Ojochegbe Orah
College of Information and Communication Technology
Salem University Lokoja
Kogi State, Nigeria.
orahseun@gmail.com

ABSTRACT: The dynamic nature of technology has caused an unprecedented technological and socio-economical development in everyday life. This development is making everyone to be highly vulnerable to diverse threats. Short Message Service (SMS) spam is one of such threats that affect the security of mobile devices. These spam attempts to deceive users into providing their private information which could later result in a security breach. The major problem of SMS spam is that attackers, hackers, email phishing, ransomware, etc., used it to exploit the victims. The urge to curb this has necessitated this work. Different models have been developed to detect SMS spam, some of these models include Support Vector Machine, Linear Classifier, Decision Trees, Random Forest, Logistic Regression, Naive Bayes, etc. However, most of these techniques have not addressed the point that focuses on SMS spam detection and classifies new SMS spam. The goal of this research is to develop a machine learning model for the detection and classification of new SMS spam. This paper presents a model for SMS spam detection and classification that employs the Naïve Bayes machine learning methodology. String to word vector feature extraction was used to extract the SMS Spam text file from the contents that were collected via UCL repository in its original form. At this point, the proposed system is set to perform data preprocessing, dataset feature extraction, and model training as well as model evolution. The model was learned based on an SMS dataset that consists of 5525 samples collected from an online resource and utilized effectively. The experimental results indicate classification accuracies of 99.42%, for correctly classified and 0.57% for incorrectly classified, respectively in the best cases.

Keywords: *Short Message Service(SMS) spam, Naïve Bayes, String to word, Machine Learning*

I. INTRODUCTION

With the development of technology, there have been various means used in communication. One of such is a text messaging on mobile devices. Text messaging also known as Short Messaging Service (SMS) is a text communication platform that allows mobile phone users to exchange short text messages. These messages are usually less than 160 seven-bit characters [1]. A major problem that cell phone users encounter is the reception of unsolicited SMS messages. Unsolicited messages are regarded as spam messages. These messages usually come from advertisers and other sources.[2] As the popularity of the platform increases, there is a surge in the number of unsolicited commercial advertisements sent to mobile phones using text messaging [3].

An automated technique for identifying spam to prevent its delivery is regarded as spam filtering [4]. Spam filtering exists both for text messages and emails but has some differences. One of such disparity is that emails, which have a variety of large datasets available, but real databases for SMS spams are very limited. Another difference is that text messages are short in length of words, therefore, the number of features that can be used for its classification is far less compared to emails. In text messages, there is no header as well. Additionally, text messages are full of abbreviations and have much less formal languages than what is experienced from emails. All of these factors may result in a serious degradation in the performance of major email spam filtering algorithms applied to short text messages.

Consequently, SMS spam detection and classification requires an effective and efficient method. Although models have been developed to detect SMS spam, many of these techniques have not addressed the point that focuses on SMS spam detection and classifies new SMS spam. The is a major gap this research is seeking to solve. The research focus is to develop a machine learning model for the detection and classification of new SMS spam.

The objectives of the research are the application of a machine-learning algorithm to SMS spam detection and classification problem. The research further explores the problem, and design an application based on one of this algorithm that can detect and classify new SMS spam with high-performance accuracy.

II. DATASET DESCRIPTION

The data set adopted for the work comprised of 5574 text messages from the UCI Machine Learning repository gathered in 2012 [5] (SMS Spam collection Dataset from the UCI Machine Learning Repository.

It is comprised of a collection of 425 SMS spam messages that were manually extracted from the Grumble text Web site, a subset of 3,375 SMS that was chosen randomly, non-spam (ham) messages of the NUS SMS Corpus (NSC), a list of 450 SMS non-spam messages collected, and the SMS Spam Corpus v.0.1 Big (1,002

SMS non-spam and 322 spam messages publicly available)[5].

III. SMS SPAM DETECTION AND CLASSIFICATION WORKFLOW

Below is the working flow of SMS Spam detection and classification.

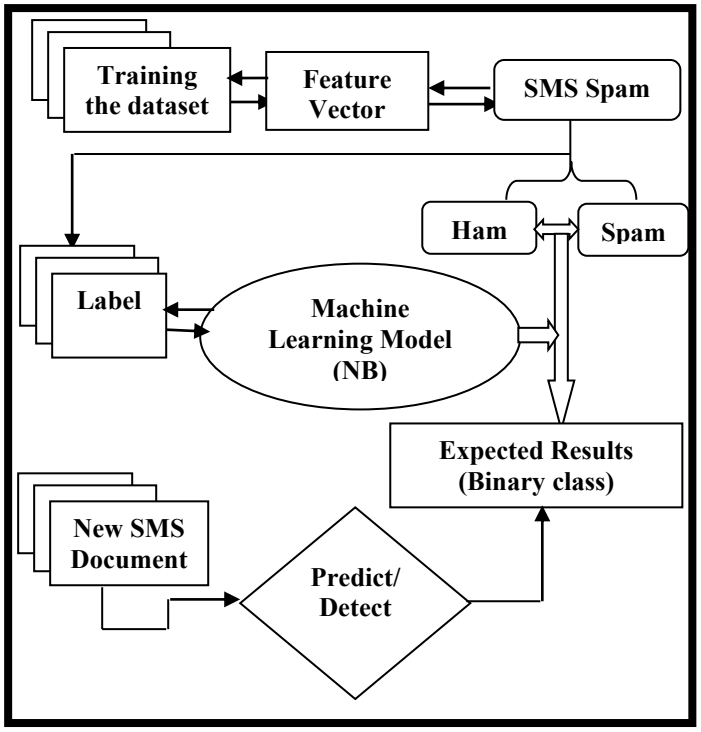


Figure 1: The working flow of SMS Spam Processes

The performance of the classifier was summarized and evaluated. Feature extraction and initial analysis of data were done with library Weka. The application of machine learning algorithms (weka plugin) was done in the NetBeans IDE for the implementation of the model.

The paper is organized as follows: Section IV discusses the related works on SMS data mining, using Naïve Bayes algorithm. Section V describes the methods of approach, and VI discuses the implementation , while VII discusses the result. The conclusion and future work is found in VIII.

IV. RELATED WORKS

Short messaging Services (SMS) has become an important means of communication today between millions of people around the world. SMS services, which are a must-have service nowadays for telecom operators, transmit their messages using standardized communications protocols. At the same time, problems are being faced which is caused by SMS spamming. Previously, it has been explained that SMS spam and email spams have similar features. Therefore, spam filtering methods used in emails can be adopted for SMS spam filtering to deal with the spread of mobile phone spams [6, 7]. Nonetheless, the properties exhibited by SMS spams is different from the email spams. SMS spam in email has few characters and is limited to 140bytes by standard text messages [8]. Due to restrictions, many times, mobile devices spams are written in less formal languages such as abbreviations or idioms. Unfortunately, SMS spams irritate users the same way as e-mails [9, 10, and 12].

Another study which is on spam filtering methods and measures was carried out by Chang et al. [13]. Spam filtering methods and features reweighting methods based on good word attack strategies were developed by them. This approach depends on the limited character and short text messages on top of the weight values which are evaluated against a dataset (i.e. SMS and comment dataset). They opined that a good word attack strategy will mislead the classifier's output with the least number of input characters. The authors in the work also introduce a feature reweighting method in which a novel rescaling function is proposed. This function is aimed at reducing the significance of the features characterizing a short word. This method is performed to rescale the weights and increase the linear classifier's robustness against a good word attack strategy.

Sethi et al. [14], compared different machine learning algorithms that filters and detect SMS spam messages using three basic procedures, namely; the raw text messages, the length of the messages, and the information gain matrix. Naïve Bayes, Random Forest, and Logistic Regression algorithms were adopted in the experiment.

Meanwhile, in [15] different machine learning algorithms were used to train four features derived from SMS text messages. These features include the size of the message, monograms with the highest frequency in the text messages, frequently occurring diagrams, and a class of messages (i.e. ham and spam as 0 and 1 respectively). The authors were able to make a discovery that the Naïve Bayes algorithm outperforms the other classifiers used in the study.

Different features for SMS spam classification were also explored and analyzed by Choudhary and Jain [16]. Numerous features were extracted from SMS text messages including mathematical symbols, special symbols, and emotions, among many others. In their study, characteristics and behaviors of SMS spam messages for classification with a successful result was achieved.

An SMS spam filtering method using non-content features was proposed by [17]. Static features were used instead of the content of an SMS text message as features, (i.e. number of messages and message size), temporal features (i.e. number of messages sent in one day, size of messages in one day and time of day) and network features (i.e. number of recipients and clustering coefficients) in the study. In the detection of spammers, it was discovered that incorporating network and temporal features into conventional static features, a better performance was achieved.

Warade et al. concept of spam detection in [18] was based on the relationship between the sender and receiver and the message contents. For lack of mutual relations between the senders and the receivers, a text message is classified as spam while the SMS displays the contents of the spam. The message is then automatically transferred into the spam box. Whereas, with mutual relation between senders and receivers, an SMS text message is considered legitimate with no visible spamming content. The

relationship between senders and receivers will be examined through the inspection of SMS logs and the direct relationship between the two.

Safie et al. [19] applied string to word vector feature extraction to prove that SMS spam detection and classification work better. They achieved this through a vector space and Artificial Neural Network (ANN) algorithm. Accuracy shows a significant improvement.

[20] aims at comparing the performance of different algorithms with feature selection and algorithms without a feature selection. The first approach was that the sampled data was being examined without any filters or features selection, then the classifiers were tested each time beginning with the best-first feature selection to be able to select the most beneficial features and then apply various classifiers for classification.

Using Random Tree classifier, achieved 99.72% accuracy which means it works best to detect spam emails. In conclusion, the accuracy of email filters was improved greatly when the algorithm with feature selection was applied to the entire process and that classifiers of tree shape are more efficient in detecting spam emails [21].

[22] in their work, also detected an unknown zero-day phishing email that relies on an evolving connectionist system. The system was named the phishing dynamic evolving neural fuzzy framework (PDENFF). This framework follows a hybrid learning approach (supervised/ unsupervised) and is supported by an offline learning feature to achieve its purpose. Adopting this system helped in enhancing the detection of zero-day phishing e-mails was improved between 3% and 13%. Moreover, it used rules, classes, or features to enhance the learning process using ECOS which provided the system with the advantage of distinguishing phishing emails from a legitimate one [22].

[23] developed a model for classifying phishing emails. They adapted the forest machine learning mechanism. The dataset used comprises of 2000 phishing emails with advanced features. This model was able to achieve an accuracy of 99.7% classification with low false negative(FN) and false positive(FP). It was further reiterated that this model is more efficient because it requires fewer features to detect phishing.

A fraudulent detection model was proposed by [24] using an advanced selection of features where the different categories were compared in terms of the fraudulent email detection rate. The study was conducted applying several classification approaches and algorithms, such as SVM, NB, J48, and CCM, in addition to different features sets. An accuracy percentage of 96% was achieved and the results indicated that the level of accuracy was affected by the type of selected features rather than the classifiers' type, [24].

In [25], Kathirvalavakumar et al proposed a multilayer neural network to detect phishing emails. The proposed network depends on a feedforward pruning algorithm that extracts distinguished data and features from the email and applies a weight trimming strategy. This pruning strategy helps in reducing the number of features that go through the algorithm resulting in minimum computation required for classification of emails into phishing or not. The network has provided fair results in terms of false positives and false negatives. This network was tested on data from 2007, thus, using this network for current data requires identifying the new features to the algorithm incorporating them into input domain for training to be useful, [25].

Consequently, effective and efficient methods are required for SMS spam detection and classification. Although different models have been developed to detect SMS spam, many of these techniques have not addressed the point that focuses on SMS spam detection and classifies new SMS spam, and that is a major gap this work seeks to address. The researchers' effort is to develop a machine learning model for the detection and classification of new SMS spam.

V. MATERIALS AND METHOD

This section focuses on the concept of spam detection using machine learning tasks. The approach was based on the samples of SMS Spam concerning their classes. Based on this fact, the system will be built with the available data set collected with other related literature reviews such as journals or articles.

A. Machine learning Approach

1) Collect the sample data (SMS Spam/historical data)

2) Pre-processing (that is the data were provided with two labels, spam, and ham), since it is a supervised learning approach, then it is a binary classification.

3) Apply feature extraction with Weka library (to convert the SMS Spam into binary classification analysis)

4) Resample the dataset by applies training set and testing set during system development analysis using Weka tools.

Develop the model with Weka plugin and used java Netbeans IDE environment to implement the system with all the requirements stated above and used the proposed algorithm to perform the classification model and structured data analytics.

B. Naïve Bayes Classifier

The Naïve Bayes classifier provides a new way of analyzing data based on Bayes theorem. It is based on evidence by maintaining a relation between the target and the problem space. It is a probabilistic classifier that uses Bayes theorem with some solid assumptions. It is used for text classification. The real-world applications use Naïve Bayes classifier for email sorting, spam detection, document categorization, etc. It is a very efficient method because it is less computationally intensive in CPU and memory use as it uses a small amount of training data. In general, a Naïve Bayes classifier assumes the presence and absence of a particular feature required to classify a data set. The probability model for a classifier is denoted by p(C|F1 ,.....,Fn). Where c denotes the class variable which is used to classify the sample dataset, and F_1 to F_n is the number of features. If the number of features n is large or a single feature is containing a large number of values, the probability table becomes infeasible. So, the Bayes theorem is rewritten as equation (1) below:

$$P^{(C|F_1}; \ldots; F_n) = \frac{p(C)\, p(F_1;\ldots;F_n\, F|C}{p(F_1;\ldots;F_n)} \quad (1)$$

C. System Design

The method adopted to achieve this work is as follows:

SMS Spam data collection

SMS Spam data pre-processing

SMS Spam Feature extraction

Training set and Test set

Build the model

Based on this concept above, supervised learning will be used for training of the algorithm with a label of the class it belongs., the algorithm learns the relationship between the feature sets and the output by using the labeled data and hence it is then able to classify the unlabeled data from the learned relationship. Figure 3 shows the conceptual framework of the model.

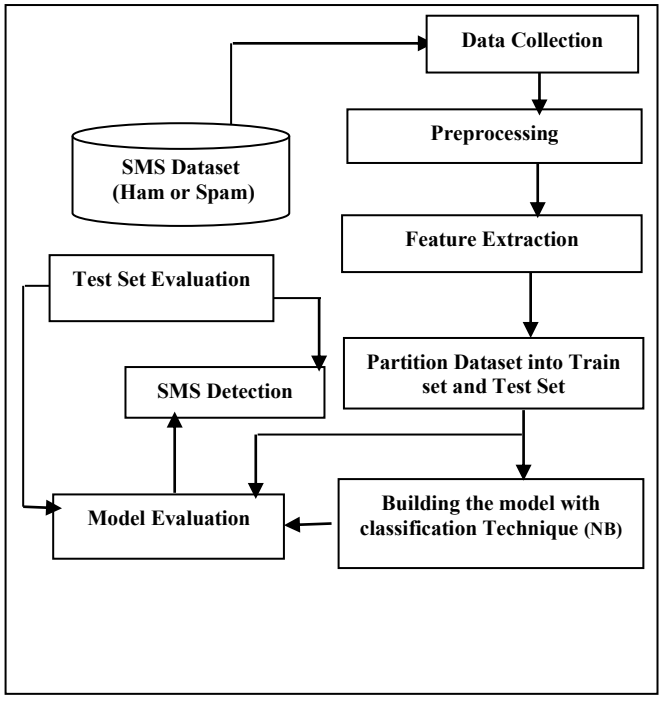


Figure 3. Steps for SMS Spam classification

Pre-Processing

In this step, complete geometric correction and filtering are done. The preprocessing uses the output of the classifier to take the required action to improve the performance.

Dataset Description

The dataset used in this paper is freely available on the internet. This was collected via the UCI repository was used for this analysis. This dataset consists of 2 attributes and 5525 instances. The first attribute, class_att has two possible values spam and ham which are nothing but class labels. Spam has 747 instances whereas ham has 4778 instances. Attribute one represents the name of the label. The second attribute is text, whose values are nothing but a text message, [26].

Experimental Set-Up

All the experiments that were carried out in this section are computed using open source tool Weka 3.8.0[27] and java programming language with Netbeans IDE under the OS Windows for implementation of the machine learning model and processor with 4GB of main memory. Weka is a collection of a machine learning algorithm for data mining tasks. These algorithms may be applied directly using the default algorithm in the tool itself or we can call the algorithm using java code [28]. The following subsection discusses more content of dataset, pre-processing of the dataset, and performed classification and detection using naïve Bayes.

Selection of Training Data

In this step, the particular attributes are selected which best describes the pattern for detecting either the messages is spam or ham.

Classification of Outputs

The output of the expected result is classified as to different categories accordingly namely ham or spam.

VI. IMPLEMENTATION

This section focuses on the general implementation and results of the research. The system was implemented with a sample of SMS datasets, for a binary classification technique namely ham and spam. Based on these concepts the data was collected and utilized for the detection and classification of the machine learning model. This was achieved with the proposed model namely Naïve Bayes. This algorithm was used to train the data collected and the model was built by calling the java code without using the default algorithm. These SMS datasets were pre-processed and features were extracted before applying a classification algorithm on it. The classification method used for this work was based on the Naïve Bayes algorithm which was able to capture all the required training sets and used the test set to make prediction/detection and classification.

The system was implemented with the set of two (2) features to distinguish their performance. When those factors were structured into the Weka model and java NetBeans for parameter turning, the proposed model was achieved successfully with five thousand, five hundred and twenty-five (5525) instances, which was used to perform this analysis. This result was used to build the model for predicting a promising result. Here the binary value from a given sample was transformed into an excel format with an extension of csv and arff for the machine-readable task.

Model Evaluation

The experiment of SMS detection or classification was done on two folds, which are the sample of the dataset collected that was used to perform SMS classification. And

the training set was used to build the model and then used the test set for predicting the result with an unknown class label to predict a new class label with their respective classes as shown below

Correctly Classified Instances	*522*	*99.4286 %*
Incorrectly Classified Instances	*3*	*0.5714 %*
Kappa statistic		*0.9763*
Mean absolute error		*0.011*
Root mean squared error		*0.0742*
Relative absolute error		*4.5086 %*
Root relative squared error		*21.3327 %*
Total Number of Instances		*525*

Table 1. Detail Performance Evaluation by class

class	Precision	Recall	F-Measure	ROC Area
spam	0.986	0.973	0.980	0.997
ham	0.996	0.998	0.997	0.997

Notably, Naïve Bayes achieved a good performance in this experiment in terms of accuracy by class with 0.986-0.996 in precision, 0.973-0.998 in recall, 0.980-0.997 in F-measure while ROC is 0.997-0.997 in both cases.

Table 2. The New SMS Test set for model evaluation

	New SMS Detection and Classification	Binary Class
1	Hello, brother, you have won a brand new car for yourself, call this landline for claiming your price	spam
2	Congratulation!!! You have won yourself a free brand new laptop, contact this 0807890786323 for collection	spam
3	Sorry, I was unable to make it yesterday	ham
4	Wow!!! special offer for you get 4GB for 1000 to enjoy this amazing offer, just recharged above 200	spam
5	Please if you reach inform me about your school fees to tell your dad	ham
6	It's ok, I will keep you abreast	ham
7	ATM BLOCK: Dear customer your ATM card has been blocked due to BVN upgrade of the year quickly call 09052207076 to reactivate within 24h	spam

VII) DISCUSSION OF RESULTS

The results of this work were achieved with the SMS dataset and the model evaluations were done with training data as showing above in under section VI. The result obtained is based on the proposed model that was used to classify the total number of 5525 instances and the accuracy of the model is 99%. This could be inferred that the system was able to learn well and captured all the required sample data for effective utilization.

VIII) CONCLUSION AND FUTURE WORK

The SMS spam messages problem is of the increase in almost every country today. The increase is without a sign of slowing down, as the number of mobile users increases. The cheap rates of SMS services are also a contributing factor to this increase. Therefore, this paper presents the spam detection and classification using Naïve Bayes algorithms.

Before the analysis was done the proposed system used a weka tool to perform the resampling technique, where the dataset where partition into the training set and testing set with the following file format (arrf and txt). Our partition was done with 90% of the training set and 10% of the testing set. After this, the researchers implemented the model with java code written in weka machine learning that was able to handle feature extraction with embedded n-grams feature technique as well as string to word vector function. The data set was trained in both arrf and txt file format. Based on this concepts the model was built with the training set and evaluation was done using the test set and this was able to classify the message into binary classification with our proposed model (Naïve Bayes) and detect the SMS spam being sent to the receiver and the expected results is either spam or ham.

However, it is not enough to evaluate the performance of the model based on the accuracy alone, since the dataset is experiencing imbalanced; therefore, the precision, recall, f-measure and ROC Area of the algorithms must also be observed. After some examinations, Naïve Bayes provides good accuracy by class with 0.986-0.996 in precision, 0.973-0.998, in recall, 0.980-0.997 in F-measure while ROC is 0.997-0.997 in both cases and the results based on the features used. For future works, adding more discretization feature set as a necessary step in the model estimation for better performance.

From the analysis of the results obtained, Naïve Bayes copes well with the SMS dataset. It was well concluded that these results are of sufficient accuracy to be of much practical use. Hence, the effort of future research is to improve classification performance with the discretization feature set as a necessary step in the model estimation for better performance.

It is therefore recommended that SMS Spam message detection and classification using the Naïve Bayes will be of help to the society from such messages that can deceive them to supply all their necessary personal details for easy tracking.

References/Bibliography

[46] Shirani-Mehr, Houshmand. "SMS spam detection using machine learning approach." (2013): 1-4.

[47] Alzahrani A, Rawat DB. Comparative Study of Machine Learning Algorithms for SMS Spam Detection. SoutheastCon (2019) Apr 11 (pp. 1-6). IEEE.

[48] Qian, Wang, Han Xue, and Wang Xiaoyu. "Studying of classifying junk messages based on data mining." Management and Service Science, 2009. MASS'09. International Conference on. IEEE, 2009

[49] Cormack GV. Email spam filtering: A systematic review. Now Publishers Inc; 2008.

[50] SMS Spam Collection Data Set from UCI Machine Learning Repository,"http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection"

[51] Q. Xu, E., W. Xiang, Q. Yang, J. Du, and J. Zhong. (2012) "SMS Spam Detection Using Noncontent Features." IEEE Intell. Syst. 27(6): 44–51.

[52] Sethi, G., and V. Bhootna. (2014) SMS Spam Filtering Application Using Android.

[53] Nagwani, N. K. (2017) "A Bi-Level Text Classification Approach for SMS Spam Filtering and Identifying Priority Messages." 14 (4): 8

[54] Almeida, T. A., J. M. Gómez, and A. Yamakami. (2011) "Contributions to the Study of SMS Spam Filtering: New Collection and Results." p. 4.

[55] Mujtaba, D. G., and M. Yasin. (2014) "SMS Spam Detection Using Simple Message Content Features." J. Basic Appl. Sci. Res. 4 (4): 5.

[56] Delany, S. J., M. Buckley, and D. Greene. (2012) "SMS Spam Filtering: Methods and Data," Expert Syst. Appl. 39(10): 9899–9908

[57] Shirani-Mehr, H. (2013) "SMS Spam Detection using Machine Learning Approach." p. 4.

[58] Chang, P. P. K., C. Yang, D. S. Yeung, and W. W. Y. Ng. (2015) "Spam Filtering for Short Messages in Adversarial Environment." Neurocomputing 155: 167–176.

[59] Sethi, P., V. Bhandari, and B. Kohli. (2017) "SMS Spam Detection and Comparison of Various Machine Learning Algorithms", in 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN). pp. 28–31

[60] Mujtaba, D. G., and M. Yasin. (2014) "SMS Spam Detection Using Simple Message Content Features." J. Basic Appl. Sci. Res. 4 (4): 5.

[61] Choudhary, N., and A. K. Jain. (2017) "Towards Filtering of SMS Spam Messages Using Machine Learning-Based Technique", in Advanced Informatics for Computing Research 712: 18-30.

[62] Q. Xu, E., W. Xiang, Q. Yang, J. Du, and J. Zhong. (2012) "SMS Spam Detection Using Noncontent Features." IEEE Intell. Syst. 27(6): 44–51.

[63] Warade, S. J., P. A. Tijare, and S. N. Sawalkar. (2014) "An Approach for SMS Spam Detection." Int. J. Res. Advent Technol. 2 (2): 4.

[64] Safie, W., N.N.A. Sjarif, N.F.M. Azmi, S.S. Yuhaniz, R.C. Mohd, and S.Y. Yusof. (2018) "SMS Spam Classification using Vector Space Model and Artificial Neural Network." International Journal of Advances in Soft Computing & Its Applications 10 (3): 129-141.

[65] Rathi, M., & Pareek, V. (2013). Spam Mail Detection through Data Mining-A Comparative Performance Analysis. International Journal of Modern Education and Computer Science, (12), 31

[66] Al-Momani, A., Gupta, B. B., Wan, T. C., Altaher, A., & Manickam, S. (2013). Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email

[67] Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics

[68] Nizamani, S., Memon, N., Glasdam, M., & Nguyen, D. D. (2014). Detection of fraudulent emails by employing advanced feature abundance. Egyptian Informatics Journal, 15(3), 169-174.

[69] Sa'id Abdullah Al-Saaidah (2017), Detecting Phishing Emails Using Machine Learning Techniques, https://www.meu.edu.jo/libraryTheses/590422b4d5dd8_1.pdf, Retrieved 23/06/2020

[70] Kathirvalavakumar, T., Kavitha, K., & Palaniappan, R. (2015). Efficient Harmful Email Identification Using Neural Network, British Journal of Mathematics & Computer Science, (1), 58

[71] Almeida, T.A., GÃ³mez Hidalgo, J.M., Yamakami, A. Contributions to the Study of SMS Spam Filtering: New Collection and Results. Proceedings of the 2011 ACM Symposium on Document Engineering (DOCENG'11), Mountain View, CA, USA, 2011.

[72] Kotthoff L, Thornton C, Hoos HH, Hutter F, Leyton-Brown K. Auto-WEKA 2.0: Automatic model selection and hyperparameter optimization in WEKA. The Journal of Machine Learning Research. 2017 Jan 1;18(1):826-30.

[73] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, Ian H. Witten (2009); The WEKA Data Mining Software: An update; SIGKDD Explorations, Volume 11, Issue 1. [Available Online: http :// www.cs. waikato.ac.nz/ ml/weka/index.html]

Flattening the Curve of COVID-19 Through Emerging Disruptive Technologies in Nigeria

Cosmas Ifeanyi Nwakanma
IT Conergence Engineering, School of Electronics Engineering,
Kumoh National Institute of Technology
Gumi, South Korea
http://orcid.org/0000-0003-3614-2687

Grace Egbi Alilu
Computer Science and Engineering Department,
Postgraduate College, Obafemi Awolowo University)
Ile Ife, Nigeria
graceegbi@gmail.com

Jane ChigozieNwakanma
Public Health Technology, School of Health Technology
Federal University of Technology
Owerri, Nigeria
hellojanecos@yahoo.com

***Abstract*-The coronavirus (COVID-19) which originated from Wuhan, China in December 2019, has become a global issue as it has spread rapidly to other countries. The aim of this paper is to look at how the curve of the virus can be flattened using emerging disruptive technologies such as Artificial Intelligence (AI), Virtual/Augmented reality and Internet of Things (IoT). Data for this research were collected using questionnaire which was created using Google forms. From the analysis carried out, all the emerging disruptive technologies played significant roles in flattening the curve of COVID-19 in Nigeria. In terms of the disruptive technologies that played most significant role in the pandemic, 72.7% of respondents attributed it to IoT. However, beyond Pandemic, 42%, 45% and 86% of respondents believed that AI, VR/AR and IoT respectively will play major roles towards disease control and public health emergencies.**

Keywords- artificial intelligence, COVID-19, internet of things, public health, virtual reality

I. INTRODUCTION

According to World Health Organization (WHO), the COVID-19 is an infectious disease caused by a newly discovered coronavirus and it spreads primarily through droplets of saliva or discharge from nose of an infected person [1]. The virus originated from Wuhan, China in December 2019. By early 2020, it has spread to other parts of the world which made the World Health Organization declare it a pandemic.

According to the European Centre for Disease Prevention and Control, COVID-19 has claimed the life of 327,904 people as of 21 May 2020, with over four million confirmed cases in 212 countries worldwide. In Nigeria, there are 6,677 confirmed cases with about 200 deaths as of 21 May 2020 [2]. The virus is spreading very fast and its end cannot be seen in the nearest future. It might even be a virus that has come to stay like the human immunodeficiency virus (HIV). Nigeria is even yet to reach its climax of the virus infection as the number of infected persons keeps increasing every day. The challenge globally with respect to COVID-19 is on flattening the curve while hope of potent vaccines and cure is gotten.

Flattening the curve here means slowing down the spread of the COVID-19. The curve can be flattened by using emerging disruptive technologies especially in the area of Information and Communication Technologies (emerging ICTs). The aim of this paper is to provide answers the following research questions (RQ):

RQ1: Which of the emerging Information and Communication Technologies has been the most effective in flattening the curve of COVID-19?

RQ2: Which of the emerging technologies has the Nigerian government been using in the fight against COVID-19 and, have they been using it effectively?

RQ3: What are the factors that can hinder the use of the emerging technologies in Nigeria?

RQ4: What are the factors that can aid the use of the emerging technologies in Nigeria?

RQ5: Beyond the pandemic, which emerging technology will remain in use?

There are over 200 countries that are suffering from the COVID-19 pandemic but this research will focus on Nigeria. The focus on Nigeria in this paper is due to the unique approach adopted by various countries and regions in addressing the pandemic [3] and due to coverage area of research interest due to limited works on Nigeria in similar area. To the best of our knowledge, this work is one of the few with Nigeria as a focus. While researchers have focused on several disruptive technologies, most works have identified internet of things (IOT) [4], artificial intelligence (AI) [5], [6] and virtual/augment reality (VR/AR) [7] as promising to the flattening of the COVID-19 curve. This justified the focus of this paper on these three.

II. EMERGING DISRUPTIVE TECHNOLOGIES AND HOW THEY CAN FLATTEN THE CURVE OF COVID-19

Emerging technology may mean different things to different people and as such, there is no universally adopted definition of the term.

Emerging technologies are technologies whose development, practical applications, or both are still largely unrealized, such that they are figuratively emerging into prominence from a background of non-existence or obscurity. A technology is emerging if it is not yet a “must have” [8], [9].

Some of the emerging disruptive technologies that is reported by recent works [5]-[7] in the areas of information and communication technologies are:

A. Artificial intelligence
B. Virtual/Augmented reality.
C. Internet of Things (IoT)

A. Artificial Intelligence (AI)

"Artificial intelligence is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings" [5].

Frankenfield [10], noted that artificial intelligence is based on the principle that human intelligence can be defined in a way that machine can easily mimic it and execute tasks, from most simple to more complex ones [10].

AI is continuously evolving to benefit many different industries and individuals and as such, it can be used to flatten the curve of COVID-19 in the following different ways [11],[12]:

a) Diagnosis: According to Samer, pneumonia, which is a common symptom of COVID 19 infection, can now be diagnosed by computed tomography (CT) scan in less than sixty seconds with an accuracy of 92% and a recall rate of 97% on test data sets [6].From this, AI technologies can be used to diagnose persons with COVID-19 or detect persons with COVID 19 symptoms for isolation [11]. Thermal cameras are also being used to detect people with fever which is also a symptom of COVID-19 [12].

b) Contact Tracing: Advancements in artificial intelligence applications such as speech recognition, data analytics, machine learning and facial recognition have not only been utilized for diagnosis but also for contact tracing [6]. With AI, contact tracing can be easily carried out with data analytics to know the travel history of a COVID-19 patient and those he/she might have encounter [13]. These people will be isolated to prevent them from infecting more people.

c) Treatment: AI technologies are now being used for dosing drugs and different treatment of COVID-19 patients. Also, the time required to develop medicine is reduced since AI can learn and make deductions based on the virus and other medical data. Patients that are being treated can be monitored with AI technologies. In China, robots were used to test and treat COVID-19 patients while healthcare workers stood at safe distance to minimise the risk of infection. A hospital in Wuhan, the epicentre of the outbreak, was being staffed entirely by robots [13], [14]. In the same way, authors in [15] reviewed the potentials of ICT implementation in the Nigerian healthcare system pointing out the promising use of ICT for effective healthcare services and managing the large population in the country. Humanoid robots that can screen people and deliver drugs and food to coronavirus patients have been deployed in some part of Africa like Rwanda thus, reducing exposure of health workers to COVID-19 patients [15].

d) Social Distancing: AI technologies can also be used to enforce social distancing. Singapore announced on May 7, 2020, that the country will henceforth be deploying robot dogs to help people practise social distancing [10]. Social distancing is very important in the fight against COVID-9.

e) Disinfection: Agricultural drones were used to spray disinfectants public spaces in most developed countries [4]. This will go a long way to help since the disinfectant will kill the virus that might be on surface in public. The role of drones in COVID-19 management was highlighted by [4].

f) Transportation of Medical Equipment/Samples: Drones were used in countries like China to transport medical equipment and patient samples [14]. This prevents the contamination of the samples and saves time of delivery.

B. *Virtual/Augmented Reality (VR/AR)*

In Virtual reality (VR), a person is placed in a computer-generated world. In Augmented reality (AR), the real world is augmented by computer generated content. The aim of both concepts is to blur the line between the real world and computer-generated content.

VR/AR can flatten the curve of COVID-19 in the following ways:

a) Treatment: VR/AR technologies aid the treatment of patients with COVID-19 by providing virtual overlays to guide medical practitioners. It can also offer a repetitive cost effective on how to handle COVID-19 patients.

b) Video games: VR/AR can also help people self-isolate in a fun-filled way without getting bored. This can be achieved through video games that use VR/AR technologies like AR air hockey, Titans of space, Jurassic World Alive, Zombies, Run! etc. With these, someone who has met an infected person can self-isolate without any fear of boredom. This will go a long way to flatten the curve of COVID-19.

c) Education: The use of virtual reality has demonstrated being capable of promoting the interest and commitment of student [16]. With AR/VR technologies like the virtual classroom, Construct3D, HP Reveal, etc students can study from home effectively [17]. This will also help to mitigate the spread of COVID-19 because; going to school where they will mingle with students/pupils from different locations can increase the spread of the virus.

d) Social interaction: AR is used to facilitate social interaction. An AR social network framework called Talk2me enables people to disseminate information and view information in an augmented reality way [18]. In Nigeria, applications like zoom and WhatsApp video conferencing are being used the conduct activities like wedding ceremonies, court hearings, meetings etc. With these, people can interact with each other without having to meet physically.

C. Internet of Things (IoT)

Internet of Things (IoT) is a network of interconnected devices containing software, electronics and actuators that interact and exchange data [19]. Simply put, IoT is the concept of connecting any device (like cell phones, lamp, cars, computers, wearable devices, etc) with an on/off switch to the internet and/or to each other [20]. IoT can help flatten the curve of COVID-19 by offering crucial data that will help in the fight against COVID-19.

IoT can help flatten the curve of COVID-19 in the following ways.

a) Telemedicine: This connects patients and healthcare professions through telecom and mobile devices. Telemedicine allows medical appointments to be done physical contact. Telemedicine protects patients and health professionals from possible exposure and, the healthier health professionals can stay, the slower the spread of the virus [4].

b) Home monitoring: Some COVID-19 patients quarantine from home, making room for the patients whose cases are more severe. These home bound patients may be provided medical devices like blood pressure monitoring tools and these devices sends physiological data to healthcare professionals [21]. Some of these devices can also remind patients to take their medications.

c) Vaccine: The raw data collected via medical devices can also hasten the search for a COVID-19 vaccine and, researchers can share what they have learnt with each other [14].

d) Enforcement of Lockdown: The use of IoT has been efficient in enforcing lockdown. The use of devices like the CCTV camera has been helpful in monitoring the boarders to prevent people from travelling between states and countries. For instance, in Nigeria, states like Plateau state installed CCTV cameras at their boarders in order to monitor effectively, those going in and out of the state. This goes a long way to prevent those from affected states from coming into the state and eventually infecting people with the virus.

e) Contact Tracing: The use of QR (Quick Response) codes can be very helpful in contact tracing. South Korea made known her desire to use QR codes to replace the list of names and contact details that people are required to write before entering entertainment locations [22]. This arose as a result of the fact that some people do not give their correct names and contact details. A digital card that contains QR codes will be issued by telecom carriers and these cards will be scanned before entry into public places [23]. With this, those that an infected person had met can be contacted and ask to self-isolate.

III. DATA COLLECTION METHOD

Primary data was used for this research. The primary data was generated from questionnaire which was created using Google forms. The link to the Google form was then shared on various social media to allow for Nigerians to give their perceptions. Data collection was done for a period of one month with no limit to who can give their perception.

IV. RESULT AND DISCUSSION

Results will be discussed in line with research questions and data gotten from questionnaire as follows:

RQ1: Which of the emerging Information and Communication Technologies has been the most effective in flattening the curve of COVID-19?

From figures 1 to 3, the emerging Information and communication technology that has been most effective in flattening the curve of COVID-19 is the Internet of Things. This is followed by virtual/augmented reality then, artificial intelligence. All over the world, IoT has been very helpful in terms of contact tracing, enforcement of lockdown, home monitoring, telemedicine, etc [21], [24].

Also, IoT has been helpful to individuals in this period of pandemic as can be seen in figure 4. Most of the way it has helped individual is in using their mobile phones to access data and information about the corona virus from the internet and sharing this information with each other.

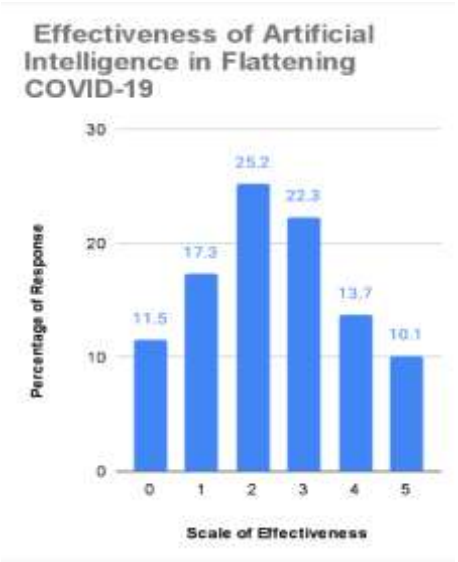


Fig 1: Effectiveness of AI

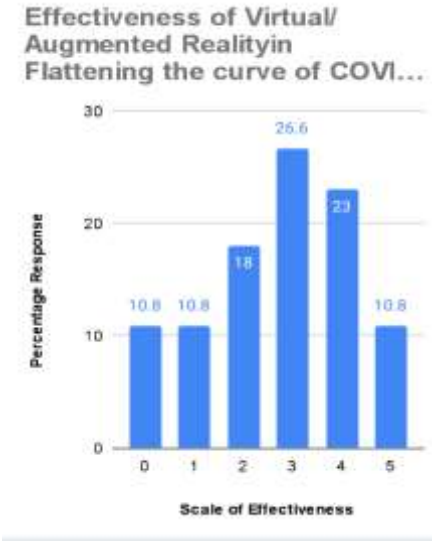


Fig 2: Effectiveness of Virtual/Augmented reality

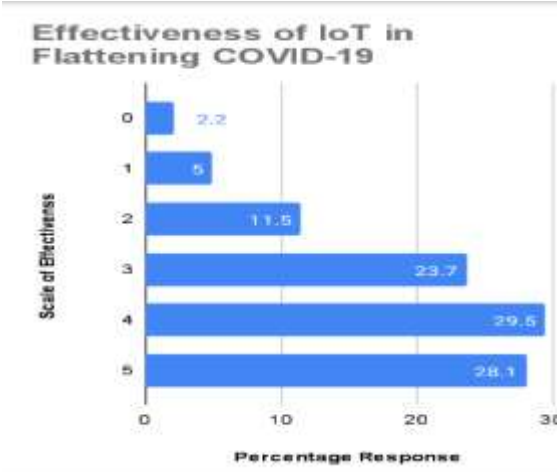


Fig 3: Effectiveness of IoT

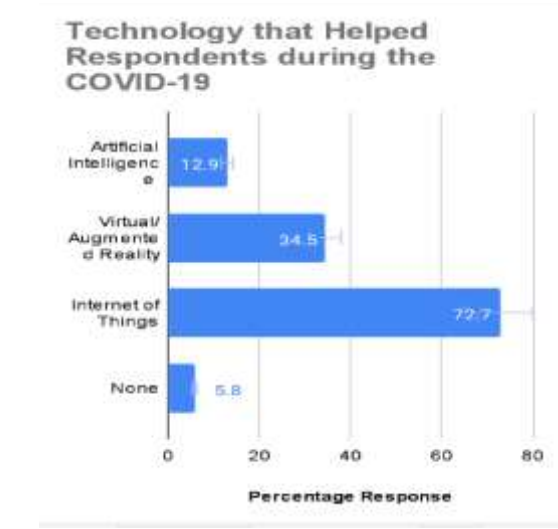


Fig 4: Most used emerging ICT

RQ2: Which of the emerging technologies has the Nigerian government been using in the fight against COVID-19 and, have they been using it effectively?

From figure 5, the Nigerian government has used IoT in her fight against COVID-19 more than it has used other disruptive technologies. For instance, the use of CCTV cameras by the Plateau state government to monitor their borders. CCTV cameras are installed at the land border and monitored on a computer system. Once a vehicle or individuals are seen approaching any of the land borders, security operatives are alerted to question the individuals in order to know whether to allow them into the state or not. Also, the Kogi state government developed an application that allows individuals to know whether they are at a high risk of contacting the coronavirus or not. The application asks the individual if they have any of the coronavirus symptoms, then goes ahead to ask if the person has met an infected person or been to a state or country that has recorded cases of the corona virus. From these, appropriate recommendations will be given.

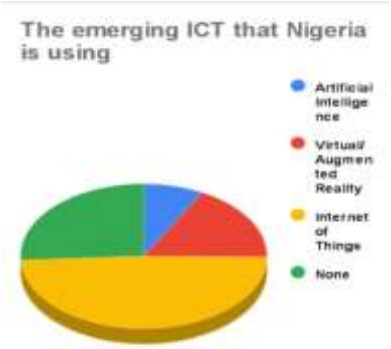


Fig 5: The emerging ICT being used by the Nigerian government

From figure 6, the highest percentage (which is 26.6%) on the rating is on scale 2 and 2 is below average on a scale of 0 to 5. 14.4% of the respondents feel the emerging ICTs are not being used effectively with their rating of zero. Only 2.9% of the respondents feel the emerging ICTs are being utilised effectively. From these the emerging ICTs are not yet fully utilised in Nigeria.

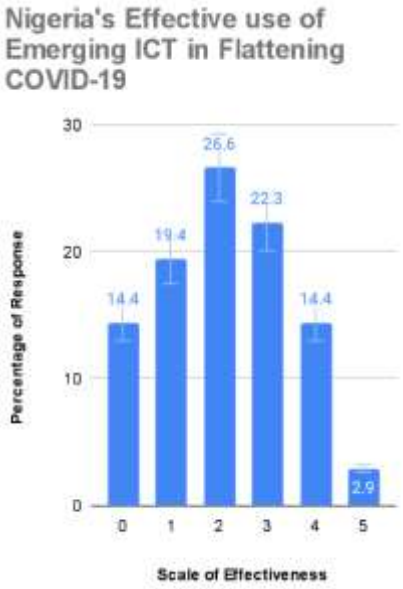


Fig 6: How effective the emerging ICT is being used

RQ3: What are the factors that can hinder the use of the emerging technologies in Nigeria?

There are so many factors that can hinder the use of emerging technologies in Nigeria. Some of them are:

I. Ignorance: most Nigerians are ignorant when it comes to the use of ICT devices. This ignorance is as a result of illiteracy and not being opened to new ideas.
II. Lack of Skills: Nigeria like most developing countries lack skilled individuals in the area if technology and that is why emerging technologies especially the use of AI is being under-utilised.
III. Lack of Stable Power Supply: power supply has always been an issue in Nigeria. And without electricity, most of the emerging ICTs cannot be used effectively.
IV. Internet Access: most rural areas has poor mobile network and because of this, activities like attending a meeting through Zoom, surfing the web for

information, and others are difficult. Also, the cost of data is expensive making it hard to access the internet.

V. Corruption: Corrupt government has also hindered the use of emerging ICTs in Nigeria. Money to be used in purchasing some of the devices for the emerging technologies or for developing the devices might end up being embezzled by some people in government.

RQ4: What are the factors that can aid the use of the emerging technologies in Nigeria?

The following can be helpful in aiding the use of emerging ICTs in Nigeria:

I. Awareness/Enlightenment: Awareness should be created on the benefits of using ICT devices. Those that do not know how to use them should be enlightened on the use [15].

II. Internet Access: Telecommunications companies should try and improve on their mobile network. They should also make the cost of data reasonably cheap so that it can be affordable by all.

III. Power Supply: The government should try and make some improvement in the power sector so that there will be stable power supply.

IV. Training: individuals should be trained on how to develop, use and maintain ICT devices.

RQ5: Beyond the pandemic, which emerging technology will remain in use?

According to figure 7, IoT has 86.3% chance of being used after the pandemic. This is followed by virtual/augmented reality with a percentage of 45.3 and then, AI with 41.7%. One can say IoT has a higher percentage of being used even after the pandemic because so far, most people has used it more than the other emerging ICTs and it has been the most effective in flattening the curve of COVID-19. Even though the percentage of virtual/augmented reality is below average, it also has a chance of remaining in use after the pandemic. This is because Nigerians are beginning to embrace it for activities like weddings, meetings, seminars, talk shows etc.

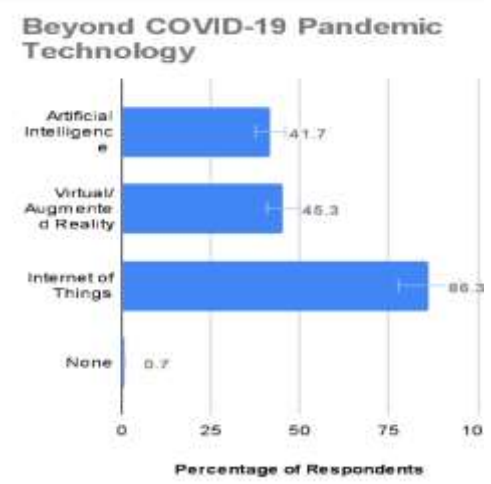


Fig 7: The technology that will continue to be in use beyond the pandemic.

V. CONCLUSION

Even though COVID-19 is a deadly disease that has a very high rate of transmission, its curve can be flattened in so many ways. The use of emerging information and communication technologies has proven to be effective in flattening the curve in countries like South Korea and China. Even in Nigeria, emerging ICTs has also played vital roles in the fight against COVID-19. The most used and most effective of these technology in Nigeria is the IoT. The virtual/augmented reality is also becoming acceptable for social activities and learning in Nigeria with people using Zoom to conduct wedding ceremonies, business meetings seminar and workshops and a host of others. Nigeria, like other developing countries is yet to fully utilize AI in terms of robots and drones making AI the least utilized and considered not effective in the fight against COVID-19 in Nigeria. The emerging ICTs use in this paper are not fully utilized due to some factors some of which are, lack of stable power supply, lack of skilled individuals and ignorance. In this paper, a perception evaluation of how these disruptive technologies have assisted in flattening the curve of COVID-19 was carried out using online perception survey. It was observed that IoT played major role while it is expected that beyond the pandemic, other disruptive technologies such as VR/AR and AI will continue to play roles in public health emergencies and disease control in Nigeria. However, challenges impeding the full adoption of these disruptive technologies can be resolved through creating awareness, training of individuals, improvement in the power supply and improved internet access. It is believed that embracing the use of emerging information and communication technologies, will assist countries worldwide (Nigeria inclusive) in flattening the curve of COVID-19 as the world awaits potent cure and vaccination.

REFERENCES

[1] World Health Organization. (2020, April 17). Q & A on Coronaviruses (COVID-19). Available: https://www.who.int/news-room/q-a-detail/q-a-coronavirus

[2] European Centre for Disease Prevention and Control (ECDC), COVID-19 Situation update worldwide, as of 21 May 2020. Available: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[3] A. Kuzdeuov et al., "A Network-Based Stochastic Epidemic Simulator: Controlling COVID-19 with Region-Specific Policies," in *IEEE Journal of Biomedical and Health Informatics,* doi: 10.1109/JBHI.2020.3005160.

[4] 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," in *IEEE Access,* vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341.

[5] Q. Pham, D. C. Nguyen, T. Huynh-The, W. Hwang and P. N. Pathirana, "Artificial Intelligence (AI) and Big Data for Coronavirus (COVID-19) Pandemic: A Survey on the State-of-the-Arts," in *IEEE Access*, vol. 8, pp. 130820-130839, 2020, doi:10.1109/ACCESS.2020.3009328.

[6] F. Shi *et al*., "Review of Artificial Intelligence Techniques in Imaging Data Acquisition, Segmentation and Diagnosis for COVID-19," in *IEEE Reviews in Biomedical Engineering,* doi: 10.1109/RBME.2020.2987975.

[7] A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi and G. Das, "EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak," in *IEEE Consumer Electronics Magazine*, doi: 10.1109/MCE.2020.2992034.

[8] S. J. Andriole, "Innovation, Emerging Technology, and Digital Transformation," in *IT Professional*, vol. 22, no. 4, pp.69-72, July-Aug.,2020, doi:10.1109/MITP.2020.2985491.

[9] H. Mohanad, “Emerging Technologies: what is it?” *Journal of Technology Management and* Innovation [Online].Vol.8, no3,2013,doi:http://dx.doi/10.4067/S0718-27242013000400010
[10] J. Frankenfield, “Artificial Intelligence (AI)” 2020 Available: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp
[11] O. Samer, “How artificial intelligence is helping fight the COVID 19 pandemic”, 2020, Available: https://www.entrepreneur.com/article/348368
[12] M. E. H. Chowdhury *et al.,* "Can AI help in screening Viral and COVID-19 pneumonia?" in *IEEE Access*, doi: 10.1109/ACCESS.2020.3010287.
[13] J. O. Daramola, “Africa’s health systems should use AI technology in their fight against COVID-19”. 2020, Available: https://www.theconversation.com
[14] A. Chaturvedi, “The China way: use of technology to combat COVID-19”, April, 2020, Available: https://www.geospatialworld.net/article
[15] I. P. Gambo and A. H. Soriyan, "ICT Implementation in the Nigerian Healthcare System," in IT Professional, vol. 19, no. 2, pp. 12-15, March-April 2017, doi: 10.1109/MITP.2017.21.
[16] T. A. garner, “Applications of Virtual Reality”, in: *Echoes of other worlds: sound in virtual reality,* Palgrave Studies in Sound, Palgrave Macmillan, Cham, pp. 299-362, Sept. 2017, doi: 10.1007/978-3-319-65708-0_9
[17] M. O. Edeh, A. Sharma, C. E. Nwafor, A. G. Fyneface, S. Sen and E. C. Edeh “Impact of Emerging Technologies on the Job Performance of Educators in Selected Tertiary Institutions in Nigeria”, in *Journal of Computer Science and its Applications*,Vol.27,no.1,pp. 52-62, June 2020, doi: https://dx.doi.org/10.4314/jcsia.v27il.4
[18] A. Dragni and T. Szymczyk, “Contactless Interfaces in Virtual Reality”, in *Journal of Computer Sciences Institute*, Vol.15, pp. 168-171, 2020, doi: 10.35784/jcsi.2050
[19] P. Pandey and R. Litoriya. “Elderly Care through Unusual Behaviour Detection: A disaster management approach using IOT and Intelligence” [Online]. *IBMJ.RES & DEV*. Vol. 64, no. 1/2, doi: 10.1147/JRD.2019.2947018
[20] M. S. Hossain, C. I. Nwakanma, J. M. Lee and D.S. Kim “Edge Computational Task Offloading Scheme using Reinforcement Learning for IIoT Scenario” in ICT Express (2020), doi: https://doi.org/10.1016/j.icte.2020.06.002
[21] Aeris. (2020, April 29). IoT Helps with COVID-19 Relief: Providing intelligence and speed to flatten the curve. Available: www.aeris.com/news/post/IoT-helps-with-COVID-19 -relief-providing-intelligence-and-speed-to-flatten-the-curve.mht
[22] P. Han-na., “ Korea in critical moment in fight against second wave of infections”. The Korea Herald (online).Available:http://www.koreaherald.com/view.php?ud=2020o514000811 Accessed on May 15, 2020.
[23] N. Ahmed *et al*., "A Survey of COVID-19 Contact Tracing Apps," in *IEEE Access*, doi: 10.1109/ACCESS.2020.3010226.
[24] G. B. Rehm et al., "Leveraging IoTs and Machine Learning for Patient Diagnosis and Ventilation Management in the Intensive Care Unit," in IEEE Pervasive Computing, doi: 10.1109/MPRV.2020.2986767.

Cybercrimes in Southern Nigeria and Survey of IoT Implications

Stephen Ugwuanyi
Department of Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

Agbo Okechukwu
Department of Electrical & Electronic Education
Federal College of Education (Tech.)
Omoku, River State, Nigeria
okechukwu.agbo@fcetomoku.edu.ng

Ohia Prince
Department of Computer Science
Federal College of Education Technical
Omoku, River State, Nigeria
opwservices@yahoo.com

Ndukwe Ogechukwu
Department of Computer Science
University of Port Harcourt
Rivers State, Nigeria
ogeking2004@yahoo.com

James Irvine
Department of Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—This study comprises of a survey on the cybercrime situational awareness in the southern part of Nigeria and the readiness for IoT implications resulting from the challenges of IoT technology adoption for consumer and industrial use cases. We considered cybercrimes in the forms of identity theft, data theft, false alert, dating and romance scam and online shopping scam. The analysis shows among others, 84% of involvement in identity theft and 20% of involvement in data theft with the mode operation being highest through web-based applications. Although cybercriminals are yet to fully utilize the vast potentials of emerging IoT technology and their vulnerability to commit cybercrimes in the region, the rate is on the increase. Also presented is a generic background study on IoT security concerning device capabilities, threat landscape, policy frameworks and applications from which cybercrime trend mitigations and recommendations to reduce the impending dangers of IoT cybercrimes were proposed.**

Keywords—cybercrimes, internet of things (IoT), network, cybersecurity

I. INTRODUCTION

The advent of technology has made the human life easy with its use in almost every human activity ranging from ease of communication, conducting business transactions, health care management, education delivery, environmental monitoring, etc. The heavy reliance on technology has made humans susceptible to various kinds of threats associated with wrongful use of technology like the Internet of Things (IoT) technology. The use of IoT devices is estimated to reach 20 billion in 2020 [1] and 50 billion in 2030 [2]but with new cybersecurity threats. Cybercrime is as a result of the wrongful use of technological devices as evidenced in [2] and [3]. The extent to which these connected devices are used to execute cybercrimes has not been established especially in the developing countries. Cybercrime involves the use of electronic devices to further illegal ends, such as committing financial fraud, child trafficking, promoting pornography materials, intellectual property theft, stealing identities or violating privacy. In[4], cybercrime is seen as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. With reference to the ITU and Budapest Convention on cybercrime definition[5], cybercrime is focused on real-world critical information technology facilities. In the real-life scenarios, laws and regulations in additions to the insurance and legal implications outlined in [6] are however needed to reduce the cyber-security level resulting from the heavy reliance on modern IoT technology devices. Intrusion and threat detection systems are increasing sort after to protect IoT user' data and privacy breaches [7].

According to a report by the Nigerian National Information Technology Development Agency (NITDA), there are over 97 million internet users in Nigeria in 2017. This figure surpassed 100 million users in 2019. This is possible due to the increase in the use of smartphones in Nigeria and the availability of internet facilities, hence, the high reliance on computers and the internet for the everyday activity such as messaging, business transaction, banking operations and other business activities. The use of the internet has brought about various forms of crime known as cybercrime and cybercriminals in Nigeria are mostly regarded as *"Yahoo Boys"*. This involves Automatic Teller Machine (ATM)frauds, phishing, identity theft etc. According to a report by NITDA in 2017, about 14% of the total internet users in Nigeria have experienced cybercrime of different scale and magnitude. It was proven that 39.6% African users of the internet are Nigerian, hence, the high increase in the rate of internet crime in Nigeria[3]. In Nigeria, people of all ages involve on different kinds of cybercrimes because of the high rate of unemployment in the country which is currently 23.1% in 2019 according to the National Bureau of Statistics[8].

According to an analysis carried out by KPMG forensic service in Nigeria, there is an increase in cyber-related offences between 2013 and 2015 as a result of the adoption of various forms of technology [9] with targets of financial gains. This study involves a survey carried out through an online questionnaire, administered to1700 active computer users in 17 southern states of Nigeria to determine the levels of involvement of the respondents on the various type of cybercrime such as identitytheft, malicious spamming, data theft, false alert, and online shopping scams with discussions on IoT implications on cybercrime, aiming at determining its level of involvement in cybercrime. The survey also

examines the mode of operations through which these crimes are committed.

II. Related Literature

Today, tasks and events globally are connected through information systems and communication networks, enabling among others, critical activities such as financial transactions, shopping, education and even research[11].However, as the knowledge in these areas deepens, criminal activities become imminent as against its original operational principles[12]. Transmitting these criminal activities using information and communication technology devices has consistently been on the rise and has resulted in the hike of the cost of maintaining the global communication infrastructure [11]. Some of the techniques implemented by researchers to tackle these menaces need constant update due to the dynamic nature of cyber-attacks. Cybercrime comes in different forms and is generally difficult to categorize [10]. Some of the solutions include;[13] the use of encryption techniques and development of Radio Frequency Identifier (RFID) to provide authentication and integrity for the communication between RFID tags.

In [11], a design thinking approach to cybersecurity awareness among youth was conducted in Malaysia with IoT, cyber-attack, password, privacy and safer society identified as the key terms in cybersecurity investigations. The findings, however, showed that IoT devices aided cyber-attacks, but the experiences varied across organizations. As new consumer IoT devices continue to emerge, some are left unsupervised and referred to as "*Cyber Debris"* in [12]. The inability to properly manage the devices also constitutes a cyber vulnerability. Practical testing of IoT solution is the optimal approach to identifying vulnerability surfaces as seen in the Wi-Fi experimentation in a city in Denmark [13]. A global approach to tackling cybercrime has been proposed since it does not respect national boundary [14]. The study profiled the developing countries to be more vulnerable and recommended global strategic collaborative effort for sustainable cyberspace.

To understand the concept of cybersecurity in the Nigerian context and its impact on the national development, we made the following observations; that the evidence exists on the direct effect of cybercrime on foreign investment and national development. It also creates trust issues and damages national credibility[15].Data security and digital privacy protection are identified as a key driver in the NCC 2020 -2024 strategic plan with regulatory frameworks intended outcome of reducing the incidence of cybersecurity and data breaches [16].

III. Methodology

A survey design was adopted for the study. The researchers considered this design appropriate for this study since it intended to collect data from the population of people who operate online/internet-based transactions in the southernregion in Nigeria. One thousand (1700) people who do online transactions were randomly selected from the six (6) states of the south-south region of Nigeria consisting of one hundred (100) respondents. The instrument for data collection was a structured questionnaire titled "*Survey of Internet of Things(IoT) Implication on Cybercrime*(SIOTIC)''. Qualtrics statistical tool was used to administer the survey and the results analyzed using classic report feature. The research focused on addressing three key research questions: What are the types of IoT cybercrimes?;How frequently are the different IoT cybercrime committed?;and How are such cybercrimes evolving with time among different groups?. We adopted this research method because it provides a detailed opinion about IoT and its security implications.

Figure 1. Societal and Technological IoT Solution Model[17]

The framework above depicts the required multi-facets fights against cybercrime which is expected in our society. With the emergence of technologies such as IoT into basic activities of man, it becomes paramount that technology may have to interface with law, ethics and attitude awareness to check online security.

IV. Government Policies on Cybercrime

On the 15th May 2015, the Nigerian Government enacted the cybercrime bill into law, summarized in [15], which allows for Prohibition, Prevention, Detection, Prosecution and Punishment (PPDPP) of Cyber related offences in Nigeria. The 2015 cybercrime act is the first of such in Nigeria that deals with cybersecurity. One of the objectives of the 2015 cybercrime act is to promote cybersecurity and protect computer systems and network electronic communications, data and computer programs, intellectual property and privacy rights.

The 2015 Nigeria cybercrime act prescribes a jail term of up to 5 years and a fine of up to 10 million Naira for internet fraudsters that perpetuate their act by sending electronic mails with the purpose of defrauding an individual, government or organization[18].It also identifies identity theft and gives a punishment of 7 million or a 3-year jail term or both. Identity theft is when a fraudster pretends to be someone else on the internet for financial gain or to cause other damages.

The Nigerian Economic and Financial Crimes Commission(EFCC) was enacted in 2002 and started full operation in 2003 with the sole aim to investigate and prosecute all financial criminal cases which includes cybercrime. The following are some of the internet related offences and crimes in Nigeria.

A. Credit Card or ATM Fraud

This is the process of stealing credit/debit card information by hackers when the user enters credit/debit card information when performing an online transaction on a

webpage. Another form of the electronic card fraud is the fake and unauthorized messages sent by Fraudsters requesting for an update of the Bank Verification Number (BVN). In such cases, personal information and debit card information are collected from the victims and in some cases phishing sites are sent to the victims. According to a report by the Central Bank of Nigeria (CBN), commercial banks in Nigeria have lost about 199billion Naira to e-fraud alone between 2000 and 2014.

B. Advance Fee Fraud

In Nigeria, fraudulent activities are popular with the use of technology and the internet. The proliferation of scams associated with IoT in Nigeria may be difficult to compare to other countries. In Nigeria, cybercrime involves the use of spam to unleash various dubious gimmick propositions like sending an e-mail to various people asking them to transfer a sum of money to an account for non-existing products and services. In another dimension, cybercrime victims are promised a percentage of a huge sum of money for third-party activities. After the money has been transferred, they never hear from the person again. The Advance Fee Fraud and other Related Offences Act, Criminal Code Act, The Financial Crimes Commission Act and Money Laundering Prohibition Act of 2016 are the regulatory frameworks available to combat fraudulent activities known as "419" in Nigeria[41]. Given the available frameworks, the prevalence of internet scams in Nigeria is however due to lack of enforcement.

C. Phishing Attacks

A phishing attack involves cloning of a webpage such as social media pages, e-commerce store and bank websites to collect sensitive personal information such as smart card information, username and password etc. Due to the increase in the use of mobile phones and banking application in Nigeria e-fraudsters deploy many fake applications which are used to fetch and extract user's personal information. Palo Alto networks indicated that Nigerian phishers used a trojan-spy called Key base to lodge an attack with the major industrial companies as targets. According to an estimate by the Federal Bureau of Investigation (FBI), the damages done by Nigerians through phishing activities from 2013 to 2016 exceeds US$3 billion with an estimate of 22,143 companies across 79 countries[19].

D. Online Sale Fraud

This is a type of cybercrime that involves the sale of products that do not exist. The problem with online shopping is that users sometimes cannot differentiate between a genuine e-commerce site and fake websites. The various forms of social media scams include; the beneficiary of a will scam, charity funds, cyber-stalking, blackmailing scam, and social hijacking[20]. An account number is displayed sometimes on the advertisement and users are asked to pay for the product to be delivered. This scam is possible because people are asked to make full or part payment before the item is delivered.

V. IoT and SecurityEvolution

The internet has evolved from interlinked hypertext into a network of people, applications and devices. The total number of devices currently connected to the internet has increased from millions to billions with an estimate of six billion devices connected to the internet[21]. As a result of too many devices connected to the internet, there is a need for adequate security in every section of the communication infrastructure. The IoT application evolved to the internet of people, regarded as social networking. The internet of people gave birth to the IoT[21].IoT is a network of connected devices through the internet which receives and sends data. The internet connects servers; the IoT network connects devices which are made smart by sensors - from thermostats, light bulbs, fridges to container ships and beyond. As seen in figure 1[22], the security evolution of IoT has been linear

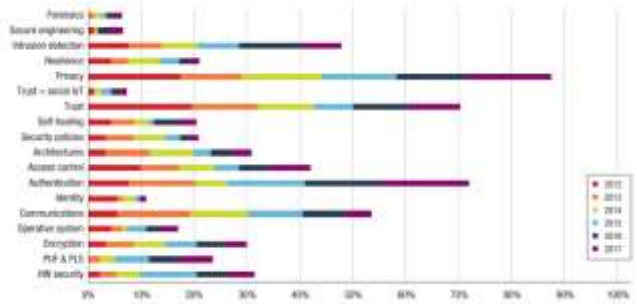


Figure 2. Security evolution of IoT

over since 2012. Trust, identity and social sides of IoT security remain relatively lower than other bold security approaches.

VI. Applications of IoT Technologies

The Internet of Things has various applications ranging from, home automation, smart banking, education and training services, advancing manufacturing, transportation and agriculture to e-government. They all present a different set of challenges, some of which are presented in [23].Data security and privacy remain critical requirements as discussed in the following IoT use cases:

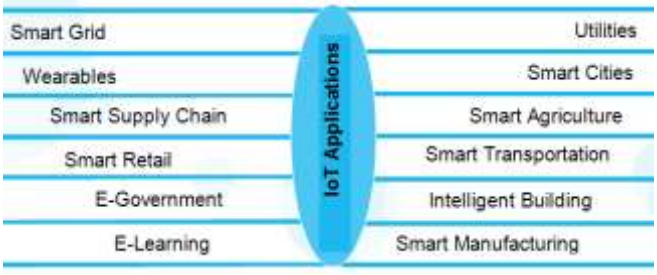


Figure 3. IoT Applications and Use cases

A. Home Automation/Intelligent Building

IoT devices are used to build a smart home which comprises of a smart lighting system, security, heating and air-conditioning system controlled by an application. An example of such application is the Amazon Echo and Google home smart speakers, which are mostly based on Wireless Sensor Networks [24]. Their use, however, is accompanied by huge privacy and security vulnerabilities. According to [25], the hardware, software and the network analysis of

home and industrial IoT solutions revealed that they are prone to different attacks types as a result of IoT adoption. Solutions such as multipath and split channel Onion IoT gateway proposed in [26]are used to filter connections at the gateway level. The choice of cybersecurity solutions like multiple authentication and encryption system lies in a compromise between cost and performance due to factors such as increased data overhead.

B. Smart Banking

IoT technology is also transforming how banking and financial services are conducted. IoT devices and applications are increasingly used to facilitate banking activities. In [27], the general view of adopting IoT in the banking sector focuses on transforming the IoT data into profitable financial gains. The data is acquired through IoT banking devices and analyzed through integrated analytics platforms. The customer data can be used to offer solutions and advice that can help the customer in making a secure and sound financial decision[28]. The layers of IoT framework must have unique security features. The data generation layer ranges from smartphone to token generators for initiating and validating banking transactions. The connectivity level ensures that the data gets to the banking server. Using public or private connectivity technology presents different cyber risks. The security of the data processing and the user interface layer depends on the tools and technologies established by the bank IT employees. The banking infrastructure, management, third-party service providers, employees and customers are different cyber-levels that also require adequate security mechanisms.

C. Transportation

The application of IoT in the transportation sector is driving services such assmart traffic control, smart parking, fleet management, vehicle control, etc. Some of the benefits are improved revenue, public safety, service on demand, and resource optimization like fuel consumption feedback and traffic route recommendation. With these new efficient and economic offerings, safety, security and privacy are the cybersecurity challenges associated with such smart city solution[29]. For instance, a smart packing system when compromised becomes underutilized and leads to economic wastages. Similarly, when a critical traffic control or fleets monitoring systems are compromised, the result is catastrophic and must be detected and mitigated using the alert scheme as proposed in [30].

D. Health Care

Smart health care is an application of IoT in the health care management system. It involves data collection and analysis for research and treatment purposes. IoT technology connects patients, medical professionals and healthcare resources intelligently. The condition of patients with medical devices such as heart rate monitors can be remotely diagnosed accurately and timely. With these capabilities, the pressure on the medical facilities use can be reduced through early diagnosis and detection of illnesses. We recommend the widespread use of this technology, especially in developing countries if the data security and privacy challenges of adopting IoT in the healthcare sector as recommended in [31]are addressed.

VII. Implications of IoT on Cybercrimes

IoT is the perfect recipe for cybercrime as it presents an opportunity for cybercrimes to be committed and the implications of its use have been understated. IoT as new and emerging technology requires stakeholders to pay more attention to security issues to drive market competitiveness. This has not been the norm and as a result, IoT devices are manufactured with security vulnerabilities, paving way for cybercrimes to be committed as new devices are introduced [32].As highlighted by Amy Webb of Future Today Institute that "Technology can be like junk food. We will consume it, even when we know it's bad for us" [33].The implications of the use of IoT devices is the vulnerability of data and privacy. IoT devices pose a high level of vulnerabilities, whichare present in IoT devices due to:

A. Poor Authentication

IoT manufacturers play a critical role in establishing the security features of IoT devices and their focus should include both ease of use and security. A return on the investment trade-off makes most IoT devices lack the proper authentication and other security features. Some IoT devices use the default security credential which is the same for similar or the same products. This makes it easy for an attacker to gain access to such a device. As IoT scales, lightweight authentication techniques using private and public keying infrastructure are needed to resolve these issues[34].

B. Unencrypted Messages Between IoT Devices

When the messages exchanged between two IoT devices are obscured from cybercriminals, confidentiality is guaranteed. The confidentiality of a network can be evaluated using either plaintext, encoded, or encrypted data types exchanged between devices or devices and servers[32]. Due to the ease of use of many IoT devices, the communication between these devices appears to be unencrypted, making it possible for a man-in-the-middle, side-channel and other data-driven attacks to take place. When a request is routed over the internet, it passes through various networked devices which are manned by different people and organizations. When these devices transmit the data as plain text (unencrypted) then it is possible for software on any of the devices to read such data [35].The threats also come from known operational inefficiencies like the inability to restrict access from a non-secure network, data mobility which leaves sensitive information in the attacker's domain, etc. In [36], a wireless radio network was vulnerable to a DDoS attack due to unencrypted data at the radio link level. Encrypted data does not mean absolute security. For instance, encrypted data tags available to an attacker can be used to obtain other information such as the number of people in a building [37].

C. Lack of Authentication

Enough validation of software, hardware and log activities ensures the authenticity and confidentiality of a network. Strong authentication pairs ensure secure access to the IoT network and prevent attacks like Distributed Denial of Service (DDoS) and replay attacks. If network access control and updates are not properly authenticated to know if the data is from a trusted source, then malicious programs can be installed in the guise of a genuine update. Usually, the firmware update will equip IoT devices with an upgrade

which will enable them to perform improved operational instructions without a corresponding upgrade in the hardware. The updated firmware will be able to bring new experiences in various functions of the devices such as security. IoT devices can take care of some of its security challenges if authentications of update of firmware are periodically made to ensure new security features in place [35]. This is common in edge computing level and in a training machine learning algorithm, where fake dataset or nodes are introduced early to deviate the system from learning valid model [37].

Future research in authentication should be focused on Android devices because wearable is on the increase. The combination of intrusion detection and authentication scheme; group authentication and key agreement; and electrocardiogram-based authentication with privacy preservation are the future research direction recommended for smart mobile devices in [38].

VIII. Security Threats and Attacks in IoT Network

The security of IoT network is vulnerable to various attacks, this is since most IoT devices are installed in public places e.g. IP camera can be subject to cloning, replacement and other physical attacks. Most of these attacks can be categorized based on the structure of the IoT. The attacks and threat to IoT can be divided into four[39].

A. Physical Layer Attack

This is the most important part of the IoT network that must be protected from all forms of attacks. IoT devices are mostly made of various remotely interconnected nodes. In the physical layer attack, when the attacker exploits a vulnerable node to extract security information, the result is catastrophic and can lead to a total failure of the network. All forms of physical security are associated with IoT users. An overload attack is a type of physical layer attack on an IoT. This attack is used to decrease the strength of an IoT network. One of the ways to provide a solution to the attacks at this layer is by fixing strong physical layer security. Physical Unclonable Function (PUF) is physical layer security that provides IoT devices with fingerprint identification[22].

B. Perceptual Layer Attack

A perception layer is an attack on the various nodes responsible for the collection of data from the external world. These nodes are sensors and example are RFID and wireless sensor network. These attacks are possible since little or no security exists on the sensors hereby, they are prone to attacks. The solution to this kind of attack is to provide a means of authentication for each node or to allow for a node to node authentication, which is possible only if nodes becomes powerful to support parallel processing.

C. Network Layer Attack

The main security threat in the network layer consists of routing attacks such as malicious behaviour against right path topology and forwarding data, Distributed Denial of Service (DDoS) attacks, cyber-attacks across a heterogeneous network, asynchronous attacks, collusion attacks and the man-in-the-middle attacks[39]. Another type of attack is when a malicious node tries to drain network resources. Other attacks include node impersonation attack and it happens when a malicious node tries to gain access to a network in the guise of a genuine node. Spoofing attack; this type of attack occurs when an attacker tries to gain access to a device by pretending to be someone else. Replay Attacks; the attacker captures network data and replays it on the network to slow down the network operation. These types of attacks can be stopped by restricting traffic on each network node.

D. Support Layer Attack

The attacks on this layer include Denial of Service (DOS) attack, sessionattack and Denial of Access (DOA) attacks. The support layer attacks can be stopped by using security tools to detect malicious codes, such security tool can be an antivirus.The support layer performs two major roles;To confirm that information is sent by an authenticated user and protected from threats andto send information to the network layer through wireless or wired technology [29]. The verification of the user and the information can be done in various ways, likethe method of authentication which is implemented by using secret keys and passwords.

E. Application Layer Attack

The application layer is responsible for handling user data, management processes, control, visualization, etc. An attack on the application layer targets the user confidential information by compromising specific web service applications. Cybercriminals use complex DDoS like HTTP floods, and brute force attack to steal, destroy or modify the user data. The major concern for application-level security is the issue of data sharing. Other factors include passwords and key agreement. The attacker is likely to destroy privacy in the application layer by a known vulnerability.

IX. Cybercrimes Trends in IoT

IoT development comes with different sensing and control capabilities applicable to industrial and consumer solutions. It has been estimated by Cisco that IoT connection will reach 50 billion in 2020. This is a serious concern due to the security and vulnerability issues in IoT as most businesses and organization are relying heavily on smart devices. Any approach to IoT security must include availability, integrity and confidentiality if the following cybercrimes are to be mitigated.

A. Fraud

Due to the lack of control of infrastructure in most IoT devices, low-level infrastructure can be used to cause serious damage. An example is the first fraud of IoT that happened when a network of ATM used by the banks was attacked by fraudsters through the use of web-based control. And in most cases, it takes just one compromised node for fraudsters to gain access into an entire system. According to a report by Forrester, hackers are now targeting IoT devices for financial gain, it is no longer for social or political reason. This is because of any sensitive business data which is held by most IoT devices, for example, a smartwatch and phone can contain some user sensitive data such as; name, address, health information and debit/credit card information.

B. Data Theft

Between 2017 and 2018[40], a trojan VPN filter and other malware types were found to be used in extracting sensitive information such as username and password and extracting other important data from IoT users. With the adoption of IoT devices by the public, the issue of privacy of data is a thing of concern. Most IoT such as smartwatch and entertainment smart devices store user data and such data

give detailed information about an individual.Cybercriminals upon obtaining these data, use them to usurp the personality of the original data owners. Sometimes, the data is stolen and sold or directly used to enable them to act or operate in the capacity of the victims.

C. Malicious Spamming

IoT devices are now used by hackers as tools to cause attacks. An example was the use of over 100,000 devices which includes smart devices, routers and other devices that were manipulated by hackers into sending out more than 750,000 malicious emails.In a case where those smart devices are infected with a trojan, they will continue sending malicious messages except they are taken offline in some cases a security update from the manufacturer can stop the trojan.

D. Identity Theft

With IoT devices, cyber-criminals can gain access to personal information of victims such as bank account details, credit and debit card information through theft and tampering and are used for both cash and internet transaction in the victim's name. This is because IoT devices make current data readily available and store historical user data [7]. Due to the security vulnerability of IoT devices, hackers can easily access such information in the form of hijacking.

X. Results and Analysis of the Survey

Based on the responses, the analysis of the results in **Error! Reference source not found.** reveals among others an 84% high involvement in identity theft and 20% lower in data theft in southern Nigeria. Figure 4 shows the different percentages of involvements in various cybercrime identifies in southern Nigeria. The survey results provide an overview of cybercrime in southern Nigeria and how frequently specific IoT devices have been used to commit cybercrimes. The implication of these findings is to enable faster design

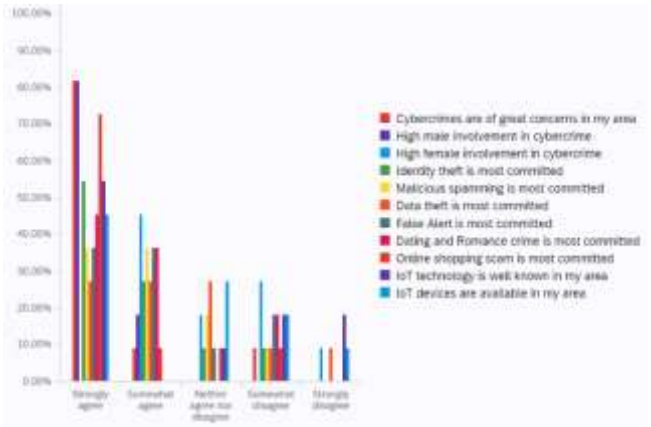


Figure 4. Percentages of involvements in cybercrime

and adoption of the best security architecture that will ensure confidentiality, integrity and availability of IoT services. It will also serve as the guide for creating a cybercrime awareness campaign and making necessary recommendations for IoT use and regulations.The data generated during the study was used in determining the percentage of modes of operation of cyber-related crimes in Southern Nigeria as shown in Table 1.

The types of cybercrime spread across the different modes of IoT operation. Web-based applications are the most common means of cybercrimesin southern Nigeria with 1.6% higher than social networking. While others like text messagingand mobile applications were lower, they are still as important as other aspects of IoT ecosystemnot captured in this study.

Table 1. Percentage of Mode of Operations

Mode of Operation	Percentage of Operations
Web-based Application	34.6%
Social Networking	33%
Text Messages	7.3%
Mobile Application	10%
E-mail	15.1%

XI. Future Directions

The IoT technology is a promising area of research which has been widely embraced across many fields. With the actual deployment figures very close to most of the growth forecasts, the security and privacy requirements and cybercrimes related to the use of this technology cannot be over emphasized. The emergence of this technology in virtually every area of human endeavours makes its security consciousness of interest to any concerned researcher and indeed the teaming users. The advances in IoT research in the future will take on the security direction. From the standardization of IoT product security approach down to the cybercrimes; the focus of this paper. The researchers project IoT to be enabling intelligent decision making if security is addressed at every layer of the architecture, including their role in the realms of cybercrimes.

XII. Conclusion/Recommendation

This study has revealed an increasing interest in IoT to advancing global interconnectedness. While IoT technology is available for consumer and industrial use for convenience and innovations, it has also become a tool for data breaches and a myriad of other cybercrimes. We reviewed IoT related service users in the southern part of Nigeria to gain an insight into how IoT devices are used to commit cybercrime. The focus was to understand the users' perception as it relates to cybercrimes in different locations. Although, the findings show that cybercriminals have not fully utilized the potentials of IoT devices and their vulnerabilities to attack and cause harm of great magnitude in this region. However, there are indications that IoT technology might be sought after by the hackers and cybercriminals in Nigeria.The following are put forward as recommendations from this study:

- Criminalize the Act of cybercrime: Although in Nigeria, all forms of internet-related offences are punishable according to the cybercrime Act of 2015. Cyber laws should be made available to the public and enforcement implemented.
- The co-operation of international communities: In the fight against cybercrimes, especially in southern Nigeria, the international community has an important role to play especially for crimes that require the extradition of criminals. This is because most cybercrimes have an international dimension. From the technology point of view, we recommend a global

approach to regulations and standardization since technology violates national boundaries.

- Research development / Specialized Training: Grants should be made available by the Federal Government of Nigeria specifically for interested researchers to embark on technological based research to curb the menace of cybercrimes and develop trust to resolve the present privacy issues
- Other recommendations: Education and sensitization of internet users in Nigeria on the danger of cybercrimes should be taken seriously, delegating more duties to Internet Service Providers (ISPs) such as the authority to report observed malicious communication, the introduction of cybersecurity module into Nigerian education curricula, and the setting up of a special anti-graft agency especially for cybercrime should be considered and quickly implemented.

ACKNOWLEDGMENT

The authors would like to appreciate those who responded to the study questionnaire and the Nigerian Petroleum Technology Development Fund (PTDF) for funding this research under the award number PTDF/ED/PHD/USO/1092/17.

REFERENCES

[1] N. Gershenfeld, R. Krikorian, and D. Cohen, "The Internet of things", Scientific America, vol. 291, no. 4, pp. 76-81, 2004.

[2] S. Furnell, "Technology Use, Abuse, and Public Perceptions of Cybercrime," in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Springer International Publishing, 2020, pp. 45–66.

[3] A. Bijik Hassan, F. David Lass, and J. Makinde, "ARPN Journal of Science and Technology::Cybercrime in Nigeria: Causes, Effects and the Way Out," *ARPN J. Sci. Technol.*, vol. 2, no. 7, 2012.

[4] O. Olusegun, "Impact of Immigration on Nigerian Economy," SSRN Electronic Journal, October, 2015.

[5] B. Akhgar et al., "Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism," in Advanced Sciences and Technologies for Security Applications, Springer, 2016, pp. 295–321.

[6] A. Tăbușcă, S.-M. Tăbușcă, and G. Garais, "IoT and EU Law – E-Human Security," Valahian Journal of Economic Stududies, vol. 9, no. 23, pp. 25–32, Mar. 2019.

[7] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," in Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020, 2020, pp. 22–29.

[8] Chris Ngige, "Nigeria's unemployment rate hits 33.5 per cent by 2020 – Minister | Premium Times Nigeria," May-2019. [Online], Available:https://www.premiumtimesng.com/news/top-news/328137-nigerias-unemployment-rate-hits-33-5-per-cent-by-2020-minister.html. [Accessed: 29-Jul-2020].

[9] KPMG, "Building Cyber Security & Resilience in a Digital Africa,"May, 2017. [Online], Available: https://home.kpmg/content/dam/kpmg/zm/pdf/2017/07/Building%20Cyber%20Security%20&%20Resilience%20in%20a%20Digital%20Africa-%20FINAL.pdf.[Accessed: 20-Jul-2020]

[10] R. Broadhurst, "Cybercrime in Australia," in The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice, Springer International Publishing, 2017, pp. 221–235.

[11] M. Dorasamy, G. C. Joanis, L. W. Jiun, M. Jambulingam, R. Samsudin, and N. J. Cheng, "Cybersecurity issues among working youths in an iot environment: A design thinking process for solution," in International Conference on Research and Innovation in Information Systems, ICRIIS, 2019, vol. December-2019.

[12] I. Mizukoshi and A. Nakanishi, "Subscription; Remedy for Cyber Debris!?,"*2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM),* Matsuyama, Japan, 2019, pp. 1-6, doi: 10.1109/SITIM.2019.8910190.

[13] L. S. Vestergaard, N. Kasenburg, and M. S. Jorgensen, "Implications of conducting internet of things experimentation in Urban environments," in Global IoT Summit, GIoTS 2019 - Proceedings, 2019.

[14] A. Tabassum, M. S. Mustafa, and S. A. Al Maadeed, "The need for a global response against cybercrime: Qatar as a case study," in 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, 2018, vol. 2018-January, pp. 1–6.

[15] The Communicator, "A Summary Of The Legislation On Cybercrime in Nigeria," Dec-2018. [Online]. Available: https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria&catid=23&Itemid=179. [Accessed: 25-Jul-2020].

[16] NCC, "NCC Strategic Management Plan ASPIRE 2024," 2020. [Online]. Available: https://ncc.gov.ng/accessible/documents/886-ncc-2020-2024-strategic-management-plan-aspire-2024/file. [Accessed: 25-Jul-2020].

[17] M. M. Ali, "Determinants of preventing cyber crime: a survey research," *Int. J. Manag. Sci.*, vol. 2, no. 7, pp. 16–24, 2016.

[18] ICT Policy Africa,"The Nigeria CyberCrimes (Prohibition, Prevention, etc) Act, 2015,". [Online], Available: https://ictpolicyafrica.org/en/document/h52z5b28pjr. [Accessed: 24-Jan-2020].

[19] D. Gudkova, M. Vergelis, N. Demidova, and T. Shcherbakova, "Span and phishing in Q2 2016." Kaspersky Lab, August 2016.

[20] A. Esan, B. A. Omodunbi, P. O. Odiase, O. M. Olaniyan, and A. O. Esan, "Cybercrimes in Nigeria: Analysis, Detection and Prevention.," FUOYE Journal of Engineering and Technology, vol. 1, no. 1, 2016.

[21] Infosys, "Live enterprise." Annual report, 2018-19. [Online]. Available:https://www.infosys.com/investors/reports-filings/annual-report/annual/Documents/infosys-AR-19.pdf. [Accessed: 24-Jan-2020].

[22] R. Roman-Castro, J. Lopez, and S. Gritzalis, "Evolution and Trends in IoT Security," Computer (Long. Beach. Calif)., vol. 51, no. 7, pp. 16–25, Jul. 2018.

[23] S. Thiruchadai Pandeeswari, S. Padmavathi, and N. Hemamalini, "Engineering Full Stack IoT Systems with Distributed Processing Architecture—Software Engineering Challenges, Architectures and Tools," Intelligent Systems Reference Library, vol. 185, Springer, Cham, 2020, pp. 71–87.

[24] C. S. Abella et al., "Autonomous Energy-Efficient Wireless Sensor Network Platform for Home/Office Automation," IEEE Sensor Journal, vol. 19, no. 9, pp. 3501–3512, May 2019.

[25] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," 2016 21st Asia South Pacific Des. Autom. Conf., pp. 519–524, 2016.

[26] L. Yang, C. Seasholtz, B. Luo, and F. Li, "Hide your hackable smart home from remote attacks: The multipath onion IoT gateways," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 11098 LNCS, pp. 575–594.

[27] R. S. Lande, S. A. Meshram, and P. P. Deshmukh, "Smart banking using IoT," Proceedings of the 2018 3rd IEEE International Conference on Research in Intelligent and Computing in Engineering, RICE, pp 1-4, January 2018.

[28] V. Dineshreddy and G. R. Gangadharan, "Towards an Internet of Things framework for financial services sector," in 2016 3rd International Conference on Recent Advances in Information Technology, RAIT 2016, 2016, pp. 177–181.

[29] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," Journal of Advanced research, vol. 5, no. 4, pp. 491–497, 2014.

[30] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," IEEE Internet Things J., vol. 5, no. 2, pp. 716–723, Apr. 2018.

[31] F. Nasri and A. Mtibaa, "Smart Mobile Healthcare System based on WBSN and 5G," International Journal of Advanced Computing Science and Applications, vol. 8, no. 10, 2017.

[32] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," 2017.

[33] Alisdair Faulkner, "Evolution of fraud in the IoT era ," 22-Aug-2018.[Online],Available:https://www.techradar.com/sg/news/evo

lution-of-fraud-in-the-iot-era. [Accessed: 25-Jul-2020].
[34] K. Gupta and S. Shukla, “Internet of Things: Security Challenges for Next Generation Networks,” 1st International Conferenceon Innovation and Challenges in Cyber Security, ICICCS-INBUSH, pp. 315–318, 2016.
[35] G. Nebbione and M. C. Calzarossa, “Security of IoT Application Layer Protocols: Challenges and Findings,” *Futur. Internet*, vol. 12, no. 3, p. 55, Mar. 2020.
[36] D. Pishva, “Internet of Things: Security and privacy issues and possible solution,” *2017 19th Int. Conf. Adv. Commun. Technol.*, vol. 5, no. 2, pp. 797–808, 2017.
[37] A. Mohsen Nia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 1–1, 2016.
[38] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, “Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues,” *Telecommunication Systems*, vol. 73, no. 2. Springer, pp. 317–348, 01-Feb-2020.
[39] 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 Journal, vol. 4, no. 5, pp. 1125–1142, 2017.
[40] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of Threats to the Internet of Things,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, Apr. 2019.
[41] T. Oriola, "Advance fee fraud on the Internet: Nigeria's regulatory response," Computer Law & Security Review, vol. 21, no. 3, pp.237-248, 2005.

Impact of COVID-19 Contagion on Digital Transformation and Economy

James Kunle Olorundare
Next Generation Technologies and Standardisation Unit
Nigerian Communications Commission
Abuja, Nigeria
olorundarek@ncc.gov.ng

Aderonke F. Thompson
Cybersecurity Department
The Federal University of Technology
Akure, Nigeria
afthompson@futa.edu.ng

Oluwafemi E. Ekanoye
Office and Government Contracts
Southern University and A&M College
Louisiana, USA
femiekanoye125@gmail.com

Christian N. Ahiauzu
Information and Communication Technology Center
University of Port Harcourt
Port Harcourt, Nigeria
christian.ahiauzu@gmail.com

Adebimpe Olubunmi Olorundare
Information Technology Department
National Open University of Nigeria
Abuja, Nigeria
bolorundare@gmail.com

Adebunmi Akinbo
Internet Society Nigeria Chapter
adebunmi.akinbo@gmail.com

Abiodun Ayorinde
Blockchain Research department
Blockchain Republic
Lagos, Nigeria
abiodun@blockchainrepublic.xyz

Abstract*—The novel COVID-19compelled an unannounced and indefinite holiday in the world with a ripple effect of the global economy downturn. As a result, businesses all over the world have been forced to devise business strategies with minimal negative impact from COVID-19. Since there is no timeline as to when the COVID-19 will end, this paper seeks to empirically examine the COVID-19 impact on the traditional economy vis-a-vis digital transformation paradigm shift in the economy ecosystem leveraging on digital channels. To this end, two surveys were conducted to ascertain COVID-19 effect on the traditional economy as well as the paradigm shift to digital transformation. The first was the qualitative survey which was analyzed based on Key Research Questions which were transcribed and analyzed from focus group discussion. The second survey establishes the fact got from the quantitative survey from SurveyMonkey platform. The ggplot2 package in RStudio platform was used for the data visualization using R programming Language enabling the data analysis for a technical evaluation

***Keywords*—**Digital Transformation (DX), telecommuting, E-Commerce services, Virtual events, Internet of Things (IoT), COVID-19, International Telecommunications Union(ITU), 4IR(Industry 4.0), Sustainable Development Goal (SDG)

I. INTRODUCTION

Digital Transformation (DT or DX)[1]involves the use of new, fast and frequently changing digital technology to solve problems that may include economic, social, and even governance. This can be said to be underway in some climes but the challenge is that it is not proceeding at the same speed everywhere. Each clime tries to move into digital (era) transformation at a unique pace. However, with the COVID-19 pandemic, most countries consciously or unconsciously have stepped up their digital transformation game because of the reality that the economy is already moving down the y-axis; according to the McKinsey Global Institute's 2016 Industry Digitization Index [2].

The discussion on digitalization is trending based on practical importance for governance, economic business, and human social lives. This is also connected to community development, politics and global international relationships. This paper discusses the COVID-19 impact on the traditional economy and the 'new-normal' COVID-19 has pushed us into digital transformation with the future of economy which is fully digital.

From here the next section discusses the secondary research as literature review in Section II. This is followed by Section III which deals with research methodology which is divided into two viz; primary and secondary research. Primary research consists of qualitative and quantitative analyses. The qualitative analysis is a group of Research Questions administered through an experts' focus group on the subject matter across the continents (Europe, North America, Africa, Asia/Middle East) since the research has a global focus based on COVID-19 pandemic. Also, the quantitative survey was carried out on SurveyMonkey and analyzed in the R Studio using R Programming Language to plot ggplot of the data obtained from the survey. The secondary research is the reviews of existing studies.

Data analysis was done in Section IV based on the focus group discussion of primary research for qualitative survey and ggplot was plotted for the quantitative survey. This also help in identify the gap in the knowledge as the pandemic is novel and researches are just coming up to establish how to cope with this type of pandemic using digital channels. This is followed by use case in Section V. The recommendations of our findings based on

analyzed data were done in Section VI which precludes the concluding Section VII.

The aim of the paper is to examine the impact of COVID-19 on the traditional economy and to also assess the impact of COVID-19 on the adoption of digital transformation for economic activities. And the reason for the research is the fact that COVID-19 has shut down the economic mainstay of many countries and it is logical to start looking at the changes that COVID-19 has brought into our lives. The scope of this research is quite global since COVID-19 is pandemic. Consequently, we have adopted a mixed methodology to be able to get experts' opinions in different regions of the world in both Quantitative and Qualitative Surveys conducted. As we move into the next stage of the economy due to the paradigm shift through the digital transformation, E-Commerce, virtual events, telecommuting, cloud services became major pillars through which we run both major and minor businesses and the final print of Industry 4.0. It is key that the issue of cybersecurity is seen as a major factor that will affect digital transformation as security is critical.

II. LITERATURE REVIEW

A. The COVID-19 Advent

The Covid-19 pandemic outbreak that has affected the entire World since December 2019.WHO declared COVID-19 a pandemic on March 11, 2020; which was projected to have its tentacle across the world, with the observation that governments, businesses, and individuals have substantial ability to change the disease's trajectory[3].

It is evident that the impact of the pandemic will be enormous on small and mid-size companies' global shutdown.Kraus et al,2020 empirical study COVID-19 crisis effects on family firms aiming at firm crisis management reported findings of the very short pandemic period, that the pandemic has not only claimed numerous lives worldwide but also caused severe limitations to daily private as well as business life with high impact on Small and Medium Enterprises (SMEs). The study with exploratory qualitative approach using semi-structured interviews with key informants of family firms of all sizes Western European countries that are in different stages of the crisis. The pandemic signifies a new type of challenge for companies. These companies applied measures that can be assigned to three different strategies to adapt to the crisis in the short term and emerge from it stronger in the long run. Study findings depicts how companies in all industries and of all sizes adapt their business models to changing environmental conditions within a short period of time with a major discovery of massive shift towards tentative digitalization for survival and sustenance while making effort to enhance the requisite operational and resilient realistic strategy for the new normal routine. [4]

Saracco, (2020), projection on the shared and gig economy revealed gradual growth of the human cloud business with respect to the world Gross Domestic Product (GDP). These figures are relatively small with respect to the world GDP, estimated in 86 trillion $ with 140 trillion $ – different purchase value in different countries. However, the expectation is to witness an increasing weight of the platform economy on the world GDP. The 2023 projection according to a recent International Data Corporation(IDC) report; digital economy supremacy is evident and this is based on the threshold produced by companies that have undergone the digital transformation producing 50% of world GDP. Tactlessly, Covid-19 has changed this scenario, with a high and hard impact on the platform and shared economy that have been disrupted by the pandemic.

B. A Call for Digital Transformation

The 4IR hinges on digital infrastructure that occupies a strategic position now more than ever. Various studies have established the upturn of human behaviour and changes in the modus operandi of various economic sectors such as public health, economic, social, and technological trends the advent of the pandemic across countries in the world with respect to the global supply chain. Staszkiewicz et al, :2020 elucidated on various countries' impact of COVID-19 in an empirical study on factors affecting contagion, and mortality. The study presented social media and financial markets analyses with countries data set across the globe from December. 31, 2019 until March 31, 2020. The observation from the classification tree regression and cross-sectional regression models revealed that severity and contagion speed; financial markets and social media response; differ within and across continents. However, the major common factor to all is deployed tools to execute the supply chain as the pandemic contagion increases with measures to curb the spread and still sustain citizens and the economy. Therefore, SMEs have to be proactive to ensure that business and financial flow are not totally cut-off. Thus, the decision of these operators in these sectors to leverage on digital technologies which in turn drives the digital transformation. The study outcome supports policymakers with robust information suitable for resource allocation, this is only applicable to developed nations. However, the study failed to integrate the experience from the developing nations where her major economy drivers are left with the options of how to optimally manage available, if any, scarce resources.

Although the long-term significance of the infection will depend on the degree of qualified support staff shortage as pointed out by [5], the global supply chain distortion in terms of generic drugs as indicated by Chatterjee [6], yet, drug is not the only required item for citizens upkeep, thus, Wang et al, [7] position is supported by strategic supply management of other items relying on alternative costs of the globalization of the supply chain distortion. All these lead to rapid digitization of services, while reshaping digital transformation with respect to individual

country which is opined to counter the submission of wave of bankruptcy and insolvency outbreaks as presented in [8], [9]. While, macroeconomy might struggle with the efficiency of the monetary and fiscal measures in a low-interest rate and high budget deficit environment, it is opined that the gradual or full deployment of digital technologies, leading to the digital transformation will reduce these impacts and converge on the likelihood of COVID-19 fast-tracking virtualized economy on digital infrastructure.

Robust telecommunications network is important for economic growth and constitutes a significant portion of the world's economy as well as improves productivity and efficiency in other sectors. In some ways, the present technological shift is traced to a huge digital transformation that is already well underway. In a period of days, almost any process that could be rapidly digitized has been virtualized: video conferencing enabling a case discussion and telemedicine enabling remote diagnosis and treatment, even law delivering judgement; the New York Stock Exchange just closed its trading floor and has moved to electronic trading. [10]

[11] states that a modernization of social, economic and democratic institutions, as well as greater public-private collaboration are required. Although, it is opined that these might have inherent risks which must be tactically and collectively mitigated by governments and businesses via regulatory models and policies that yield economic developments and innovation. It is also noted that fair

competitions among investors as well as users' rights guarantee the agility of intervening authorities to realizing a sustainable digital economy that is capable of transforming various revenues sector of the country; hence the necessity of maintaining adequate standard frameworks, it will in other hand, foster sustainable digitalization inspite of its inherent environmental complexities.

Thus, digital transformation brings a fundamental change in all spheres of human society, prompted by the use of information technologies which can be applied in the economy, but also in different segments of society, such as public rights, entrepreneurship, education, medicine, mass communication and agriculture [12]. It is clearly evident that digital transformation must be a continuous and comprehensive process that encompasses different spheres of society. Thus, any nation that seeks to toll its route, in attaining the ITU's 2030 Agenda for Sustainable Development Goals, can beckon on ITU's effort and reliable commitment of achieving a better-connected world. These SDGs could be realizable on the short and long run of the digital economy; SDG 3: Good Health and Well-being, SDG 4: Quality Education; SDG 8: Decent Work and Economic Growth; SDG 9: Industry, Innovation and Infrastructure; SDG 11: Sustainable Cities and Communities; and SDG 17: Partnerships for the Goals

Caping it all, COVID-19 pandemic has swept across the world at breakneck speed, impacting not just global financial markets and businesses but disrupting every aspect of human daily lives [13] with long-lasting implications global economy. As COVID-19 continues to spread around the world, more and more enterprises will miss their financial targets because of supply chain disruptions and dampened customer demand. [14]Reflecting this obscurity, this section outlines the overall problems and solutions.

III. RESEARCH METHODOLOGY

The research methodology is based on two matrices of Primary Research and Secondary Research.

A. The Primary Research was based on both Qualitative and Quantitative Surveys. The Qualitative Survey was conducted using experts in the field who were selected from North America, Europe, Africa, Middle East, and Asia and were interviewed to get their views and opinions on the Research Questions(RQs). This survey was discussed in Section IV and the data was transcribed. The research was conducted through online interview of 5 interview respondents and their responses were analyzed and grouped into categories. As such, it was established that a point of theoretical saturation had been attained. The 5 interview respondents used different words in explaining the same thing. So, the data collection at this point of the research was ended. The research team could not access NVivo and improvisation was made by "play and listen repeatedly". And to compliment this limitation, a quantitative survey was conducted at SurveyMonkey [15]. And the data from this quantitative survey was analyse in the RStudio using R Programming to plot ggplot. The data obtained from the quantitative survey are tabulated below:

Table1: Summary of Quantitative Survey

	Yes	**No**	**Partially**	**Respondents**
COVID-19 Awareness	97.98%	0%	2.02%	99
Digital Transformation Awareness	68.69%	6.06 %	25.25%	99
Impact of COVID-19 Pandemic on (National Economy, Businesses, Organisation, Education etc)	81%	2%	17%	100
Effect of Lockdown order on (National Economy, Businesses, Organization, Education etc)	89.59%	5.41 %	15%	100

From the above table, total number of respondents for question on COVID-19 Awareness was 99 while 100 respondents answered the question on Impact of COVID-19 pandemic on National economy, business, education etc. The quantitative analysis was done using R Programming Language for plotting ggplot for better data visualization of quantitative analysis in Section IV.B.

B. Secondary Research was also conducted through the review of existing literature and journals in order to get up to date information and to identify the gap within the body of knowledge that this research addressed. From the review, the review showed that the COVID-19 is novel and there is need to establish how to manage the economy vis-à-vis COVID-19 pandemic.

IV. DATA ANALYSIS

The purpose of this qualitative aspect of this study is to explore the various impact of digital transformation during and after the COVID-19 era. A qualitative aspect of this study was proposed based on the need to seek the opinion of experts on the topic and other factors within the digital transformation ecosystem as described in Section II above. The main aim sought response to the following Research Questions (RQs).

RQ1. In your opinion, how has COVID -19 impacted education e.g. more schools have moved online to complete academic semester and session?

RQ2. How has COVID-19 impacted the way we work? E.g. because of stay at home and lockdown due to COVID -19 many offices have started working online?

RQ3. How can digital economy and transformation help to suppress economic depression due to COVID -19 impact e.g. Online Banking activities, Electronic Commerce-buying food, essentials and other articles online to keep the economy going?

RQ4. What will be the impact of COVID-19 in pushing us to have a quantum thought, actions, and plans towards digital transformation/economy?

RQ5.What way can digital economy/transformation assist in reducing the effect of COVID-19 on the traditional economy?

The process used for the analysis of the qualitative data is shown in the Fig. 1 below, which include transcribing the recorded focus group discussion followed by Coding. The codes transcribed from the interview was grouped into five categories; Adaptation, Adoption, Impact, Development and Shift. The unedited codes as transcribed from the interview and also grouped into sub-category. Downsizing and reframing of the initial codesfor the purpose of easing analysis and avoiding repetition. All codes that represent same expression are been reframed to a single code (sub-category) and refined to core categories. based on which Thematic development is done. This lead structural representation. This is followed by memo writing which leads to findings and the results which were included in the conclusion and recommendations.

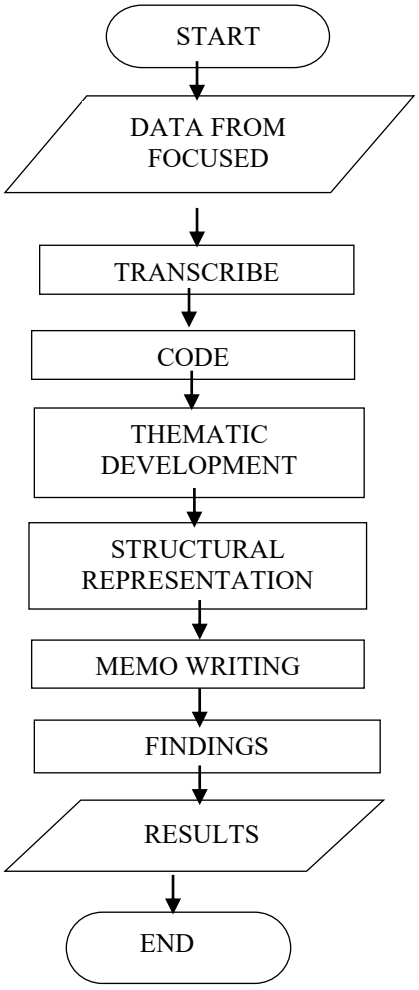


Fig. 1 Flowchart of Qualitative Analysis

A. Memo writing based on Model

Based on the above flowchart Fig. 1 above, the final codes are explained in the memo writing below:

- Adaptation comprises all codes that represent respondent's opinion that COVID-19 has created constraints to physical learning and as result academic activities have been moved online. The experts' opinion suggested that the pandemic has led to the adaptation of online education due to restriction of in-person or face to face learning.

- Adoption here contains all codes that depict that digital transformation cannot be overemphasized as an obvious choice that has come to stay, which all activities, events and transaction must align to the fresh realities as a result of their coronavirus pandemic. Thus, the respondents highlighted the positives and negative. The positives far outweighed the negatives.

- Impact category explains all codes representing experts' opinion on the impact of COVID-19, such as factors that ensure various outcomes in the digital economy. This category covers codes which explain respondents' opinion on organizations' attitudinal response to their future performance.

- Development suggests the main responsibilities of businesses in harnessing new ideas within the bounds of digital transformation in the era of COVID-19 and beyond. Coming up with structures that would be favourable to both employers and employees without diminishing in output. This category depicts codes that are concerned with communicating operational changes for sustenance.

- Shift explains the codes that are concerned with a new level of thinking which the COVID-19 has forced upon all countries' leadership. This category covers the codes that depict the need for fresh thinking that have resulted in creating a global level plain.

From the memo, the findings showed that the main point of discussion during the COVID-19 pandemic is the adoption of online activities, events and transaction which is a barometer for the digital transformation. Educational institutions, businesses and people's way life have been forced to adopt digital transformation as result of the limited interaction that the COVID-19 has brought. Organizations are beginning to realize the gains of adopting digital transformation in improving their bottom and increasing productivity with less overhead burden.

B. Data Analysis based on the Quantitative Survey

The quantitative analysis below was based on the quantitative survey conducted on survey monkey at [15].Data visualization of the data collected from this survey was done using ggplot2 package in R Programming Language. Results of the plots generated were used to conduct the analysis of the questions as tabulated in Table 1, Table 2 and Table 3.

- COVID-19 Awareness

The ggplot generated from RStudio for Table 1 is shown below in Fig. 2

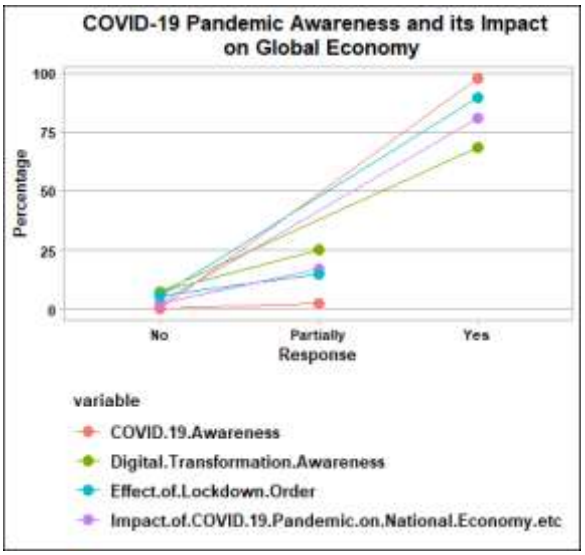


Fig. 2: COVID-19 Pandemic Awareness and its Impact on Global Economy

The above ggplot shows the visualization of data from the survey results and it established and validated the following facts which is similar to the findings of qualitative analysis.

C. Colour Interpretation of ggplot

Colour red from the ggplot legends shows that the awareness of on COVID-19 is very high as shown in the ggplot. The value 97.98% showed a sharp and rapid paradigm shift to online activities.

Colour green from the legend also established the fact that there is high level awareness with value 68.69% on digital transformation based on the impact of COVID-19.

Colour purple showed that 81% of businesses that were not ready to transformdigitally before COVID -19 have moved very fast to embrace digital transformation.

Colour blue from the ggplot showed 89.59% negative effect of lockdown on businesses. And hence the need to digitally transformed. Colour purple shows that COVID -19 has greatly impacted on national economy and this also brings the need to digitally transform businesses based on the impact on national economy.

The sharp rise and change of direction can be interpreted that the paradigm shift became rapidly visible. This confirms the memo and the findings from the qualitative analysis.

- Acceptance of Telecommuting

Table 2 below shows that the society is ready to accept a policy on working from home if it is included in the national policy as part of Digital economy and transformation using the available digital channels like the internet viz:

Rate of acceptance of the work-from-home/work remotely, if included in the National Policy as part of Digital Economy and Transformation using the available digital channels.	
Response	**Percentage**
Yes	62.63%
No	14.14%
Yes, I will at certain times like COVID-19 pandemic	23.23%
Total Respondents	99

Table 2: Showing Rate of Acceptance of Telecommuting if the government brings such policy

Table 2 is a tabulated data based on conditional question of telecommuting. The large percentage of "Yes" shows that telecommuting will be acceptable if such policy is put in place. And the ggplot below shows the data visualizationon the above question.

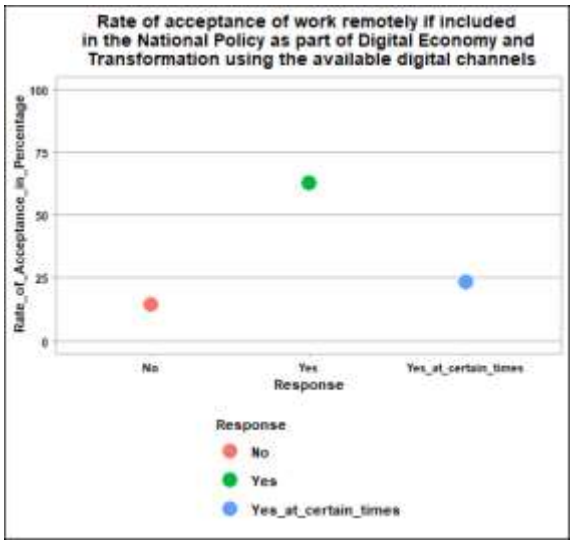


Fig. 3: ggplot for Rate of Acceptance of work remotely policy adoption

The ggplot above showed that telecommuting will be accepted if there is a national policy on it. 62.63% (Colour green) wants to telecommute if the government brings a policy on that. And the citizens are ready to embrace it to keep safe especially in times of pandemic like COVID-19 pandemic. The legend showed that colour red (14.14%). is a very low percentage of people not ready to accept telecommuting. This also confirm the qualitative part of the qualitative survey transcribed in section 4a memo. Based on the strong evidence gathered from both the qualitative and quantitative survey, Section V below analysis a proposed use case of how digital platform can be deployed.

Impact of digital economy and transformation during COVID-19 pandemic

Impact of Digital Economy and Transformation during COVID-19 Pandemic e.g. [Online Banking, Electronic Commerce (Business transaction, goods and services delivery), Telemedicine, E-Pharmacy, etc.]	
Response	**Percentage**
Yes	41%
To a large extent	38%
Minimal	16%
No	5%
Total Respondents	100

Table 3: showing impact of digital economy and transformation during COVID-19.

Table 3 above showed the impact of digital transformation and transformation during COVID-19. And the ggplot in Fig. 4 below showed the data visualization.

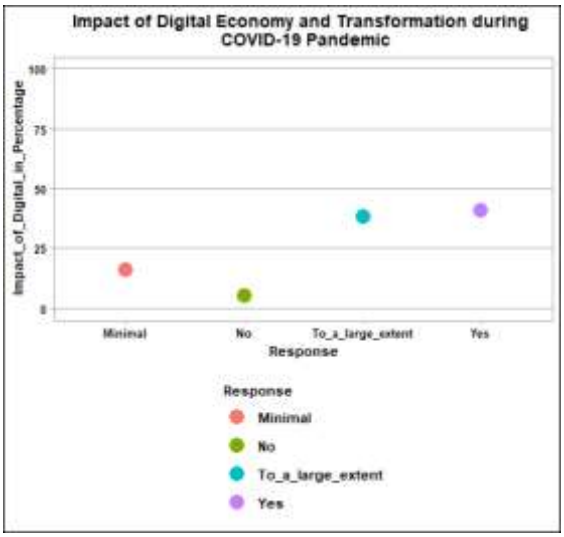


Fig. 4: Impactof Digital Economy and Transformation during COVID-19 Pandemic

The ggplot showed that an aggregated total of (41+38%= Colours Purple and Blue) summing up to 79% rapidly adopted digital channels to transact businesses at the advent of COVID-19 so as to limit person to person contact as lockdown was implemented in many climes all over the world together with social distancing. Hence, digital economy and transformation which allow businesses to be done on digital channels with less human contact became the most favorite business strategy.

V. USE CASES AND SOLUTIONS

There are a number of technology-based solutions which can be used as digital transformation agents during this period of Covid19. Most of these solutions are aimed at reducing human to human contact. They cannot all be

discussed in this section thus we focus on a modified ecommerce system which uses drones for item delivery.

Fig. 5 shows the highlevel use case diagram of an electronic purchase / delivery system while Fig. 6 shows the flowchart. The traditional human to human interaction during delivery is totally eliminated.

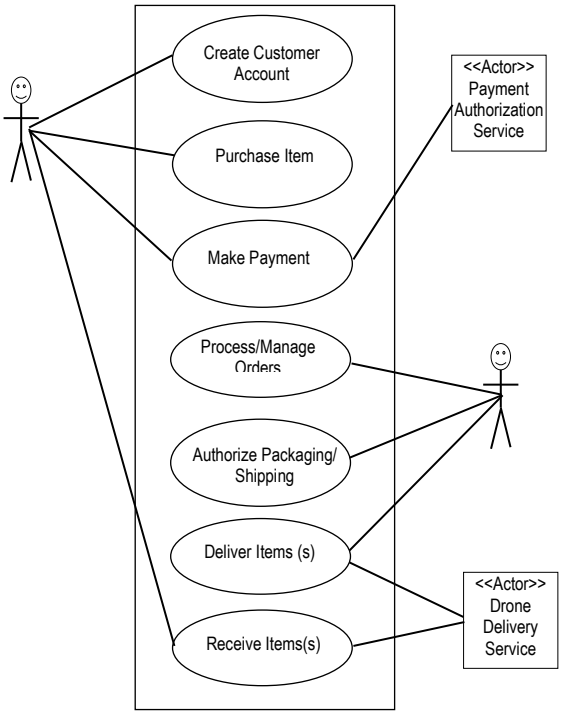


Fig. 5: High level use case diagram for a modified electronic purchase/drone delivery system

The diagram shows four actors, one of which is the primary (customer-LHS), while the others are secondary. Two of the secondary actors are system actors (Payment Authorization Service and Drone Delivery Service). The other secondary actor is a human actor (Sales Personnel). Section 5.1 shows the detailed Use Case for the "Deliver Item" goal.

5.1 Use Case : [Deliver Item]

5.1.1 Description: One amongst a fleet of delivery drones carries out the delivery of the purchased package (one or more items) as assigned by the sales personnel.

5.1.2 Level: Summary

5.1.3 Trigger: A Sales Personnel clicks the “deliver item(s)” button on the administrative interface.

5.1.4 Primary Actor: The Primary Actor is the Customer who bought the item(s) using the mobile app.

5.1.5 Additional/Supporting Actors: Sales Personnel and Drone Delivery Service (Secondary Actors)

5.1.6 Stakeholders: Packaging Department, Onloading screw, Quality Control Department

5.1.7 Preconditions: A customer placed an order which has been confirmed and authorized by a sales personnel.

5.1.8 Main Success Scenario

1. Drone Delivery System confirms an available/functional drone in the fleet.
2. Drone Delivery System Assigns specific delivery to a drone in the fleet.
3. Drone Delivery System documents the assignment.
4. Assigned drone in fleet reconfirms functional status.
5. Assigned drone leaves the fleet bay area and flies to the loading area.
6. On-loading crew loads package(s) on the assigned drone.
7. Assigned drone reconfirms battery status, GPS status, etc
8. Assigned drone loads customer location information in memory.
9. Assigned drone delivers packages to customer destinations using GPS data.

5.1.9 Extensions

a. **Exception**: No available drone in fleet: System displays a drone unavailable warning message, calculates estimated time of arrival of a drone to fleet and places delivery on queue.

b**.** **Exception**: Assigned drone functionality faulty: System returns to main command path item 1.

c**.** **Exception**: Battery Status or GPS Status etc faulty: Assigned drone displays an error message and notifies the Drone Delivery System. Drone Delivery System restarts from command item 1 on the main command path. Loading Crew unloads package from drone.

5.1.10 Post Conditions

a **Success End Condition:** The customer receives package delivery notification for confirmation.

b **Minimal Guarantees:** The Drone Delivery System logs all activities and takes snapshot of customer.

c Failure End Condition: The customer does not receive the desired item, and the Company’s inventory remains the same.

5.1.11Frequency: As often as a purchase is made from a particular neighborhood.

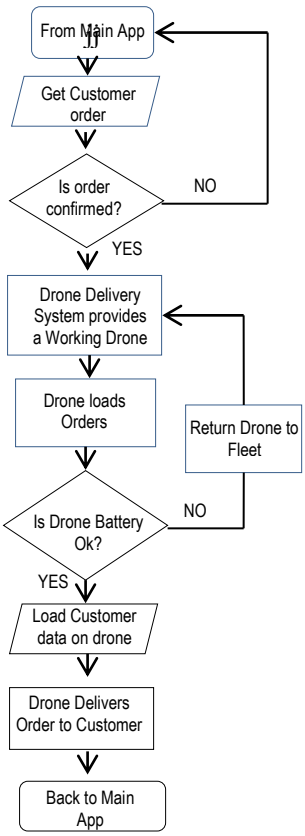


Figure 6: The Flow Chart for a modified Electronic Purchase/Drone Delivery System

5.1.12 Special Requirements

a **Performance, Security and Usability/Accessibility:** The drone battery life must be good enough to execute the package delivery. Technologies such as voice recognition, facial recognition and encryption will be used. Drone operations must be as approved by the regulatory agencies and it should support major languages

5.2 System Use, Influence on Digital Economy and Encouragement During the Pandemic:

Amazon Prime Air is a drone delivery service currently in development by Amazon. It is one of the first major efforts on drone delivery service by a major ecommerce company. This was reported on BBC news [16]. There is currently no evidence that this effort has been used in large commercial settings yet, aside from the tests and promises.

According to Corrigan [17], delivery drones can be used in medical supplies, food and other package deliveries. Big players like Alphabet Inc. (Google's Parent Company), Walmart and UPS are becoming major players.

One of the major reasons for decrease in commercial activities in both developed and developing countries during this covid19 pandemic is the imposition of lockdowns and the reduction of human to human contact through social distancing. Commercial activities all over the world have reduced to its barest minimum. This has led to low demand for goods and services which can also be interpreted as low access to them. As may have been noticed from above, drone delivery systems have been suggested a long time ago before the covid19 era. Its suggested introduction was to reduce delivery cost and time. Now, using it during this pandemic era would also have these advantages of delivery cost and time reduction, and then human to human interaction reduction. Thus, businesses will begin to get demands once again and orders fulfilled without largely affecting the lockdowns.

This system reduces human to human contact to the barest minimum as customers only interact with the mobile and web apps, and the drone which delivers the package. Thus, the customer has no business having any physical interaction with humans which can be carriers of the dreaded covid19 virus.

VI. RECOMMENDATIONS

A. From the Qualitative survey memo and the findings, it is established that COVID-19 has catalyzed the speed of transiting from traditional economy to online businesses which is an integral part of digital transformation. This is also evidenced in the result of quantitative survey conducted in which Table 3 and Figure 4 established the high rate of impact of digital economy and transformation during COVID-19 pandemic in which the aggregated impact is (41+38)% implies total aggregate of 79%. This is both established in both developed and developing countries because the scope of the research had been established to be global. Consequently, it is recommended that it is important for both major and minor businesses to reengineer their business strategies towards the use of digital channels as this is the future of economy.

B. Figure 3 and Table 2 showed the results of quantitative survey on policy on telecommuting. The ggplot put the acceptance rate at an aggregate of (62.63 +.23.23)% implies a total aggregate of 85.86%. The implication of this is that if the government put this policy in place majority are ready to embrace it. For telecommuting to be implemented, it has been shown from the literature review that the ICT infrastructure is key to a successful implementation of digital transformation in which telecommuting is a subset. This is also verified from the findings of the qualitative focus group investigation RQ2 in Section 4. Consequently, it is recommended that government at all level should commence work on National Policy on Telecommuting.

VII. CONCLUSION

From the investigation conducted, it has been successfully established that Digital transformation can only be implemented based on the availability of digital channels

with developed countries having advantage of readily available infrastructures to accelerate the implementation of digital businesses during the COVID-19 pandemic. Fig. 4 and Table 3 showed fast adoption of digital economy and transformation as very high percentage of businesses moved unto the digital platform at the advent of COVID-19; 79% of respondents agreed that digital economy and transformation greatly impacted on business activities at the advent of COVID-19. This is also valid for the developing countries. The need for appropriate policies has also been successfully validated.

REFERENCES

[1] J. O'Donnell, "IDC says get on board with the DX economy or be left behind". Source: techtarget.com. 2017.[Accessed: 15-April-2020].

[2] J. Bughin, E. Hazan, E. Labaye, J. Manyika, P. Dahlstrom, S. Ramaawamy and C. Cochin de Billy, Digital Europe: Realizing the continent's potential, McKinsey Global Institute,[online].Source: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-europe-realizing-the-continents-potential [Accessed:15-April-2020]

[3] The ITU News, 5G | Broadband/Network | Infrastructure | Policy/ Regulatory Reform, 2019.

[4] The digital transformation of Mauritius: Q+A with Minister Sawmynaden[online] Available: https://news.itu.int/the-digital-transformation-of-mauritius-qa-with-minister-sawmynaden/ [Accessed April 21, 2020]

[5] H.Catton,''Globalchallengesinhealthandhealthcare for nurses andmidwiveseverywhere,'' Int. Nursing Rev., vol. 67, no. 1, pp. 4–6, Mar. 2020, doi: 10.1111/inr.12578.

[6] P. Chatterjee, ''Indian pharma threatened by COVID-19 shutdowns in China,'' LANCET, vol. 395, no. 10225, p. 675, Feb. 2020, doi: 10.1016/ S0140-6736(20)30459-1.

[7] X. Wang, X. Zhang, and J. He, ''Challenges to the system of reserve medical supplies for public health emergencies: Reflections on the outbreak of the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) epidemic in China,''BioSci.Trends,vol.14,no.1,pp. 3–8,Feb.2020,doi: 10.5582/bst.2020.01043.

[8] P. Staszkiewicz and B. Witkowski, ''Failure models for insolvency and bankruptcy,'' in Contemporary Trends and Challenges in Finance, K.Jajuga, H.Locarek-Junge and L.T. Orlowski, Eds. Cham, Switzerland: Springer, pp. 219–225, 2018.

[9] A. Nocoń and I. Pyka, ''Sectoral analysis of the effectiveness of bank risk capital in the visegrad group countries,'' J. Bus. Econ. Manage., vol. 20, no. 3, pp. 424–445, Apr. 2019, doi: 10.3846/jbem.2019.9606.

[10] M. Iansiti and G. Richards. 'Coronavirus Is Widening the Corporate Digital Divide', 2020. [Online]. Available: https://hbr.org/2020/03/coronavirus-is-widening-the-corporate-digital-divide. [Accessed: 23- Apr- 2020].

[11] Global Telecoms Maturity Index - Top 20 Countries (2019) https://www.budde.com.au/Research/Global-Telecoms-Maturity-Index-Top-20-Countries. [Accessed 21-April - 2020].

[12] ITU's 2017 ICT Development Index (IDI), 2017.Available: https://www.itu.int/net4/ITU-D/idi/2017/index.html'. [Accessed : 21-April - 2020].

[13] Matt Craven, L. Liu, M. Mysore and M. Wilson, 'COVID-19: Implications for business', 2020. [Online].Available: https://www.aedcr.com/sites/default/files/docs/mckinsey-full_article.pdf.pdf.pdf . [Accessed: 23- Apr- 2020].

[14] The World Bank, The Global Economic Outlook during the COVID-19 Pandemic: A changed world, 2020. Source:https://www.worldbank.org/en/news/feature/2020/06/08/the-global-economic-outlook-during-the-covid-19-pandemic-a-changed-world [Accessed: May 20, 2020]

[15] https://www.surveymonkey.com/r/XT26WJW.

[16] D. Lee. D,. "Amazon to deliver by drone 'within months' [online].2019. Available: ".https://www.bbc.com/news/technology-48536319 [Accessed: 24/04/2020]

[17] F. Corrigan, "Drones For Deliveries From Medicine To Post, Packages and Pizza".2019. [online] Available: https://www.dronezon.com/drones-for-good/drone-parcel-pizza-delivery-service. [Accessed: 24- April- /2020].

Hidden Markov – Based Computational Intelligence for Behavioral Analysis of Organized Criminal Network

M. E. Nwanga
Department of Electrical Electronic Engineering
Federal University of Technology
Owerri, Nigeria
enwanga@yahoo.com

K. C. Okafor
Mechatronics Engineering Department
Federal University of Technology
Owerri, Nigeria.
kennedy.okafor@futo.edu.ng

***Abstract*— Increasing terrorist activities globally have attracted the attentions of many researchers, policy makers and security agencies towards counterterrorism. The clandestine nature of terrorist networks makes them difficult for detection. Terrorist actions occur in two inseparable stages: the planning stage and the execution stage. The planning stage is invisible and unnoticed to public while the execution stage is the last and lethal stage. Understanding the flow of command and intelligence within the active internal communication (AIC) of the network becomes imperative for proper counterterrorism. In this paper, Hidden Markov Model (HMM) is used to computationally analyze the level of connections and strategic alliance within the terrorist group in Nigeria. The result obtained revealed that the adjacency matrix of criminal network is a determinant factor of its operation and intelligence. The criminal network was observed to have a property of symmetric adjacency matrix while the social network have both asymmetric and symmetric adjacency matrix. It was observed that the unique property of criminal network such as symmetric and idempotent property conferred a special protection to the network resilience.**

Keywords—Computational Intelligence, Counterterrorism, HMM, Network Adjacency Matrix, Terrorist Network.

I. INTRODUCTION

The spate of organized criminal attacks in the world has been on the increase in the last few years and has posed the greatest threat to the societies across the globe. In the same range, Nigeria has experienced a lot of this organized criminal attacks ranging from kidnapping, Boko - Haram (BH) and most recently the Herdsmen attack. These consist of the violent criminal attacks of state and non-state actors in their covert and overt interdependence [1]. It has the highest negative social and economic consequence to any nation as it hinders the economic development of any nation and degrades its gross domestic products (GDP) [2][3]. Thus, attacks of terrorist have great lethal and destructive impact on every nation in economic terms of huge casualties and property losses.

The recent successes recorded by the criminal elements in any nation have been attributed to lack of actionable intelligence (AI) that would have enabled predictive and detective actions against them [4][5]. Hence, the traditional command and control techniques of tackling criminality has become ineffective [6]. In the wake of present terrorist incidents in the world, a paradigm shift is necessitated to data - driven mindset via actionable intelligence. Then a shift from the traditional approach of "Sense and Response" *(SaR)*; the command and control techniques to modern dimension of "Predict and Prevent" *(PaP)* using computational intelligence (CI) becomes vital.

Processing of intelligence information within the organized criminal networks to discover hidden links and structures is paramount for any successful counterterrorism. The clandestine nature of criminal networks makes them difficult to be detected [7], but they could be possibly detected through application of computational approach on the hidden links (HLs) [8], [9]. This enables proper analysis of their adversaries' goals and intentions and further reveals new information about entities within the network. Every criminal networks consist of interconnected criminal states (CS) in their covert nature [10], active internal communications (AIC), time frame of attack (TFA) and mapped states (MS) [11]. The criminal state is made up of Commander Cd , Gatekeeper Gk and Foot-Soldiers Fs .

Understanding the complex dynamics of terrorist network offers a great deal of probability of detection [12]. Computational intelligence for counterterrorism provides the structural and hierarchical knowledge of criminal networks [13], [14]. When this approach is applied with HMM for this purpose, based on its stochastic and tractability, a data- driven architecture is generated. This could fuel smart security initiative to combat terrorism and other organized criminal networks [15].

Hidden Markov model (HMM) is a partially hidden Markov Chain, named after Andrey Markov, 1856–1922[16]. The Markov Chain Model is defined as a mathematical model for predicting the future state depending only on the current state [17], [18]. HMM) is a finite set of states, each of which is associated with a probability distribution. Transitions among these states are governed by a set of probabilities called state transition probabilities. In a particular state an outcome or observation can be generated, according to the associated probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model [19]. Since terrorist activities is a time series event and occurs in two stages that is planning and execution stages. Then HMM is applied based on its relative mathematical ease of immense versatility which makes it

suitable for use as a stochastic process in the analysis of terrorist records[20].

Motivated by these backgrounds, HMM is used to computationally analyze the behavior of Boko-Haram (BH) and Herdsmen with data-driven intelligence for the period of 2010 to 2016. This paper contributes to knowledge by providing the network relational intelligence within the BH and Herdsmen networks through computation of their network adjacency matric (NAM). It further provides some mathematical uniqueness of criminal networks from social networks that aid foundation of computational methods of counterterrorism and mathematics of criminal networks.

The rest of the paper is organized as follows: Section 2 presents some existing research works on criminal networks, computational intelligence and HMM for analysis of organized criminal networks. Section 3 provides the methodology of the research. Section 4 presents and discusses the results and findings of the work. Section 5 concludes the paper and gives recommendations for future work.

II. LITERATURE REVIEW

Several studies on organized criminal networks (Boko-Haram & Herdsmen), computational intelligence and Hidden Markov Model have been carried out over the years. Some of such recent literatures are reviewed and presented in this section.

The work in [21]presented the historical evolution of Boko Haram in Nigeria and stated the causes, recruitment, ideology, area of operation and the ways through which the problem can be solved. The authors further presented that more than six million Nigerians have been killed by this group while more than 300,000 people have been displaced. It also includes the destruction of hundreds of schools and government buildings mostly in the North East of Nigeria which had devastated its already ravaged economy.

Similarly, [10], [22] discussed the threat of terrorism (Boko-Haram group) and the challenges in countering their operations on the set targets. Lack of a clear-cut counterterrorism strategy, dearth in technological and mutual trust between actors and locals in the management and utilization of intelligence were recommended as the major challenges for destabilizing the attacks of terrorism in Nigeria.

The work in [1] revealed that the socio-demographic network characteristics and antecedent behaviors of were the major drivers of lone-actor terrorists. The work examined whether lone-actor terrorists differed based on their ideologies or network connectivity from group terrorism (organized criminal network). The work further stated that wide range of activities and experiences preceded lone actors' plots or events and that Lone-actor terrorists regularly engaged in a detectable and observable range of activities with a wider pressure.

The authors in [23] presented the three groups of organized crime topologies as follows: models that focus on the physical structure and operation of an organized crime groups (OCGs), activities of OCGs, and the social, cultural and historical conditions that facilitate organized crime activities. The work [14] investigated the structural position of covert (terrorist or criminal) networks using secrecy versus information tradeoff characterization. The result shown that network structures are generally not small-worlds, in contradistinction to many overt social networks. This finding was backed by empirical evidence concerning Jemaah Islamiyah's Bali bombing and a heroin distribution network in New York.

[24] Proposed a model for finding the correlation of communication contents of all nodes with data dictionary and detects nodes based on a threshold correlation value. New network was drawn and its density was calculated and centrality measures were applied on the new network that produced different key players with different roles in the network.

The authors in [25] propose a visual analytics approach to support analysts in monitoring and reasoning about the dynamics in a complex system. The authors approach systematically mapped relations onto the user interface and supported both overview and provenance over temporal dynamics.

The work [26] built and implemented graph base knowledge called TKG from GTD and Wikipedia. The authors Compared with GTD and observed that TKG enhanced the organizations of terrorism entities and relationships, and enriched the description by attaching Wikipedia knowledges. Finally, they concluded that TKG can better the understanding of terrorism attacks for both human beings and machine processing such as graph mining and knowledge reasoning.

The concept of extracting knowledge from graph data in adversarial setting was similarly presented in [27]. The author discussed several approaches to analyze graph data and illustrated with examples from Al-Qaeda terrorist network. Computation of node properties including adjacency matrix was done. Similarly the authors in [28] discussed the counterterrorism in a dynamic and complex threat environment. The authors proposed some finding, summarized and evaluated the relevant information from large and dynamic data stores. Counter-efforts of finding actionable intelligence was also proposed by finding meaningful pattern hidden in masses of noisy data items.

The authors [13] presented the first computational analysis of terrorist organization and proposed two algorithms for computing Lindelauf *et al.*'s centrality metric. The algorithm was exact, and ran in time linear by number of connected subgraphs in the network and further identified key players in the WTC 9/11 terrorist network, constructed of 36 members and 125 links, in less than 40 minutes.

The work in [29] discussed the application of HMM for computational intelligence with mathematical proofs. The report focused on the three common problems of HMM such as evaluation problem, uncovering problem, and learning problem, in which learning problem with support of optimization theory was the main subject.

The work [30] described a HMM for the evolution of an advanced persistent threat (APT). The authors model was to validate whether the evolution of the partially reconstructed attack campaigns were indeed consistent with the evolution of an APT. The score obtained enabled the

comparing of fit of APTs of different lengths and was validated with the score using data obtained from experts.

This paper focused on determining the network relational intelligence within the terrorist elements by computing the network adjacency matrix as well as the mathematical uniqueness of criminal networks that differentiates it from social networks. Further work on this, will include the application of the computational intelligence in driven a HMM algorithm for prediction of terrorist attacks in Nigeria.

III. METHODOLGY

This paper generated the network information within terrorist elements. It computed the mathematical network adjacency matric that exists among the elements of criminal network. The computation was based on trend and sequence of communications and intelligence within the terrorist network. The data used in this study was collected from the global terrorism database (GTD) for the period of 2010 - 2016.

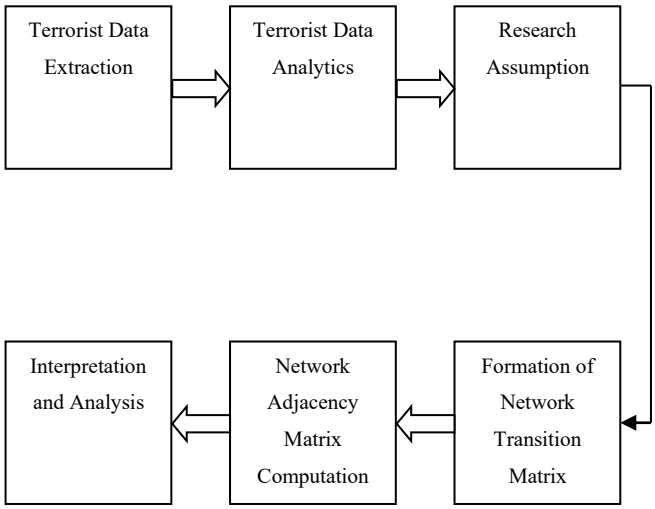


Figure 1: System Architecture.

A. Research Assumption

Every criminal network maintain high and low profile actors with the cross–ties emerging dormant after coordinated attack. The ergodic nature of terrorist network in space and time creates transition among the elements, with transitory shortcuts. There exist the network kingpin otherwise known as the commander Cd *(high profile actor)*, the gatekeeper Gk and foot-solider Fs as the low profile actors. We therefore denote them as the hidden elements within a terrorist states H_S in eq. (1) as an association of three different nodes.

$$H_S = \{H_{Cd}, H_{Gk}, H_{Fs}\} \quad (1)$$

Then, how significant each node is as a conduit for information or influence becomes key and imperative. This necessitated the following six (6) assumptions to guide the node classification, network formation and data analysis.

i. There exist hidden active internal communication (AIC) in the network.
ii. The flow of the communication is directed from the leader to the gatekeeper and from the gatekeeper to the foot-soldier.
iii. There exist no feedback communication within the network.
iv. The commander does not have any link with the foot-soldier in order to maintain a transitory shortcuts.

The data contained the names of suspected criminal groups that carried out an attack, the targets of the attack, the target sub-type, description of the attack, geographic location of the attack among other events. The time frame of attack and terrorist states that carried the attacks were sieved out of the dataset and subsequently used to drive home some attack information (intelligence). The system architecture, represented in figure 1, is made up of the following components: terrorist data extraction (TDE), Terrorist data analytics (TDA), markov assumption (MA), formation of network transition matrix (NTM), network adjacency matrix and interpretation and analysis (IA).

v. An attack always precede a particular active internal communication.
vi. Commanding group and the gatekeeping group do not carry out suicide attack. Consequently only the foot-soldiers carry out suicide attacks which are usually masterminded by the Cd and Gk.

The existence of the states is now put to use in accordance with Hidden Markov Model (HMM) principles. Markov process is assumed since there is a possible step in movement of transition with the states. AIC originate from Cd to Gk and from Gk to Fs. A first order Markov Model is formed in eq. (2). Here the future state depends only on the current state. That is, the probability of entering a certain state depends only on the last state and not on any earlier state.

$$p\left[s_{t+1} / s_t, ..., s_2, s_1\right] = p\left[s_{t+1} / s_t\right] \quad (2)$$

Where s_{t+1} is a state lower in rank in the terrorist network, given a next high state in rank with directional AIC.

B Formation of Network Transition Matrix

There exist transitions within the network due to changes in criminal state(s). The network transition matrix is a conditional probabilities that a criminal attack was carried out by *state j* given that an active internal communication was made by *state i*. It is the probability that the stochastic event (terrorist action) changes current states s_i to next state s_j. Statistically, the sum of the probabilities of transitioning from any given state to other next state is 1. The above statements are illustrated in eq. (3) and eq. (4).

$$p_{ij} = p\left(s_i / s_j\right) \tag{3}$$

$$p_{ij} = p\left(s_i / s_j\right) \tag{4}$$

Where s_i the initiating state of the terrorist action is, s_j is the execution state of the network, S represent the terrorist states variables and S the criminal computational space. The transition matrix of the network is then formed in Eq. 5.

$$\begin{bmatrix} (CdCd) & (CdGk) & (CdFs) \\ (GkCd) & (GkGk) & (GkFs) \\ (FsCd) & (FsGk) & (FsFs) \end{bmatrix} \tag{5}$$

The transition matrix is then computed from the data obtained on the various attack traces of the terrorist elements using the above assumptions.

C Computation of network adjacency matrix

The importance of adjacency matrix in a criminal network is to understand the dynamics of the network. It helps to determine the level of interactions and flow of command among the hidden elements of any terrorist network. It is a dependent factor in determining the secrecy and efficiency of within the network operation and its resilience.

Generally, given a criminal network G, an adjacency matrix A is formed as follows:

$$G = (V, E) \tag{6}$$

Where V is the criminal (terrorist) elements while E is the AIC.

$$A_{ij} = \begin{cases} 1 \\ 0 \end{cases} \tag{7}$$

Here $a_{ij} = 1$, if i is adjacent to j and 0, if i is not adjacent to j.

A node as a terrorist element is adjacent to another node if the two nodes share a common tie. In criminal network, on the bases of its nature and mission, there exist two levels of ties (relationship).

i. Relationship with criminal elements'(actors) themselves
ii. Relationship that each criminal element (actor) has with one another.

Actors' relationships with themselves are ignored in social network but rather the relationship that each actor has with one another is deeply considered. Thus the cells along the diagonals are usually recorded as 0's. This is not so in criminal (terrorist) network where the both relationship(s) above are tightly considered and is recorded as 1's along the diagonal.

Considering the fact that Cd and Fs do not communicate and the non-existence of feedback communication within the network due to transitory shortcuts. In extracting the adjacency matrix, these ties (relationship) is invoked. The relationship the actors have with themselves as well as the relationship the actors have with one another are considered as I's, where it exist and 0's otherwise.

D RESULTS AND DISCUSSION

The results obtained are shown in the Table 1 and 2. Total of 269 attacks were recorded for the period of 2010 to 2016. Table 1 presents the criminal state attack statistics. Here the commander (Cd), carried out a total of 6 attacks, gatekeeper carried out 19 attacks and 244 attacks were done by the foot soldiers. This shows that the commander only carries out high profile and strategic attacks while gatekeeper and foot soldiers are both responsible for 97.8% of all the terrorist attacks that took place within the period. This further reveals that foot soldiers are more prevalent and vulnerable in every terrorist actions.

Table 1: Criminal State Attack Statistics

State (i, j)	Frequency	Percent
Cd	6	2.2
Fs	244	90.7
Gk	19	7.1
Total	269	100.0

Considering the assumption of active internal communication within the network (AIC), Table 2 is generated with the network assumptions applied. The table presents the results of transitions of the terrorist hidden elements. The computation is done base on the fact that the probability of entry a certain state in Markov chain depends only on the immediate last state. This result shows a square matrix taking into cognizance the state dependence within the terrorist network. In network centrality, the importance score of a node (terrorist element) is the fraction of AIC made by the criminal element. It is assumed that all attacks are masterminded by the commander, thus having the highest centrality score of 269, followed by the gatekeeper with a centrality score of 263 and foot-soldier with 244. The result is used to compute the transition probabilities of the network in eq. 8 as a stochastic matrix. That is the matrix in which all the rows are nonnegative and all the rows sums up to 1.

Precisely the edge weights of the criminal network can be altered by changing the matrix appropriately [27].

Normalizing the rows of the network matrix and applying eq. 3 and eq.5, we obtained the result in eq. 8.

Table 2: Network Centrality Scores

State (i, j)	Cd	Gk	Fs	Total
Cd	6+19+244 = 269	19	0	288
Gk	19+244 =263	19+244 =263	244	770
Fs	0	244	244	488
Total				1546

$$p_{ij} = p\begin{vmatrix} 0.934 & 0.066 & 0 \\ 0.3416 & 0.3416 & 0.3168 \\ 0 & 0.5 & 0.5 \end{vmatrix} \quad (8)$$

The result shows that the conditional probability of an attack by a commander given that AIC is from the foot-soldier is 0 and conversely the same. This is because terrorist network maintained transitory shortcut to avoid been uncovered as communication between the leader and foot-soldier is completely avoided. The computation of the network adjacency matrix is done base on these analysis and is used to differentiate criminal network from social network. The network adjacency is computed using eq.7 and eq. 8.

$$a_{ij} = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} \quad (9)$$

It shows that the a_{ij} (adjacency matrix) of a criminal network has its leading diagonal elements as 1's and is a symmetrical matrix. This gives rise to the uniqueness of criminal network as this study set to identify. Here, both the upper and lower half of the matrix are the same. Social network has 0's along its diagonal since the ties of the social network actors with themselves are always ignored. An adjacency matrix of social network can be an asymmetric matrix or symmetric matrix. In asymmetric matrix the top right half of the diagonal does not match the bottom left half. Thus terrorist network exhibits these unique properties of symmetric and idempotent. Idempotent accounts for the resilience in every organized criminal network and confers its ability to reorganize or regroup after external attack.

V. CONCLUSION

The study applied Hidden Markov Model to computationally analyze the behaviors of Boko-Haram (BH) and Herdsmen with data-driven intelligence for the period of 2010 to 2016. It characterized the behaviors of terrorist elements within the context of their active internal communications, strategic operations and alliance. The network adjacency matrix computed from the network transition matrix shows that criminal network exhibits different features from social networks. The results illustrated the uniqueness of terrorist network in making incessant attacks while remaining resilient after every perturbation.

The study laid a good foundation to computational methods of counterterrorism and mathematical counterterrorism in the wake of the current terrorism globally.

REFERENCES

[1] S. Andrew *et al.*, "Lone-actor terrorism," in *Routledge Handbook of Terrorism and Counterterrorism*, 2018.

[2] Y. Gao, X. Wang, Q. Chen, and Y. G. et Al., "Suspects Prediction towards terrorist attacks based on machine learning," vol. 10, 2019.

[3] F. Ayoola, M. Adeyemi, and S. O. Jabaru, "On the Estimation of crime rate in the southwest of Nigeria: principal Content Analysis: Global Journal of science frontier research," *Glob. J. Sci. Front. Res.*, vol. 15, no. 2, pp. 2–4, 2015.

[4] E. Budur, S. Lee, and V. S. Kong, "Structural Analysis of Criminal Network and Predicting Hidden Links using Machine Learning," 2015.

[5] K. Taha and P. D. Yoo, "Using the spanning tree of a criminal network for identifying its leaders," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 2, pp. 445–453, 2017.

[6] J. Ogunleye, "The concepts of predictive analytics." *Int. J. Dev. Big data Anal.*, vol. 1, no. 1, pp. 86–94, 2014.

[7] L. M. Gerdes, "MAPPing dark networks: A data transformation method to study clandestine organizations," *Netw. Sci.*, vol. 2, no. 2, pp. 213–253, Aug. 2014.

[8] G. Marciani, M. Porretta, M. Nardelli, and G. F. Italiano, "A data streaming approach to link mining in criminal networks," in *Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017*, 2017.

[9] D. Uzlov, O. Vlasov, and V. Strukov, "Using Data Mining for Intelligence-Led Policing and Crime Analysis," in *2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings*, 2019, pp. 499–502.

[10] K. D. Maza, U. Koldas, and S. Aksit, "Challenges of Countering Terrorist Recruitment in," 2020.

[11] L. M. Gerdes, *Illuminating dark networks: The study of clandestine groups and organizations*. Cambridge University Press, 2015.

[12] P. J. Dey and S. Medya, "Covert networks: How hard is it to hide?," in *Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS*, 2019.

[13] T. P. Michalak *et al.*, "Computational analysis of connectivity games with applications to the investigation of terrorist networks," in *IJCAI International Joint Conference on Artificial Intelligence*, 2013.

[14] R. H. A. Lindelauf, P. E. M. Borm, and H. Hamers, "Understanding Terrorist Network Topologies and Their Resilience Against Disruption," *SSRN Electron. J.*, 2011.

[15] M. Franzese and A. Iuliano, "Hidden Markov Models," in *Encyclopedia of Bioinformatics and Computational Biology*, Elsevier, 2019, pp. 753–762.

[16] P. Saini and S. Godara, "Intrusion Detection System and Hidden Markov Models," vol. 4, no. 10, pp. 738–740, 2014.

[17] I. Visser and M. Speekenbrink, "Package 'depmixS4,'" *CRAN*. 2020.

[18] M. M. M. Farag, T. Elghazaly, and H. A. Hefny, "Face recognition system using HMM-PSO for feature selection," in *2016 12th International Computer Engineering Conference, ICENCO 2016: Boundless Smart Societies*, 2017.

[19] X. Yin *et al.*, "ARGs-OAP v2.0 with an expanded SARG database and Hidden Markov Models for enhancement characterization and quantification of antibiotic resistance genes in environmental metagenomes," in *Bioinformatics*, 2018.

[20] V. Raghavan, A. Galstyan, and A. G. Tartakovsky, "Hidden Markov models for the activity profile of terrorist groups," *Ann. Appl. Stat.*, 2013.

[21] S. S. Shuaibu and M. A. Salleh, "Historical Evolution of Boko Haram in Nigeria : Causes," *Proc. Icic 2015*, no. September, pp. 217–226, 2015.

[22] H. S. Bello, I. S. Galadima, and B. I. Aliyu, "An Assessment of the Effects of Boko-Haram Insurgency on Business Development

in North-Eastern States of Nigeria," *Bus. Ethics Leadersh.*, 2018.
[23] V. Le, "Organised Crime Typologies: Structure, Activities and Conditions." *Int. J. Criminol. Sociol.*, vol. 1, pp. 121–131, 2012.
[24] E. Farooq, S. A. Khan, and W. H. Butt, "Covert network analysis to detect key players using correlation and social network analysis," in *ACM International Conference Proceeding Series*, 2017.
[25] P. Seidler, J. Haider, N. Kodagoda, B. L. William Wong, M. Pohl, and R. Adderley, "Design for intelligence analysis of complex systems: Evolution of criminal networks," in *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, 2017.
[26] T. Xia and Y. Gu, "Building terrorist knowledge graph from global terrorism database and wikipedia," in *2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019*, 2019, pp. 194–196.
[27] D. Skillicorn, "Extracting Knowledge from Graph Data in Adversarial settings". In Memon. N., David F.Y., Hicks D.L., Rosenorn T. (eds) Mathematical methods in counterterrorism," *J. Comput. Anal. Appl.*, pp. 34–40, 2009.
[28] S. Argamon and N. Howard, *Computational methods for counterterrorism*. 2009.
[29] L. Nguyen, "Tutorial on Hidden Markov Model," *Appl. Comput. Math.*, vol. 6, no. 4, p. 16, 2016.
[30] G. Brogi and E. Di Bernardino, "Hidden Markov models for advanced persistent threats," *Int. J. Secur. Networks*, vol. 14, no. 4, pp. 181–190, 2019.