1st CoNIMS International Conference and Workshop

Digital Security Considerations for Development (DiSec 2018)

Conference Proceedings

COMPUTER NETWORKS, INFRASTRUCTURE MANAGEMENT AND SECURITY (CoNIMS)

Research Group, Department of Computer Sciences University of Lagos, Nigeria

1st CoNIMS International Conference and Workshop

Theme: Digital Security Considerations for Development

23 – 25th October, 2018

Arthur Mbanefo Digital Research Centre,

University of Lagos, Nigeria

Editor

Prof. Charles UWADIA

Table of Content

A Deep Learning Model for Predicting Multistage Cyberattacks (C001)

Ayei E. Ibor
Department of Computer Science
University of Calabar
Calabar, Nigeria
e-mail: ayei.ibor@gmail.com

Florence A. Oladeji, Olusoji B. Okunoye
Department of Computer Sciences
University of Lagos
Lagos, Nigeria

Abstract—The prediction of cyberattacks has been a major concern in cybersecurity. This is due to the huge financial and resource losses incurred by organisations after a cyberattack. The emergence of new applications and disruptive technologies has come with new vulnerabilities, most of which are novel – with no immediate remediation available. Consequently, recent attacks signatures are becoming evasive, deploying very complex techniques and algorithms to infiltrate a network perimeter, leading to unauthorized access and modification of system parameters and classified data. Although there exists several approaches to mitigating attacks in the public domain, challenges of using stored signatures of known attacks as well as modeled behavioural profiles of dynamic network environments still linger. One significant similarity among all available solutions is their reactive nature – only responding when an attack has occurred – for which most approaches are not feasible for the current sophistication of the attack surface. To this effect, this paper focuses on the use of a cascade of multiple layers of nonlinear processing components with unsupervised statistical analysis and supervised deep learning techniques to predict attacks by mapping hyper-alerts to class labels of attacks. This will enhance the processes of feature extraction and transformation, as a means of giving structured interpretation of the dynamic profiles of a network.

I. INTRODUCTION

There is a seeming expansion in the threat landscape with the emergence of new cyberattacks. As cyberattacks proliferate, including the new breed of zero day exploits and ransomware, more critical resources are compromised, lost and stolen while some are inadvertently divulged [1]. With the contents of critical data ranging from product patents, business and military intelligence, system parameters and configuration data, accounting reports, data from financial transactions, scientific and experimental data, it is likely that a well-organized cyberattack can create unprecedented overheads for an organization. Such overheads can have significant impact on available computing resources and infrastructure including but not limited to system breakdown, huge financial loses, and the unavailability of services.

, therefore, participates in the transformation of the feature space of the given attack dataset to choose the best features that will enhance the processes of feature extraction and transformation, as a means of giving structured interpretation of the dynamic profiles of a network. In this manner, diverse attack scenarios can be predicted by using labelled attack patterns (types), which correspond to different structured hyper-alerts. Further deviations from the labelled attack patterns can be flagged as new patterns to predict novel attacks.

II. ATTACK PREDICTION WITH ALERT CORRELATION AND CLUSTERING TECHNIQUES

Alert correlation is a multi-step process that analyses network events such as packets from disparate intrusion detection systems (IDSs), to generate a hyper alert that gives details of the state of the connections in a network. Intrusion detection systems (IDSs) are configured with predefined rules and profiles, which serve as preconditions for detecting the presence or absence of an anomalous traffic pattern. When an attack signature is detected, an alert is generated on the IDS indicating the type of attack vector identified.

An alert is basically a notification of the type of event detected on a network. These alerts, most of the time, can be false positives and false negatives, and as such misleading. With most IDSs depending largely on known attack signatures and network usage profiles, alert correlation provides a means of identifying and grouping similar patterns of alerts into attack steps. This process enhances the accuracy of clustering as posited by [9].

Several alert correlation techniques have been proposed by different authors over the years. In [10], an entropy-based alert correlation system called E-correlator is

While new paradigms such as the Internet of Things (IoT), Cyber Physical Systems (CPS), Cloud Computing, Blockchain Technology, Biohacking, Cybernetics, Wearable technology, to mention but a few, have come with new applications and vulnerabilities [2], [3], [4], [5], [6], [7], current cybersecurity approaches have found it difficult to cope with the new challenges posed by this advancement in technology and widespread digitalization of processes and functions. This has resulted in the difficulty to proffer a suitable model for predicting the likelihood of attacks in networks.

Similarly, the widespread acceptance of portable devices such as smart phones, which provide access to the Internet on the go, has come as a major concern for organisations, which rely on "bring your own device – BYOD" paradigm for operational efficiency [8]. With portable devices, the rate of malware spread becomes even easier and faster, leading to an increase in the attack surface. As the attack surface is increasingly expanding, more attack vectors become sophisticated, and as such, have been able to exploit the weaknesses of current detection and prediction approaches.

Computing processes are witnessing a new level of complexity and attack vectors are escalating in the context of the cyberspace. It is also not farfetched to assert that the interconnectedness of devices and systems has created a high caliber virtual proximity terrain from advancement in cyber physical systems. Such advancement also creates a plethora of vulnerabilities, which are likely to be exploited to stage attacks in the wild.

To address this concerns, this approach will use a deep learning model to learn multiple layers of representations, which map to different levels of abstraction. With the current sophistication of the attack surface, this representation will help to generate a cascade of concepts for interpreting different attack scenarios (existing and novel). In this context, the feature representation and transformation in the hidden layers of the model serve as inputs to the next layer. Every hidden layer

proposed to simplify the analysis of a large set of alerts in such a way that there is no information loss between the correlated and the original raw alerts. The E-correlator system takes raw alerts as input and generates a hyper-alerts graph as output. This process is achieved with the use of the density-based spatial clustering of applications with noise (DBSCAN) algorithm.

A structural-based alert correlation underpinned by feature selection using information gain is discussed in [9]. This approach was focused on the selection of precise and significant features of alerts. The authors claim that such selection is a representative of the apposite attack steps in order to improve the clustering accuracy of the proposed model.

An anomaly based network intrusion detection characterised by feature correlation analysis is proposed in [11]. The proposed approach uses a heuristic technique for anomaly based intrusion detection by defining a scale that helps to ascertain the significance of the network transaction in order to extract features, enforce dimensionality reduction, and maximize feature selection based on the criteria for classification.

An alert correlation system that is used to analyse DDoS attacks is proposed in [12]. The model attempts to minimize the volume of low-level alerts in a bid to generate hyper-alerts. These hyper-alerts form the basis for identifying complex attack strategies in a multistage attack scenario using correlation at different levels of abstraction and time points. Low level alerts are categorized based on similarity with the help of a clustering algorithm to generate hyper-alerts, which are in turn correlated to find the attack graph.

In [13], an intrusion alert correlation technique for managing security incidents is given. The technique deploys two components namely offline and online correlators respectively. The offline correlator is responsible for the aggregation of historical events that constitute alerts from an intrusion detection system (IDS) with the help of the connected component method. It also extracts and hierarchically clusters similar attack strategy graphs in order to classify the attack features of each generated cluster.

Although alert correlation approaches have been used in an attempt to detect attacks, most of these approaches are based on the manual analysis of log files with no hidden layers of feature representations for predicting attacks.

III. Understanding Deep Learning For Network Attack Prediction

Deng and Yu in [14] posit that deep learning is a machine learning approach that relies on several layers of non-linear information processing to perform supervised or unsupervised feature extraction and transformation as well as pattern recognition. Deep learning also performs the classification of instances given an input dataset. Similarly, [15] and [16] state that deep learning is characterised by several architectures including deep neural networks, deep belief networks, as well as recurrent neural networks).

Most applications of deep learning have been in the field of computer vision, speech recognition, natural language processing, the design of drugs, audio recognition, machine translation, to mention but a few. With deep learning models loosely depicting the processes of biological neurons, they have found relevance in information processing and communication patterns [17], [18], [19], [20].

Deep learning models have multiple hidden layers of feature representation from the given input data. At each layer, there is a transformation of the input data, resulting in a fixed abstract and compressed representation of the data. Through this process, the model can learn the features to optimally choose within each layer to enhance its output. Transforming the data through several layers implies a significant credit assignment path (CAP) depth, which describes the chain of transformations from the input to the output, and can also describe the casual connections between the input and output data [21], [22].

LeCun et al in [15] describes feedforward and recurrent neural networks as common models of a deep learning process, and can be constructed with a greedy layer-by-layer approach such that it is possible to select the features, which improve the performance of the model from each layer in a supervised or unsupervised learning process. It is important to note that all data can be represented in the same format for computing processes using text and numbers, in which case, deep learning can find application in the prediction of multistage cyberattacks given a dataset of intrusions. This can be achieved by superimposing the attack datasets on deep learning models such as deep neural networks, deep belief networks and recurrent neural networks [15], [21].

IV. Methodology

This research uses a novel approach to predict the likelihood of an attack in a controlled network environment. The approach exploits the power of unsupervised statistical analysis and supervised deep learning techniques to derive a hybrid model that is able to build attack tracks relevant for predicting future attacks given an alert space (a_{Δ}).

At the initial stage, the alert space is normalized using Principal Components Analysis (PCA) to remove noise from the raw alerts in a process called dimensionality reduction. The choice of (PCA) is based on the need to use a fewer number of instances to train the model given a large dimensionality space of the dataset with respect to the output required. Similarly, the use of (PCA) will help to enforce the automatic selection of the best features required to achieve a very high prediction accuracy without necessarily relying on explicit feature selection.

The application of (PCA) on the raw dataset creates an alert subspace $(a_u) \leq (a_{\Delta})$ that contains only the relevant features needed for creating clusters. Similarly, the use of principal components will help the model to learn the

prediction of an attack given a compressed representation of the dataset for a given timestamp (t).

The normalized dataset is then filtered using unsupervised attribute based principal components to generate a set of k hyper-features (hyper-alerts). The k hyper-features are identified based on a class label for the supervised classification of the instances using deep learning multilayer perceptron classifier. The k hyper-features are then used as training samples for the model. At the completion of the training phase, the model is fed with test data to predict the classification of the attack labels.

A. The Proposed Model

The architecture of the proposed model is depicted in Figure 1. In Figure 1, a data stream consisting of IDS alerts generated at disparate sensors are captured into an alert database. The alerts are normalized and filtered to remove noise from the dataset through unsupervised attribute-based dimensionality reduction. The new dataset with labelled hyper-alerts, is matched to labelled outputs in the supervised deep learning module. This allows the model to accurately learn and predict existing and novel attacks. The identified attacks are reported and new attack instances stored for future inference. The formal description of the model is presented in subsequent sections.

B. Modeling Alert Correlation and Clustering

Alert correlation captures the casual relationship between alerts, thereby generating a high level view of the attack scenario using the analysis of the relationship between the causes and consequences of an attack. Kawakani et al in [13], Alsmadi et al in [23], and Ahmed and Zaman in [24] assert that creating a sequence of alerts helps to establish attack tracks, which trace the source and plan of the attack. Additionally, in [9] and [10], it is posited that in correlating alerts, there is always the likelihood of information loss when aggregating the raw alerts. To solve this problem, hyper-alerts can be generated, which cluster raw alerts into logical components based on casual relationships.

1) IDS Raw Alerts

Every IDS is configured with rules and profiles to detect the presence of anomalous traffic. Anomalous traffic is network packets that may have signatures of known attacks, and as such is considered to meet some of the preconditions of an attack vector. When such packets are detected by an IDS, a message or notification called an alert is triggered. These raw alerts are stored in an alert database, and may include a collection of false positives. Raw alerts are usually aggregated from different IDS sensors across the network, and may not convey any form of meaning required to trace an attack source.

Let us consider disparate IDS sensors,

$$S_i, (1 \leq i \leq n) \quad (1)$$

(1)

where n is the number of IDS sensors monitoring a network, each S_i can generate a high amount of alerts, say,

$$a_x, (a_x | \int x) \quad (2)$$

depending on the state of the network. For each a_x in S_i, an $\lfloor n \quad x \quad m \rfloor$ matrix can be generated depicting the alert sequence from different sensors. These alert matrices are stored in an alert database, and can be correlated by constructing hyper-alerts using similarity measures defined as an n-tuple comprising a feature space of *n-features defined as* $\{f_1, f_2, \ldots, f_n\}$. By aggregation of parameters, we denote an alert by,

$$a_x = (\langle f_1, f_2, \ldots, f_n \rangle | \int x) \quad (3)$$

such that for each *x*, the value of a_x, grows incrementally as low level alerts are captured by different sensors until a threshold (T) is reached. When two alerts demonstrate a certain level of acceptable similarity rate, then a value of 1 is returned. A value of 0 implies that two alerts are not similar. That is;

$$\{a_x, a_{x+1}\} = \begin{cases} 1, & if\ (a_x = a_{x+1}) \\ 0, & otherwise \end{cases} \quad (4)$$

The representation of an alert sequence is shown in Figure 2.

to learn low-dimensional representation very similar to the

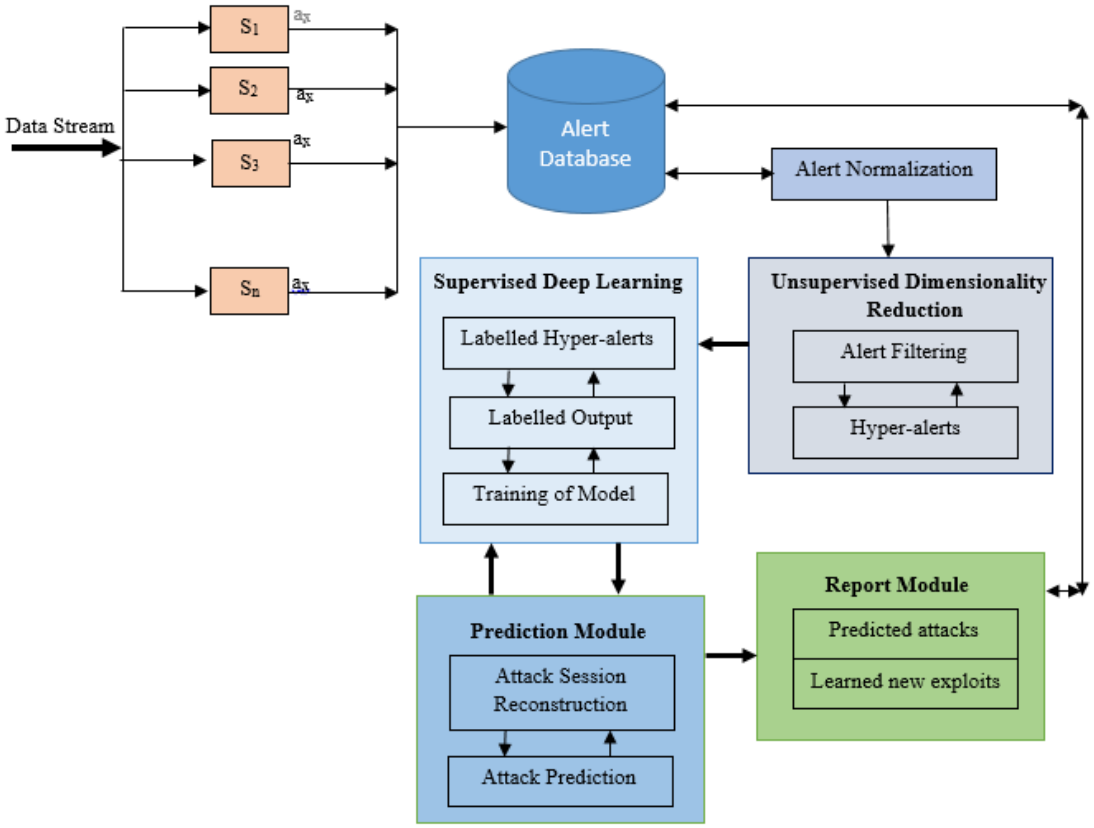

Figure 1. Architecture of the Proposed Approach

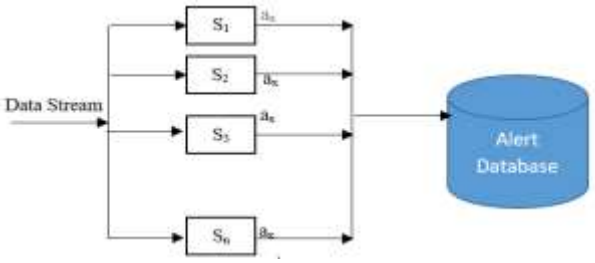

Figure 2. An Alert Sequence captured and stored in a Database

2) Alert Normalisation

Alert normalization involves the process of removing noise in the dataset. To normalize a given dataset (with noise) at the early stage of alert collection from the IDS sensors, PCA is used. PCA basically compresses the feature space, which serves as the input into a latent-space representation [25]. With the approach considering the correlation of alerts, the use of PCA will be helpful in discovering the correlations in the dataset given *p* variables and *n* instances, and orthogonally transforming them into a few uncorrelated principal components. These principal components retain the variations in the dataset and are used original feature space [26].

Given an original dataset with a number of instances, say *n*, and *p* variables, PCA generates $\min(n-1, p)$ distinct principal components from which the target output can be reconstructed. In this way, a large dataset can be easily represented by projecting it on more than a one dimensional vector [27]. The transformed low-dimensional representation is based on the preservation of the variance of the dataset based on the ranking of the principal components. That is, the first principal component contains the largest possible variance, and this threshold decreases with each succeeding principal component.

In the modeled dataset, a threshold of 0.5 is used on a subset of features to search for the principal components relevant for expressing the variability in the data. Let us consider a set of *p*-dimensional variables depicting vectors of weights w_j defined as:

$$w_j = \left(w_1, w_2, \ldots, w_p\right)_j \quad (5)$$

Assuming each of these weights are mapped to each row vector, say, b_k in the feature space, to obtain a new vector of principal component scores y_k, given by:

$$y_k = (y_1, y_2, \ldots, y_m)_k \quad (6)$$

Then,

$$y_{jk} = b_k \,.\, w_j \,; 1 \leq k \leq n, 1 \leq j \leq m \quad (7)$$

For each individual variable y_k considered over the dataset, $y_k \in y$ consecutively inherits the maximum possible variance from *b*, with the $coefficinet\ vector\ (w) \equiv unit\ vector.$ Furthermore, the first principal component must have its coefficient vector satisfying the following relation:

$$w_1 = \underset{\|w\| = 1}{argmax} \{\sum_k (y_1)_k^2\} \quad (8)$$

Equivalently, using the definition of y_{jk} in equation (8), then we will have:

$$w_1 = \underset{\|w\| = 1}{argmax} \{\sum_k (b_k \,.\, w)^2\} \quad (9)$$

We can achieve the value of subsequent i^{th} components by reducing the data matrix, B (having column-wise zero empirical mean) with the first $i = 1$ principal components.

3) Formal Description of Alert Clusters

Clustering is a technique used to aggregate data into groups that share similar characteristics using a specific criteria [9], [13], and [28]. Alerts captured from an IDS sensors can be clustered to divulge the hidden patterns in the low level alerts towards correlating the alerts and also, to reduce the alert count, given an enormous alert space.

IDS sensors can generate multiple alerts across the network, and such alerts, which can be stored as $\lfloor n \quad x \quad m \rfloor$ matrices for each S_i, will be difficult to correlate without creating clusters, which reduce the alert count in relation to the number of clusters created. Given an alert count, say, *count*, for some alert space; a_Δ, defined as:

$$a_\Delta \lfloor count \rfloor = \sum a_x \quad (10)$$

and an alert cluster; a_p, denoted by:

$$a_p = [\![\cup a_x \in a_\Delta \lfloor count \rfloor : (\{a_x, a_{x+1}\} = 1)]\!] \quad (11)$$

then,

$$a_p[k] < a_\Delta[count], for\ some\ k, where\ k\ is\ a\ cluster\ descriptor \quad [12]$$

4) Hyper-alert Construction

Low level or raw alerts captured by IDS sensors can be enormous, and one way to reduce the number of these alerts in order to generate attack tracks for tracing the source and plan of the attack is to use hyper-alerts. In [12] and [29], it is affirmed that hyper-alerts are useful for identifying complex attack strategies in a multistage attack scenario. The correlation of these hyper-alerts at different levels of abstraction and timestamps is targeted at establishing the casual relationships between alerts in order to recreate an attack scenario from the point of initiation to its actualization.

Considering an alert sequence, say, $a_{x+1}, a_{x+2}, \ldots, a_k, \ldots, a_{x+k}$, for some arbitrary value of *k*, depicting the alert count, a hyper-alert is generated through alert clustering. A hyper-alert will be defined mathematically as follows:

$$\bar{a} = \cup_k a_p \quad (13)$$

A hyper-alert is a high level alert structure representing a cluster of alerts correlated based on similar characteristics. A collection of the reconstructed hyper-alerts from the given dataset constitute the hyper-alert space denoted by:

$$\bar{A}_\theta = \cup \bar{a} \quad (14)$$

V. Theoretical Formulation Of The Proposed Model

The model will use supervised deep learning implemented through a deep learning multilayer perceptron classifier (deep neural network) to reconstruct the attack types from a given hyper-alert space, $\bar{A}_\theta$ in the dataset with the application of backpropagation. This follows that the model will set the target labels (in this case, the attack types) to be equal to the inputs. That is, given an attack type, say, T_i, and an hyper-alert space, $(\bar{A}_\theta)$, with *i* hyper-alerts, the model computes:

$$T_i = \bar{a}_i \in \bar{A}_\theta \quad (15)$$

where each hyper-alert represents a reconstructed attack type using the generated alert clusters in equation (11).

In the process of identifying an attack type, T_i, the model learns the function:

$$f(\bar{a}) = \max(\bar{a}, 0) \quad (16)$$

such that the output is 0 for $\bar{a} < 0$, otherwise the output is equal to the input, which is an approximation to the identity function. This will allow the model to output T_i that is equivalent to $\bar{a}_i \in \bar{A}_\theta$. Learning the identity function can be enhanced with the use of constraints on the network.

These constraints can include placing a limit on the number of hidden layers that represent a cascade of concepts for developing feature representations, which can discover patterns in the data for predicting multistage attacks. The function in equation (16) thus represents a rectified linear unit (ReLU) [30].

Rectified linear units (ReLU) are used in the hidden layers of the model. These hidden layers are defined as dense layers with a specific number of units (neurons). The number of units (*N)* is computed as follows:

$$N = \left\lfloor \sqrt{n(\bar{A}_\theta).n(T_i)} \right\rfloor \quad (17)$$

where; $n(\bar{A}_\theta)$ is the number of inputs in the feature space, and $n(T_i)$ is the number of expected outputs. At the hidden layers, the network can learn a compressed representation of the hyper-alert space $(\bar{A}_\theta)$. This compressed representation is classified with the softmax function at the output layer. In solving classification problems, the softmax function partitions the output such that the total sum is 1, which is equivalent to a categorical probability distribution. Assuming we have *i* output units $(1 \leq i \leq n)$ for a given number of input vectors, say, *h (h =* $\bar{A}_\theta$*)*, then the softmax function achieves classification as discussed in [30] using :the function in equation (18).

$$\grave{T}\ (h)_i = \frac{e^{h_i}}{\sum_{i=1}^{n} e^{h_i}} \quad (18)$$

with $\grave{T}$ as the predicted class.

We implement the deep learning model using a feed forward neural network (FFNN) with $(n+1), 0 \leq n \leq 2$ hidden dense layers of size *N*, and one (1) output layer of size 5 (representing the number of outputs in the modeled dataset). The hidden dense layers are configured with ReLU as the activation function while the output layer uses the softmax function for classification with a standard categorical cross-entropy loss function. The default dropout value of 0.0 is used at the dense layer to avoid under-fitting. An initial learning rate of 0.1 is applied.

The FFNN is optimized using stochastic gradient descent algorithm with an Adam updater $\left(\begin{matrix}\beta_1 = 9\,x\,10^{-1}, \beta_2 = 999\,x\,10^{-1}; \\ \beta_1 \textit{ is mean decay}, \beta_2 \textit{ is variance decay}\end{matrix}\right)$ and Xavier weight initialization [31], [32].

VI. TESTBED OF THE PROPOSED MODEL

The model is implemented using WEKA (Waikato Environment for Knowledge Analysis) and MATLAB. The experimentation involves processes comprising data preparation, attribute selection, and classification of the dataset. The system properties of the machine used for conducting the experiments are as shown in Table I.

TABLE I. SYSTEM PROPERTIES OF THE IMPLEMENTATION MACHINE

Host Operating System	Microsoft Windows 10
Processor	Intel ® Core ™ i3 6100U CPU @2.30 GHz 2.30GHz
RAM	4.00GB
System Type	64-bit Operating System, x-64 based processor
Virtualization	Oracle VM VirtualBox Manager
Guest Operating System	Lubuntu Operating System, 64-bit

A. Data Preparation

The NSL-KDD dataset with 41 features and a large number of connection vectors labelled as either normal or a specific attack type is used for the experiments. The dataset is an enhanced and reduced version of KDDCup'99 dataset with 22 attack types in the training set and 37 attack types in the test set classified as one of the following; probe, denial of service (dos), remote to local (r2l), and user to root (u2r) attacks [33]. Twenty percent (20%) of the original NSL-KDD dataset is used as the training set with 25, 192 connection vectors summarized in Table II.

TABLE II. SUMMARY OF THE NUMBER OF CONNECTION VECTORS USED FOR TRAINING THE MODEL

Connection Vector	Number of Instances	% of Total
Normal	13, 449	53.39
Denial of Service (DoS)	9,234	36.65
Probe	2,289	9.09
Root to Local (R2L)	209	0.83
User to Root (U2R)	11	0.04
Total	25, 192	100.00

B. Feature Ranking

The model was trained using 29 principal components extracted from the set of 41 features in the NSL-KDD dataset. The 29 principal components (considered as hyper-features or hyper-alerts in this case) are selected using PCA and ranked based on a threshold of 0.5. The choice of PCA was necessitated by achieving dimensionality reduction to have a compressed feature space from which the model can learn (Vasan and Surendiran, 2016).

With deep learning being able to perform optimally with a few features, PCA enhanced the selection of the features that contribute to representing the internal structure of the data to optimize the variance in the data. This gave the representative subset of features for training the model.

To improve the predictive ability of the model, the full training set is used during the training process to evaluate the feature space. This gives an insight into the model's ability to generalize to an unknown dataset while deriving an accurate estimate of model prediction performance.

C. Performance Metrics

The performance of the model is evaluated using the following metrics as highlighted in [34]:

- **True Positive Rate (TPR):** the rate of instances of attacks or normal connections predicted correctly.
- **False Positive Rate (FPR)**: the rate of instances of attacks predicted as normal connections or vice versa.
- **Precision Rate (PR)**: the fraction of relevant instances in the dataset
- **Recall Rate (RR)**: the retrieved relevant instances over the total amount of relevant instances
- **F-Measure (F-Score)**: a measure of the accuracy of the model computed as the weighted harmonic mean of the precision and recall of the model.

D. Experimental Results and Discussion

The model is trained using a minimum of 500 epochs with an early stopping constraint of 200 epochs. The summary of the model performance for the 5 class labels (normal, dos, probe, r2l, and u2r) is shown in Table III.

TABLE III. PERFORMANCE METRICS OF THE PROPOSED MODEL FOR 5 CLASS LABELS

	Normal	**DoS**	**Probe**	**R2L**	**U2R**
TPR	1.000	0.876	0.848	0.001	0.001
FPR	0.146	0.000	0.000	0.000	0.000
PR	0.887	1.000	1.000	0.000	0.000
RR	1.000	0.876	0.848	0.000	0.000
F-Measure	0.940	0.934	0.918	0.000	0.000

We plotted the precision recall graph using the data in Table III. This graph is used to validate the model's stability while predicting the relevant attack types. The precision rate (PR) is plotted on the x-axis against the recall rate (RR) on the y-axis. As illustrated in Figure 3, the model performed well for predicting the labelled normal connection and attack types.

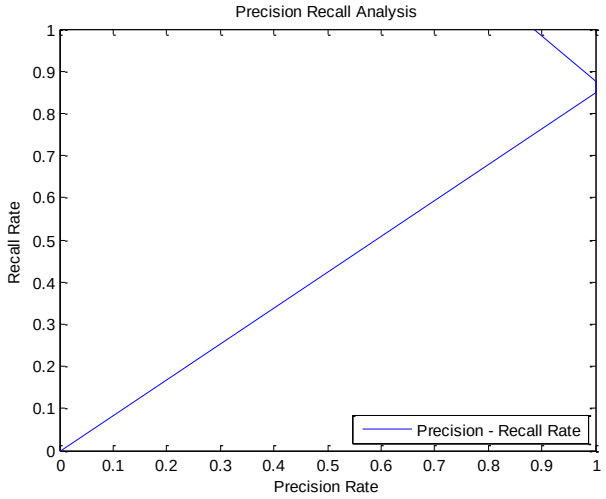

Figure 3. Precision Recall Analysis

Similarly, Figure 4 shows the Receiver Operating Characteristic (ROC) Analysis, which is used to estimate the cost and benefit analysis of the model. We achieve ROC by plotting the False Positive Rate (FPR) against the True Positive Rate (TPR) using the data in Table III [34]. The area above the curve represents a good prediction rate for the proposed model.

Other performance metrics of the model are indicated in Table IV.

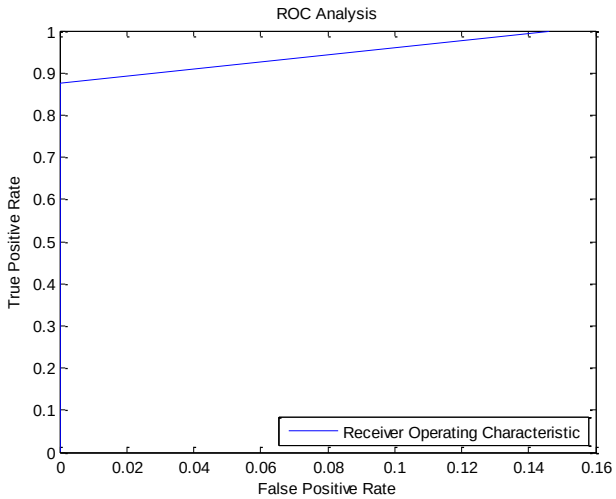

Figure 4. ROC Analysis

TABLE IV. KAPPA STATISTIC AND ERROR RATES

Metric	Value
Kappa statistic	0.8774
Mean absolute error	0.0412
Root mean squared error	0.141
Relative absolute error	17.98%

The error rates are relatively low and a Kappa Statistic of less than 1 indicates good performance.

VII. CONCLUSION

This paper proposes a model for predicting cyberattacks using a deep learning process. The model incorporates such modules as alert normalization, dimensionality reduction, prediction and reporting using unsupervised feature filtering with PCA and supervised deep learning techniques for prediction of attack types. The choice of both supervised and unsupervised methods is significant for constructing hyper-alerts (hyper-features with PCA), which can be mapped to labelled classes of attacks, with the added advantage of defining new classes of attacks as the model learns non-linear representations of the feature space.

The model was trained on the full training set and predicted more accurately existing and novel attacks using its hidden layers of compressed feature representations to learn, and reconstructing the attack class in the output. In this process, attack prediction is improved significantly. However, we hope to improve the prediction of R2L and U2R attacks in further research by adding more connection vectors of these attacks to the training set as there are only 0.87% (see Table II) of instances of these attacks used.

For future research, we intend to test the model with varying number of connection vectors as well as different thresholds for extracting the principal components that best depict the variability in the modeled data set for optimal performance.

REFERENCES

[1] A. E. Ibor, "Zero day exploits and national readiness for cyber-warfare," Nigerian Journal of Technology, vol. 36(4), 2017, pp.1174-1183.

[2] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets". arXiv preprint arXiv:1702.03681.

[3] 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 of Things Journal, vol. 4(5), 2017, pp.1125-1142.

[4] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," IEEE Internet of Things Journal, vol. 4(6), 2017, pp.1802-1831.

[5] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, 2017, pp.30-48.

[6] I.C. Lin and T.C. Liao, "A survey of blockchain security issues and challenges," IJ Network Security, vol. 19(5), 2017, pp.653-659.

[7] J. Liu and W. Sun, "Smart attacks against intelligent wearables in people-centric internet of things," IEEE Communications Magazine, vol. 54(12), 2016, pp.44-49.

[8] B. Leonard and M. Dawson, "Legal issues: Security and privacy with mobile devices," In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018, pp. 1352-1361.

[9] T.A. Alhaj, M.M. Siraj, A. Zainal, H. T. Elshoush, and F. Elhaj, "Feature selection using information gain for improved structural-based alert correlation," PloS one, vol. 11(11), 2016, p.e0166017.

[10] M. GhasemiGol and A. Ghaemi-Bafghi, "E-correlator: an entropy-based alert correlation system," Security and Communication Networks, vol. 8(5), 2015, pp.822-836.

[11] V. Jyothsna and V. R. Prasad, "FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale," ICT Express, vol. *2*(3), 2016, pp.103-116

[12] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "An alert analysis approach to DDoS attack detection," In Accessibility to Digital World (ICADW), 2016 International Conference, 2016, pp. 33-38. IEEE.

[13] C. T. Kawakani, S. B. Junior, R. S. Miani, M. Cukier, and B. B. Zarpelão, "Intrusion alert correlation to support security management," In XII Brazilian Symposium on Information Systems-Information Systems in the Cloud Computing Era, 2016, pp. 313-320.

[14] L. Deng and D. Yu, "Deep learning: methods and applications," Foundations and Trends® in Signal Processing, vol. 7(3–4), 2014, pp. 197-387.

[15] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning. *nature*, vol. *521*(7553), 2015, pp. 436.

[16] J. Schmidhuber, "Deep learning in neural networks: An overview," Neural networks, vol. 61, 2015, pp. 85-117.

[17] K. Noda, Y. Yamaguchi, K. Nakadai, H. G. Okuno, and T. Ogata, "Audio-visual speech recognition using deep learning," Applied Intelligence, vol. 42(4), 2015, pp. 722-737.

[18] G. Litjens, T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, and C. I. Sánchez, "A survey on deep learning in medical image analysis," Medical image analysis, vol. 42, 2017, pp. 60-88.

[19] S. Min, B. Lee, and S. Yoon, "Deep learning in bioinformatics,". Briefings in bioinformatics, vol. 18(5), 2017, pp. 851-869.

[20] B. R. Kiran, D. M. Thomas, and R. Parakkal, "An overview of deep learning based methods for unsupervised and semi-supervised anomaly detection in videos," Journal of Imaging, vol. 4(2), 2018, pp. 36.

[21] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," Neurocomputing, vol. 234, 2017, pp. 11-26.

[22] F. Chollet. Deep learning with python, Manning Publications Co., 2017.

[23] I. M. Alsmadi, G. Karabatis, and A. Aleroud, eds., Information fusion for cyber-security analytics, Springer International Publishing, 2017.

[24] A. A. Ahmed and N. A. K. Zaman, "Attack intention recognition: A Review," IJ Network Security, vol. 19(2), 2017, pp. 244-250.

[25] K. K. Vasan and B. Surendiran, "Dimensionality reduction using Principal Component Analysis for network intrusion detection," Perspectives in Science, vol. 8, 2016, pp.510-512.

[26] I.T. Jolliffe and J. Cadima, "Principal component analysis: a review and recent developments," Philosophical

Transactions of the Roval Society of London Series A vol. 374(2065), 2016, pp. 1-16.

[27] E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto, "PCA filtering and probabilistic SOM for network intrusion detection," Neurocomputing, vol. 164, 2015, pp.71-81.

[28] A. B. Mohamed, N. B. Idris, and B. Shanmugum, "An operational framework for alert correlation using a novel clustering approach," International Journal of Computer Applications, vol. 54(12), 2012, pp. 23-28.

[29] R. Shittu, A. Healing, R. Ghanea-Hercock, R. Bloomfield, and M. Rajarajan, "Intrusion alert prioritisation and attack detection using post-correlation analysis," Computers & Security, vol. 50, 2015, pp.1-15.

[30] A. F. Agarap, Deep Learning using Rectified Linear Units (ReLU), arXiv preprint arXiv:1803.08375, 2018.

[31] S. Ruder, An overview of gradient descent optimization algorithms, arXiv preprint arXiv:1609.04747, 2016.

[32] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," In CVPR, vol. 1(2), 2017, pp. 4700-4708.

[33] L. Dhanabal and S. P. Shantharajah, "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4(6), 2015, pp.446-452.

[34] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," ACM Computing Surveys (CSUR), vol. 48(1), 2015, pp.12:1-12:41.

Real-Time Mobile Health System for Remote Consultations

(C002)

Olutunbosun Olabode[1], Oladunni Daramola[2], Racheal Akinbo[3]
Computer Science Department
Federal University of Technology
Akure, Nigeria.
oolabode@futa.edu.ng [1], oadaramola@futa.edu.ng [2], racheal.akinbo@gmail.com[3]

***Abstract*—Health Care System is one of the most important dependencies for life sustainability and growth of a country. Mobile technologies for health care services offer a tremendous opportunity for developing countries through provision of remote medical consultations. The challenges in our health system serve as the motivation for this research. This research is therefore focused on the development of a Real-Time Mobile Health system that can be used by health providers and patients to provide medical consultations remotely with instant feedback based on android mobile phone. The Application incorporates chatting between patients and the health providers. Agile Software development life Cycle is employed. The implementation was carried out using Extensible Mark-Up Language (XML), Java Programming language and Android Studio with Android 7.0 Naugaut for the client-side while MySQL database with Django as the web framework and Anaconda as the interpreter at the server-side. To evaluate the usability and functionality of the system; the application was installed on the mobile phone of some selected people. Questionnaire method of data collection was employed, and Descriptive Statistics was used to analyze the data collected. The result of the evaluation shows that the application was rated positively and the average score from the users reached 95% Confidence Value.**

Keywords- Remote Consultations, M-health, Real-Time, Android-Phone, Doctor-Patient Interaction.

I. INTRODUCTION

The proliferation of mobile phones in the developing world has been both rapid and remarkable due to fact that global mobile phone consumption is high, with nearly 7 billion cell phone subscriptions and an estimated 96% mobile penetration in the world in 2014 [1]. This is evident according to World Bank Group report [2], that mobile device have reached more people in many developing countries than power grids, road system, water works or fibre optic networks. Therefore, a technology which would allow doctors to patients consultations remotely will therefore be of good use to the doctors and the patients. Remote consultation for outpatient defines the distant consultation for patient that is in a remote site. The remote site may be at the comfort of their house or any available place in which the services are needed without being to the hospital [3].

A. Real-Time System

In computer science, real-time computing (RTC), or reactive computing describes hardware and software systems subject to a "real-time constraint". Real-time programs must guarantee response within specified time constraints, often referred to as "deadlines". Real-time responses are often understood to be in the order of milliseconds, and sometimes microseconds [4].

A real-time system has been described as one which "controls an environment by receiving data, processing them, and returning the results sufficiently quickly to affect the environment at that time. The term "real-time" is also used in simulation to mean that the simulation's clock runs at the same speed as a real clock, and in process control and enterprise systems to mean "without significant delay"[5].

B. Mobile Health

Mobile-Health (m-Health) is a subset of e-Health that focuses on the delivery of health care services via mobile communication devices [6]. M-Health broadly encompasses the use of mobile telecommunication technology within health care delivery systems. In WHO's report [7], m-Health was defined as medical and public health practice supported by mobile devices, including mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. It focuses on the use of mobile phones (both simpler phones capable only of voice and text message communication and smartphones with many other capabilities, including access to websites and application software known as "apps" [8].

C. E-Health

E-Health (or electronic health) is broadly defined by the World Health Organization as the "use of information and communication technology for health" [9]. The main objective of e-Health programs is to use Information and Communication Technology (ICT) to improve healthcare service delivery and health outcomes through the strategic use of technologies such as:

a. Computers
b. Internet satellite receivers
c. Mobile phones
d. Personal Digital Assistants (PDA).

In addition the expansion and enhancement of wireless networks throughout low and middle income countries will increase access and capabilities of these technologies to healthcare providers and the general public in more remote geographical locations. The objective of this work is to develop a real-time mobile health system for monitoring and management of out-patient for remote consultations.

II. LITERATURE REVIEW

In 2009, the use of mobile telephone in reducing pre-natal maternal mortality for Abiye safe motherhood in Ondo State is presented. The motivation comes from the need to use mobile telephone to manage maternal mortalities resulting from childbirths. The objective was to reduce the maternal mortality rate by 75% by 2015. Short Messages Service (SMS) for push notification were used. The results shows that about 47% reduction of maternal mortality, an increase of 58% of registered patient and an increase of 96% of the number of live births in Ifedore and Idanre LGA were generated [9,10]. The limitation is that the timely delivery of notification messages was not considered.

In 2011 Dakoza mobile phone monitoring system for disease management was developed. The research was motivated by the need to improve communications between the different players in the health network and to improve the health status of patient. The objective of the research was the need to fast-track and improves critical services for HIV and TB patients. SMS/MMS based system was developed which includes auto-reminders of next appointments. The result shows an increase in patient compliance [11]. The limitation is that the system does not allow instant feedback.

A mobile phone intervention for the management of depression and Autism is proposed by Chen *et.,al*. The research was motivated by the need to reduce adolescence psychiatry. The objective is to explore the utility of text message interventions. Text-messages were deployed. The result shows that daily messages constituted the perfect amount of contact and improved patient communication with providers [12]. The limitation of the system is that text messages should not be the only benchmark for intervention in adolescent psychiatry.

Ran Wei and Zhimin Yang (2012) developed a system on Doctor-Patient Interaction based on Android mobile technology was developed. The motivation arises from the need to have a convenient and urgent means of communication between doctors and patients. The objective was to develop a doctor to patient interaction system using Android mobile phones. The design implements an e-mail system on Android platform. Embedded database system (SQLite) was used [13]. The result shows that the need for protocol conversion was reduced but communication exists in non-real-time mode.

A research work on Android Mobile Application Platform for Remote Medical Monitoring System is developed by Ziyu *et.,al* (2015). The research was motivated by the need to get more health care and doctor's professional advice when patients feel unwell. The objective is to build a remote medical monitoring system using Android mobile terminal for remote data acquisition, medical data analysis with push notifications. The research work employed development tools and application such as Google cloud messaging for push notification and Android platform on Bluetooth BLE technology, Java programming for the API, C++ for the library, MySQL for the database. The result show that the system compared with traditional medical monitoring system, significantly reduced medical resource inputs, making health care more efficient and practical [14]. The push notification messages are delivered at will and not as instant messages with no feedback. This research is therefore motivated by the need to overcome the stated limitations by developing a real-time mobile health system that can be used by health providers and patients to provide medical consultations remotely with instant feedback.

III. RESEARCH METHODOLOGY

The development of Real-Time Mobile Health application for the monitoring and management of patients is divided into two: the Android Application Design and the Database Design. The application is developed using Android Studio 2.3.3.

IV. SYSTEM FEATURES

The development of real-time mobile health application for the monitoring and management of patients incorporates the following:

- Electronic Medical Records
- Chatting
- Video Recording
- Medical Images
- Drug- Prescription
- Data transmissions include files, images and videos.

D. Software Development Method

The Agile software development is a combination of iterative and incremental process model with focus on product adaptability and satisfaction. Agile software development life cycle for mobile applications was adopted. It comprises the planning, requirement analysis, design and Testing phase. Agile methods break the product into small incremental builds (Remote Clinical Consultations Users) which are provided in iterations for functional activities and it was developed with the view of some users. The build is divided into six stages of application package kit (.apk) as follows:

- Administration *.apk*
- Doctor *.apk*
- Nurse *.apk*
- Medical Scientist *.apk*
- Pharmacist *.apk*
- Patient .apk

At the end, the *apk* was merged as one, except the admin *apk.*

E. Database Design

The database model of the clinical consultation system is presented. The MySQL data model is adopted which is of the family RDBM. Data for the Remote Clinical Consultation Application is organized into table structures. It is composed of 12 relations. The sets of relations supported in the proposed applications are given as:

- CHAT-TABLE [Id: patient_Id: doctor_Id: clinic_id: nurse_id: datetime: message]
- PATIENT [Id: Name: password: phone_number: email: profile_photo]

- HOSPITAL [hospital_Id: hospital_name: password: hospital_thumbnail_image: address: hospital_type: call_line]
- PHARMACY [Id: pharmacy_name: address: owner: pharmacy_thumbnail_image: call_line]
- PATIENT_CARD [address: date_of_birth: state_of_origin: local_goverment_area: home_town: next_of_kin: gender: blood_group :height: weight: genotype: patient_Id: patient_name: medical_images]
- MEDICAL_LAB [Id: Lab_name: address: owner: lab_thumnail_image: call_line]
- DOCTOR_DETAILS [Id: name: phone_number: specialities: year_of_experience: email: doctor_profile_photo :hospital_Id]
- NURSE_DETAILS [Id: name: phone_number: specialities: year_of_experience: email: nurse_profile_photo: hospital_Id]
- PATIENT_DOCTOR_CONSULTATION [Id: patient_card: diagnosis: treatment_prescribed: doctor_Id_assigned: amount_charged]
- PHARMACY_PATIENT_BILL_RECORDS [id: pharmacist_Id_assigned: amount_charged: amount_paid: patient_Id: pharmacy_Id: payment_type]
- LAB_PATIENT_BILL [Id: test_done: patient_card_no: treatment_prescribed: Lab_scientist_Id_assigned: amount_charged: patient_Id: lab_Id: payment_type]
- TRANSACTION [patient Id: doctor_Id: Nurse_Id: Complaints_Id: Diagnosis_Id: Pharmacist_Id:Lab_scientist Id:]

F. Android Application With The Database In Real-Time

Remote Clinical Consultation app is written in Java programming Language with XML for the interface, embedded in an android mobile phone. The real-time app resides as a tool in the Presentation Layer. When requested, it is downloaded on the client phone. Once loaded, it communicates with consultation server using the HTTP protocol. It establishes an HTTP connection and then posts HTTP requests to it. The HTTP requests are received and forwarded by the mobile phone layer to the presentation layer. At the presentation layer, the request is processed and then an HTTP request is made to the application layer which fetches the required information from the database layers.

G. Consultations In the Remote Clinical System Application

The aim is to effectively utilize the available doctors. The consultation is based on set theory, and the modeling is to increase the patient satisfaction and effectively utilize the available doctors. The parameters for the remote consultations and the modeling are denoted as follows:

$P = \{P1, P2, P3, P4, P5, \ldots Pn\}$ (1)

where P is the set of Patients in the system, where $Pi \in P$ denote specific Patient Pi

$D = \{D1, D2, D3, D4, D5,. ..Dn\}$ (2)

where D is the set of registered Doctors in the system to attend to Patient, where $Dj \in D$ denote specific Doctor Di

$A = \{AD, AD2, AD3, AD4, AD5, \ldots ADn\}$ (3)

where A is the set of available Doctors, where $ADj \in \{1,0\}$ is the availability of specific Doctor.

$Q = \{QD1, QD2, QD3, QD4, QD5, \ldots QDm\}$ (4)

where Q is the set of patient waiting for a Doctor, where $QDj \in Q$ denote the specific Doctor's queue that contains an assigned patient.

$H = \{HD1, HD2, HD3, HD4, HD5, \ldots HDm\}$ (5)

where H is the set of average patient handling time of each Doctor, where $HDj \in H$ denote specific Doctor's handling time.

V. SYSTEM ARCHITECTURE

The behaviour of the system when the patient wants to share information with the specific module, first patient need to download the App, register and login then he/she can communicate with rest of the module such as Doctor, Nurse, SMS channel, Pharmacy, Lab Scientist, Chatting Channel and Database Server. All annals are shared with the HTTP (Hypertext Transfer Protocol).The system incorporates chatting, medical images, health Tips, drug- prescription and registrations of patients all in real-time environment. The behaviour of the system when the patient wants to share information with the specific module (Doctor or Nurse) is that of an on-line chatting box. All annals are shared with the HTTP (Hypertext Transfer Protocol). The web server interacts with the database via JAVA script, it also receive query, update, and execute the query, the result are sent as a JSON object for feedback to the patient with a 3G/4G Mobile. The database contains the demographics of patients and the registration details of other users and others.

The web server interacts with the centralized database named as Relational Database Management System (RDBMS) via JAVA script, it also receive query, update, and execute the query. The client side is Android Device and server side is combination of MYSQL, PyCharm and Django web framework.

Patient is to access and input data to the system through the web browser from the Android Phone. Data transmissions include file, image and video transfers, and vital health statistics of patients. The characteristics of each of these data streams can differ greatly. The database tier is responsible for storage, retrieval, update, and integrity of the data. The connectivity of the application to the database is through the Java Script.

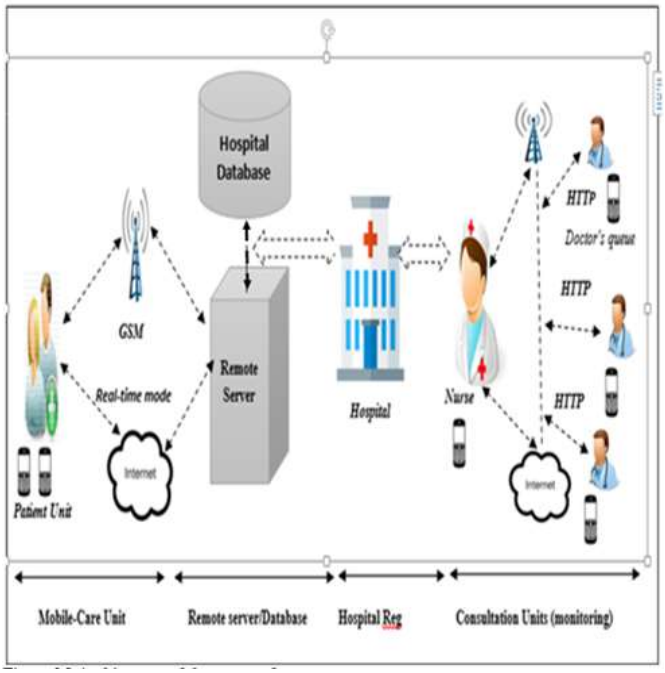

FIGURE 1: ARCHITECTURE OF THE SYSTEM

VI. COMPONENTS OF THE ARCHITECTURE

The components of the proposed system architecture are presented as follows:

- **Patient Mobile Unit:** An interface where online patients submit requests in a real time mode.
- **Remote Server:** A two-way communication link servicing the patient requests with the hospital database.
- **Hospital Database:** A repository containing the records of patients and various health providers.
- **Virtual Nurse:** An intermediary between the patients and the specific doctor in attendance for a first time user.
- **Doctors' List:** A list of doctors in attendance with different specialties.

VII. SYSTEM DESIGN REQUIREMENT

The system was implemented using the following minimum requirements:

Client Side:

a. Xml (1.0)- Interface Design
b. Android Studio 2.3.3 - Integrated Development environment for Android
c. Android o/s version 7.0 – Naugat
d. Java Runtime Environment
e. SQLites- Login Details

Server Side:

a. Pycharm (2017.2 Professional) - Integrated Development Environment (Django)
b. Django 2.0.3 - Web Framework
c. Anaconda(5.1.0) - Interpreter
d. MySQL database 2008 (5.7.21)

TABLE I THE SYSTEM FLOW ALGORITHM

Step1	Registered users go to update and start chatting
Step 2	For new users
Step 3	Users download health Apps
Step 4	Install it on their device
Step 5	Run the App
Step 6	Users create account by sign up
Step 7	Log in using username and password
Step 8	Validate users
Step 9	Communication with the Nurse
Step 10	Direct to the Doctor
Step 11	Consultation session with Doctor
Step 12	Upload data/ complaint for Doctor
Step 13	Patient can upload video or Medical Images
Step 14	Doctor post solution
Step 15	Pharmacy describe the prescription and pick up method
Step 16	Patient View the solution
Step 17	If satisfied then log out
Step 18	If not satisfied continue chatting
Step 19	End procedure

VIII. RESULT AND DISCUSSIONS

The Clinical Consultation application was tested by some experts comprises Doctors, Nurses, Pharmacist and Laboratory Scientist. The total of Sixty-Five (65) questionnaires and sixteen (16) questions in each was administered. Evaluation was based on ease of use, acceptability and functionality. The users had the clinical consultation system installed on their mobile phones.

Questionnaire method of data collection was applied, the questionnaires are closed-ended which allow respondents with choices of options (Strongly Agreed, Agreed, Strongly Disagreed and Disagreed). The objective of the questionnaire approach is basically to evaluate the clinical consultation system.

Descriptive statistics is used to summarize the features of the information collected from the questionnaires. It measures the central tendency and variability. The average score from the users who consented from the hospital and from those outside of the hospital gave the overall user success for the clinical consultation system, which reached 95% Confidence Value. This is quite impressive taking into account that most users were acquainted with mobile phone usage. The usefulness of the application and the functionality were rated positively. Users were comfortable with using the system. Overall, users stated that they were enthusiastic about the potential of using such applications.

TABLE II DESCRIPTIVE STATISTICS FOR STRONGLY AGREED AND STRONGLY DISAGREED

SUMMARY	STRONGLY AGREED	STRONGLY DISAGREED
Mean	32.3125	3.4375
Standard Error	0.794348528	0.4913311
Median	31.5	3.5
Mode	29	4
Standard Deviation	3.17739411	1.965324401
Sample Variance	10.09583333	3.8625
Kurtosis	0.730030896	0.348615472
Skewness	1.070088952	0.678664374
Range	11	7
Minimum	29	1
Maximum	40	8
Sum	517	55
Count	16	16
Confidence Level	95.0% (1.69311380821343)	95.0% (1.04724745018918)

TABLE III DESCRIPTIVE STSTISTICS FOR AGREED AND DISGREED

SUMMARY	AGREED	DISAGREED
Mean	26.875	2.1875
Standard Error	0.810735263	0.410474827
Median	27	2
Mode	27	3
Standard Deviation	3.242941052	1.641899307
Sample Variance	10.51666667	2.695833333
Kurtosis	0.132232113	4.384436062
Skewness	-0.354787416	1.517314989
Range	12	7
Minimum	21	0
Maximum	33	7
Sum	430	35
Count	16	16
Confidence Level	95.0% (1.72804130788405)	95.0% (0.874906382778759)

FIGURE 2: WELCOME PAGE OF THE APP

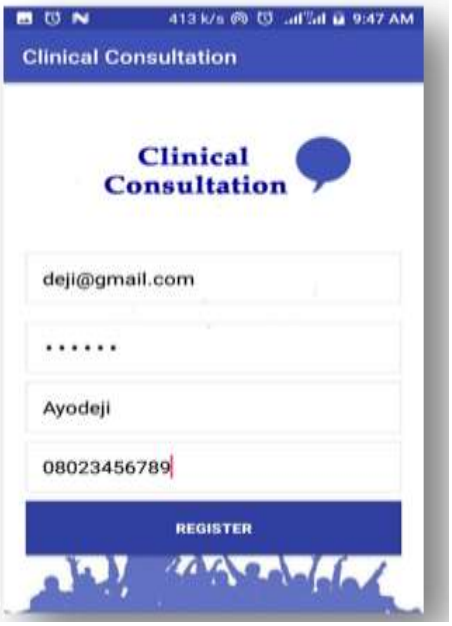

FIGURE 3: AYODEJI's REGISTRATION

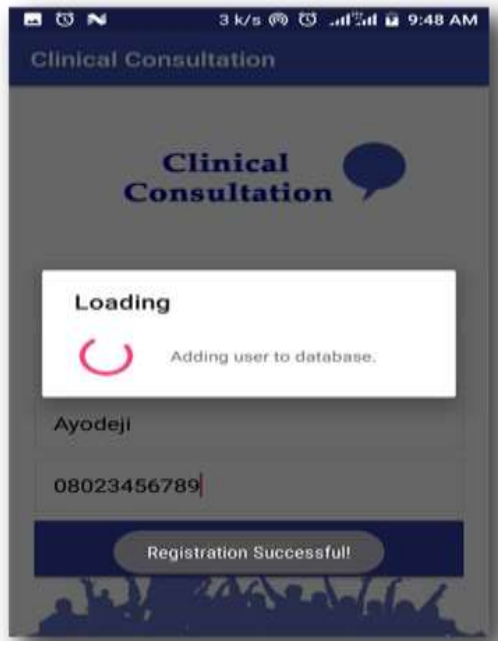

FIGURE 4: ADDING AYODEJI TO DATABASE

FIGURE 5: LIST OF PATIENTS (P) REGISTERED

FIGURE 6: TRANSACTION OF THE USERS: DOCTOR (D), NURSE (N) AND PATIENT (P)

IX. CONCLUSION

In this research work, the need to develop real time clinical consultation system has been identified. A remote patient monitoring and management system for clinical consultation that increase the doctor to patient interaction using a Java-enabled mobile android phone was developed and the file size for Remote Clinical Consultation Application version (1.0) is 16.44MB. It is a multi-way communication care and management application, with real-time feedback. This research work is recommended to medical practitioners including doctors, nurses, medical labouratory scientist, pharmacist and medical patients to enhance real time medical interaction via mobile platform. Moreover, healthcare policy makers are encouraged to peruse the contributions of this research work in the use of mobile healthcare system.

X. FUTURE WORK

Further work would be to implement live-streaming videos among medical practitioners and patients for better and improved medical consultations. Also the security of patients' records should be considered through high-level user authentication and/or cryptography.

ACKNOWLEDGMENT

My appreciation goes to Professor O. Olabode and Dr. Mrs. O.A Daramola for their encouragement, wonderful ideas, and constructive criticisms throughout the work.

REFRENCES

Figure 1. International Telecommunication Union (2014), "ICT Facts and Figures of mobile phone penetration", Geneva: International

Telecommunication Union. Retrieved from ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

Figure 2. World Bank Group Report (2012) Information and Communications for Development (2012), "Maximizing Mobile", Washington, DC: World Bank.

Figure 3. MeSH (2007), "Remote Consultation", National Center for Biotechnology Information MESH database for NCBI ID: D019114, NO4: 590.374.800.550.

Figure 4. Ben-Ari.M (1990), "Principles of Concurrent and Distributed Programming", Prentice Hall Publication:ISBN 0-13-711821-X. Ch16, Page 164.

Figure 5. Martin James (1965). "Programming Real-time Computer Systems", Englewood Cliffs, NJ: Prentice-Hall Inc. p. 4. ISBN 0-13-730507-9

Figure 6. Suter P and Johnston D.(2011), "Theory-based Tele-health and patient empowerment" Population Health Management ,Volume.14,87-92.

Figure 7. World Health Organization (2011), "mHealth: New Horizons for Health Through Mobile Technologies Global Observatory for eHealth Series", Volume 3.

Figure 8. World Health Organization (2005b), "e-Health Tools and Services: Needs of Member States" Geneva: WHO.

Figure 9. Olusola O. Isola(2009), "The Use Of Mobile Telephone In Reducing Pre-natal Maternal Mortality: Case Study Of Abiye (Safe Motherhood) Project In Ondo State, Southwest Nigeria.

Figure 10. Oluwafemi Sunday Oyeyemi and Rolf Wynn (2014), "Giving cell phones to pregnant women and improving services", reproductive health journal.com/content/11/1/8.at: https://www.vanguardngr.com/2017/01/one-doctor-still-attends-6000-patients-nigeria-don/

Figure 11. Dakoza (2004), Dokoza System for Disease Management in South Africa, "To fast-track and improve critical services for HIV and TB patients by facilitating better data management" A pilot project of Dakoza in partnership with Neil Harvey and Associates (NHA) for IT support, and Deloitte for data analysis and reporting, risk management and strategic advice.

Figure 12. Chen RY, Feltes JR, Tzeng WS, Lu ZY, Pan M, Zhao N, Talkin R, Javaherian K, Glowinski A and Ross (2017, June), " Phone-Based Intervention in Adolescent Psychiatry: A perspective and Proof of Concept Pilot Study With a Focus on Depression and Autism", JMIR Research Protocol Publication 16.06.17 Vol. 6. NO6.

Figure 13. Ran Wei and Zhimin Yang (2012), *"Design and Implementation of Doctor-Patient Interaction System Based on Android"*, 2012 International Journal Symposium on information technology in medicine and education, 978-1-4673-2108-2/12/0 ©2012 IEEE.

Figure 14. Ziyu Lv, Feng Xia, Guowei Wu, Lin Yao and Zhikui (2015), "*A Mobile Health Monitoring System for the Elderly"*, Chen School of Software Dalian University of Technology Journal, Dalian

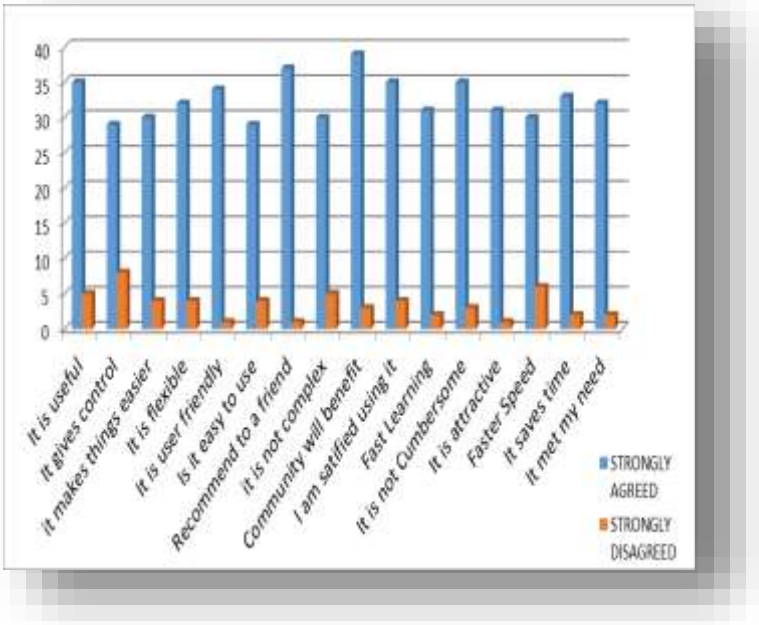

FIGURE 7: CHART OF STRONGLY AGREED AND STRONGLY DISAGREED

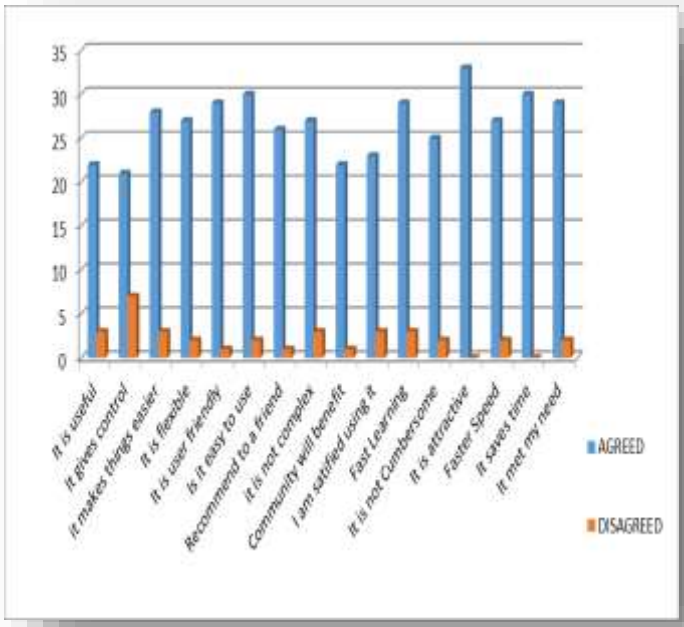

FIGURE 8: CHART OF AGREED AND DISAGREED

Deep Neural Network-Based Learning Analytics in Medical Education for Enhanced Universal Health Coverage (C003)

Okewu Emmanuel
Centre for Information Technology and Systems
University of Lagos
Lagos, Nigeria
okewue@yahoo.com

Adewole Philip
Department of Computer Sciences
University of Lagos
Lagos, Nigeria
padewole@unilag.edu.ng

Abstract*— Poor doctor to patients' ratio particularly in developing economies is concerning. Whereas the United Nations benchmarked 1 doctor to 600 patients, the reality hovers around 1 doctor to 6000 patients in extreme cases. The policy goal of healthcare accessibility and affordability by all citizens of a country as canvassed by Universal Health Coverage (UHC) will remain a mirage except deficit in the number of critical healthcare professionals such as doctors and dentists is addressed. A number of measures have been introduced to enhance the delivery capacity of medical education alongside other components of higher education. However, the continued shortage of medical personnel entails that further research and approaches are required. In this vision paper, an evidence-based approach is used to underscore high failure rate in medical schools and its impact on UHC. As a solution, we proposed a deep neural network-based learning analytics (DNN-based LA) system. The system harnesses medical students' data for generating unbiased and robust information for interest groups and critical stakeholders in medical education to formulate strategic and adaptive learning methods that promote rich learning experience, enhance student retention, and promote student progression. Against the backdrop that convergence rate and training time of neural networks are growing concerns to researchers and could impede implementation of DNN-based LA system, we reviewed the challenges confronting stochastic gradient descent (SGD) algorithms with a view to improving on them. SGD is the popular algorithm for training neural networks. Our efforts culminated in a new SGD model called Aiona which is currently undergoing evaluation in a bid to benchmark it against established SDG algorithms like Adagrad, Adadelta, RMSProp and Adam. More importantly, the implementation of a deep learning model like DNN-based LA in medical schools will address the manpower needs of a global health initiative like UHC. The study also adds to the growing body of deep learning libraries an empirical application in DNN-based LA system.

Keywords- Aiona, Deep Neural Networks, Stochastic Gradient Descent Algorithm, Learning Analytics, Medical Education, Universal Health Coverage

• INTRODUCTION

The global healthcare scheme called Universal Health Coverage (UHC) is a global initiative aimed at providing healthcare and financial protection to citizens of a country [1]. The World Health Organization (WHO) envisions a seamless scenario in which healthcare is affordable and accessible to the citizenry. However, the shortfall in number of medical personnel, particularly in developing countries, means that the ideals of UHC may remain a mirage except the situation is addressed [2]. Specifically, in contrast to WHO's recommendation of one doctor to 600 patients, the ratio in Nigeria is one doctor to 6,000 patients [3]. The world's lowest patients to doctor ratio is in Cuba with 1:155 just as U.S. trails at 1:396 [4].

The problem of inadequate medical experts to attend to medical emergencies is a socio-economic problem as health is wealth. Emotions drive people and people drive productivity. Ill-health affects emotions and productive activities slow down when the workforce is not healthy. This study investigates the issue of deficit in the number of medical professionals such as medical doctors and dentists. Medical education is a critical component of higher education charged with the responsibility of producing medical experts. Inability of higher education to respond adequately to societal needs has led to a number of reform measures including the introduction of learning analytics [5]. Learning analytics (LA) refers to the measurement, collection, analysis and reporting of data about learners and their contexts with a view to understanding and enhancing learning and the learning environments [6]. The information extracted about students could be used to put in place adaptive learning measures that saves operational cost, promotes rich learning experience, enhances students' retention, and engenders students' progression [7]. Popular data science techniques used by LA include statistics, data mining, knowledge discovery in databases (KDD), and machine learning [8].

Extracting unbiased, reliable and robust information from huge historical students' data for informed decision making is a process that requires sophisticated machine learning technique like deep neural networks (DNN). Artificial neural networks (ANN) are generally known for accuracy and high precision in pattern recognition and predictive analytics. Specifically, DNN offers cutting-edge services by engaging in rigorous and vigorous learning of hidden and useful patterns in educational data. The implication is that the application deep neural network-based learning analytics (DNN-based LA) to medical students' data will offer stakeholders in medical education precise information as to strategic interventionist measures that should be taken to curb poor academic performance and high drop-out rates in medical schools. This study analyzed student data from a College of Medicine to provide empirical evidence that there is high

students failure rate in medical schools. This trend negative impacts on the turn-out of medical graduates resulting in low student progression into labour market (medical practice).

However, the prolonged training time and convergence rate of ANN in general and DNN in particular [9] means the proposed deployment of DNN-based LA in medical education may suffer setback. In this regard, we reviewed existing stochastic gradient descent (SGD) algorithms highlighting their approaches, strengths, and weaknesses with a view to improving on them. SGD is the traditional algorithm for training deep neural networks [10, 11]. Our effort resulted in a new SGD method called Aiona which is undergoing evaluation to benchmark its performance against the performances of established SGD algorithms like Adagrad, Adadelta, RMSProp and Adam. Aiona is an extension of Adam, a popular SGD algorithm for training deep neural networks [12].

- LITERATURE REVIEW

  - *Deep Neural Networks*

First, Deep neural network (DNN) is an artificial neural network that promotes deep learning using visible (input) layer, hidden layer, and classification (output) layer [9]. The hidden layer must contain at least 2 sets of computational neurons (nodes). DNN is a component of the wider family of machine learning methods that leverage on learning data representations rather than task-specific algorithms. The information processing and communication patterns in biological nervous system inspires deep learning models like recurrent neural networks (RNNs) and convolutional neural networks (CNNs) [13]. In RNNs, data can flow in any direction and they are applied in areas such as language modeling. On the other hand, CNNS are used in computer vision and can also be applied in acoustic modeling for automatic speech recognition. In these thematic areas, they have produced commendable results which can be compared to human experts. As a class of machine learning techniques, deep learning uses a cascade of many layers of nonlinear processing units for feature extraction and transformation. The output from the previous layer is used as input by successive layer. DNN can learn in both supervised manner (e.g. classification) and unsupervised manner (e.g. pattern analysis).

The popular algorithm for training deep neural networks is the first order method called gradient descent [14]. The use of second order methods like Newton's method for DNN is discouraged in that they are computationally intensive. Moreover, DNN problems are non-convex high dimensional problems for which second order methods are unsuitable. Non-convex problems are problems whose local minimum differs from global minimum [15].

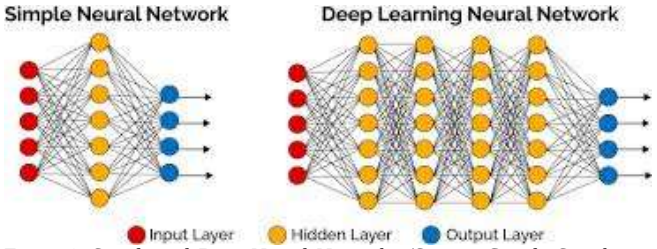

Figure 1. Simple and Deep Neural Networks (Source: Google Search Images (August 2018)

The optimization focus of DNN is to minimize the objective function with respect to (w.r.t) the network parameters and SGD algorithm is used. SGD is a stochastic approximation of gradient descent optimization [12]. It is an iterative method that optimizes the differentiable objective function. It is called stochastic for two reasons: training samples are chosen randomly or in a shuffled manner and network parameters are randomly determined or initialized. In a nutshell, it means involving chance or probability.

  - *Deep Neural Network-based Learning Analytics in Medical Education*

A sub-sector of higher education where academic work is rigorous and vigorous is medical education. Medical schools of universities are known to produce medical and para-medical graduates for attending to healthcare needs of a nation [16]. More than any other sectors of higher education, students in medical schools are known to increasingly face challenges of poor academic performance, high drop-out rate, and relatively low students' progression. These impact negatively on availability of health personnel for the actualization of the objectives of Universal Health Coverage (UHC) particularly amidst teeming population. For example, dental therapists are required for managing oral health which is critical for the success of UHC [17]. The role of institutions in enhancing UHC cannot be overemphasized [18]. Organizations such as institutions of higher learning have to re-strategize to consistently be relevant in the marketplace and be instrumental to the success of global initiatives like UHC. One of the ways higher education in general and medical education in particular can maintain global relevance and be competitive is to make meaningful use of their operational data. The large datasets can be harnessed to facilitate the three cardinal goals of higher education - teaching, research and community service through the use of learning analytics system for academic advising [5]. As students create new content, access learning materials, interact with colleagues, and take examinations, learning-related data is created. This data can be mined using machine learning techniques like deep neural networks. The use of DNN-based LA systems in medical education will ensure that hidden and useful patterns in medical students' data are elicited for evidence-based information. This robust information will guide policy makers, health professionals and other stakeholders in medical education in formulating adaptive learning measures that promote better learning experience and enhance the general learning environment. Particularly, DNN-based LA

system could offer platform for rich and adaptive learning at different layers of granularity such as departmental, course, and institutional levels with promises of cost saving and facilitation of student retention and progression [7].

o *Universal Health Coverage and Shortage of Medical Personnel*

A The global health scheme, universal health coverage (UHC) is also known as universal health care. It is a health care system that offers both health care and financial protection to the citizenry of a nation [19]. Organized around offering specific package of benefits to entire members of a given society, the cardinal goal is to avail citizens improved access to health services, provide financial risk protection, and scale up health outcomes.

The health scheme does not mean coverage for all people for everything. Rather UHC can be evaluated by three cardinal parameters: people covered, services covered, and percentage of the cost covered [20]. WHO describes UHC as a seamless situation in which citizens access healthcare services without experiencing financial hardship [21]. It has also been described as the single most powerful concept that public health has to offer in that it integrates services and delivers same in a comprehensive manner. An ambitious target by United Nations member states is to work toward worldwide universal health coverage by 2030. A cardinal goal of universal healthcare is to evolve a system of protection which offers equal opportunity for people to benefit from an attainable level of health.

To achieve the lofty ideals of UHC, researchers have focused much attention on the adequacy of health facilities and the need to strengthen health regulatory institutions. However, little attention has been paid to the issue of manpower shortage. The availability of high net-worth medical professionals like doctors and dentists is paramount to the success of UHC but they are in short supply [3]. This situation is worse in developing economies. Quantitatively, while WHO recommended doctor to patients' ratio of 1:600, Nigeria's ratio is 1:6000 while countries like Cuba and USA are ahead of WHO's benchmark with 1:155 and 1:396 respectively [4]. This study traces the deficit in countries like Nigeria to inability of her higher education to produce commensurate number of medical personnel. The medical schools are challenged by high rate of students drop-outs, poor academic performance, and low students' progression.

o *Related Works*

Previous works on deep neural networks, learning analytics and universal health coverage are discussed as follows.

[9] studied deep neural networks from the viewpoint of initialization of network parameters with a view to expediting convergence. Their efforts culminated in a new initialization scheme which has been shown to result in faster convergence. As a step towards achieving this feat, they studied how activations and gradients change across layers and during training, guided by the realization that training tends to be more difficult when each layer's singular values of the Jacobian are far from 1. Their research into deep neural networks was stimulated by the fact that prior to 2006, deep multilayer neural networks appeared not to be successfully trained but afterwards, the narrative changed. The authors posited that since 2006, many algorithms have been successfully used to train DNN with evidence of experimental results that show the superiority of deeper over vs less deep architectures. They observed that new initialization or training mechanisms were responsible for these experimental results. The cardinal objective of the researchers was to have improved understanding of why standard gradient descent from random initialization was initially doing so poorly with deep neural networks but later (recently) experienced relative successes. This quest for better knowledge was to enable them design better algorithms in the future. The quest led them to observe that non-linear activations functions had great impact. They found out that the logistic sigmoid activation is not suitable for deep networks with random initialization. This is because its mean value can drive particularly the top hidden layer into saturation. The equally discovered that saturated units can move out of saturation by themselves though in a slow fashion. This explains the plateaus intermittently observed when training neural networks. Yet another discovery is that a new non-linearity that saturates less can often be beneficial. This study largely focused on improving convergence rate by fine-tuning activation functions while the present study is aim at improving stochastic gradient descent algorithms for better and faster results by fine-tuning learning rate.

In [1], the authors used historical health financing data for 188 countries covering the period 1995 to 2015 to project future scenarios of health spending and pooled health spending for up to year 2040. This is against the backdrop that health financing systems that offer prepaid pooled resources for critical health services are required for achieving UHC. The researchers opined that making progress towards UHC requires an understanding of current and future trajectories of health financing. As part of their methodology, the researchers extracted historical data on gross domestic product (GDP) and health spending for the 188 countries spanning 1995 to 2015. Based on this data, they made projections for 2015 through 2040 on topical issues like annual GDP, development assistance for health, and prepaid private health spending. Among other analytical functions performed on the data, stochastic frontier analysis was used to investigate the relationship between pooled resources and UHC index – a measure of a nation's UHC service coverage. Of the three categories of countries, forecast shows that per capita health spending would increase fastest in upper-middle-income countries, followed by lower-middle-income countries, and lastly, low-income countries. The authors concluded by charting future scenarios for health spending and drawing attention to its relationship with UHC. In addition, they advised that achievement of UHC is dependent the ability of all countries to have sustainable pooled health resources. Though the study identified health financing as a bane of UHC, it was silent on the threat posed by shortage of medical personnel like doctors and dentists. Also, the techniques used

in the study is simple statistics whereas this present study is applying neural networks to medical students' data for regression analysis, pattern recognition, and predictive analytics in this present study.

[7] opined that the growing global rate of unemployment is the reason for heightened quest for functional and all-inclusive education as advocated by the Sustainable Development Goal 4 (SDG 4). They proffered LA as a recipe for facilitating employability of graduates and scaling up their entrepreneurial skills for self-sustenance. LA was described as a pedagogical paradigm that is capable of inculcating the twin skills of data analytics and team work in learners. Its procedure involves measuring the learning process - learner-related data collected, analyzed, and report generated for education stakeholders. The stakeholders leverage on the information generated to put in place adaptive learning solutions capable of improving learning experience and learning outcomes. The authors acknowledged that though LA could be enhance using many data science techniques, artificial neural network is exceptional as a sophisticated predictive data mining tool and machine learning technique. They therefore proposed an Artificial Neural Network-based Learning Analytics (ANN-based LA) system. To extract unbiased information from learners' data, the system relies on regression analysis, pattern recognition, and predictive analytics with a view to enhancing decision making by education stakeholders. The study outlined open issues facing ANN-based LA systems as prolonged time of training neural network, system quality issues and large memory space requirements. To tackle the system quality issues, the paper proposed an n-tier layered software architecture while hoping that upcoming researchers will resolve the remainder. As a follow up, this present study is addressing the prolonged training time of deep neural networks by improving on its traditional training algorithm, stochastic gradient descent, for faster convergence rate. Also, while the authors focused on using ANN-based LA to improve learning across educational institutions and organizations, this present study specifically use DNN-based LA to address deficit in the turn-out of medical graduates and attendant impact on UHC.

• METHODOLOGY

To validate claims of high students' failure rate being responsible for deficit in the number of medical professionals required for implementing UHC, the medical school of a university is used as case study. Harvested students' data are modelled using neural networks to classify medical students learning behaviours and predict academic performances. The aim of these learning analytics tasks is to guide interventionist measures such as strategic adaptive learning techniques capable of scaling up students' retention and progression. The progress of a DNN-based LA can be hampered by slow neural network learning speed. Hence, an approach to improving existing stochastic gradient descent algorithms using third and fourth moments of gradients is proposed. This culminated in a novel algorithm called Aiona. Aiona is an extension of Adam, a popular algorithm for training deep neural networks. In future work, Aiona is to be validated and benchmarked against established stochastic gradient descent algorithms. Details of our methodology is as follows:

The study surveyed real-life medical and dental students' data from the College of Medicine of University of Lagos for evidence-based conclusions. MBBS is a two-in-one medical degree and stands for Bachelor of Medicine, Bachelor of Surgery. BDS is a dental degree and stands for Bachelor of Dentistry. The data examined and modelled covered the period 1962 – 2017 as tabulated in Table 1.

PRODUCTS OF COLLEGE OF MEDICINE OF THE UNIVERSITY OF LAGOS (SOURCES: IPAYE (2002), COLLEGE OF MEDICINE ACADEMIC OFFICE))

SN	Year of Convocation	MBBS (No. of Graduates)	BDS (No. of Graduates)
1.	2017	238	59
2.	2016	217	85
3.	2015	60	20
4.	2014	-	-
5.	2013	208	69
6.	2012	100	24
7.	2011	127	55
8.	2010	101	13
9.	2009	116	37
10.	2008	164	25
11.	2007	222	41
12.	2006	195	39
13.	2005	272	32
14.	2004	112	35
15.	2003	91	34
16.	1967 – 2002	3,436	592
	Total	5,659	1,160

As shown in Table 1, in 1967, the first batch of 27 medical students graduated from the College while 8 Dental students graduated in 1971. To date, the College has been able to produce a total of 5659 medical doctors and 1160 dentists. It is observed that in year 2014, medical doctors and dentists were not produced due to accumulated effects of prolonged strikes and occasional students' unrests that led to discontinuation of academic activities. Same reasons for inability of the University to have graduated 2018 batch of medical doctors and dentists by the time this paper was being written in August 2018. These incidences are clear pointers to the fact that unfavourable socio-economic atmosphere in developing economies impact negatively on all sectors, higher education and medical education inclusive. The fallout is setback to the attainment of the lofty goals of global and local health initiatives owing to inadequacy of the strategic influence of medical doctors and dentists.

○ *Visual Inspection (Human Vision)*

To provide further empirical evidence of high failure rate in medical schools, the study took a closer look at a sample result – outcome of the 600 Level Bachelor of Dental Surgery Degree (Final) Examination, May 2017. The analysis is as follows:

Total No. of Students that registered for the examination = 62
Total No. of Students that passed the examination = 15
Total number of students that failed the examination = 47

The percentage of students that passed is 24% while the remaining 76% failed the examination. The visual inspection and statistical analysis further revealed that none of the students graduated within the stipulated 6-year graduation period for medical and dental students. Of the 62 students, 11 students (17.4%) graduated after spending one extra year; 3 students (4.8%) graduated after spending 2 extra years; while 1 student (1.6%) graduated after spending 6 extra years. The study observed that despite spending extra years, some students did not graduate. In this category is 1 student (1.6%) who had spent 5 extra years and 8 students (12.9%) who had spent 3 extra years. Clearly, these statistics attest to the fact that there is low student progression rate and possible high drop-out rate as some frustrated students could call it quit.

- *Computer Vision (Deep Learning)*

To elicit hidden and useful patterns in the medical and dental datasets (MBBS600 and BDS600) for purposes of addressing poor performance as statistically confirmed above, deep neural network was used to model the data. Table II summarizes the data structure for scores of a total of 5659 medical graduates that have been produced by the College of Medicine of University of Lagos since inception in 1962. The historical data of these former students show the students as subjects and their scores in the 25 compulsory professional course that must be passed as variables.

MBBS600 DATASET (1962 – 2017)

SN	X1	X2	X3	X4	….	X25
1.						
2.						
3.						
4.						
5.						
6.						
.						
.						
5659						

Key
MBBS = Bachelor of Medicine; Bachelor of Surgery
X1 = Anatomy
X2 = Biochemistry
X3 = Physiology
X4 = Morbid Anatomy
X5 = Clinical Pathology
X6 = Medical Microbiology
X7 = Pharmacology
X8 = Principles of Epidemiology and Environmental and Occupational Health
X11 = Surgery with Anaesthesia
X12 = Clinical Paediatrics
X13 = Obstetrics & Gynaecology
X14 = Medicine
X15 = Health Management, Health Education and Medical Jurisprudence
X16 = Maternal and Child Health
X17 = General Medical Practice (including Psychosocial Medicine)
X18 = Medical Sociology
X19 = Medical Psychology
X20 = General African Studies (GAS) 201
X21 = General African Studies (GAS) 202
X22 = Basic Clinical Skills
X23 = Clinical Psychology
X24 = Psychiatry
X25 = Project

It can be deduced from Table 2 that the MBBS600 dataset is a linear data structure whose elements form a sequence. The dataset is a matrix of dimension 5659 x 26 i.e. MBBS600(5659,26). The first 25 columns contain the inputs while the 26 column is the target output which is binomial (Pass, Fail) as the final classification of medical result is either pass or fail. The homogenous elements to be stored in the input columns of the matrix are students' scores while the elements in the output column are binary values 1 and 0 depending on whether a student passed or failed. Linear data structure operations like traversal, search, insertion, deletion, sorting, and merging can be performed on MBBS600.

Similarly, Table III shows abridged version of statistical features of dental students' dataset with 1,160 students as subjects and 26 courses as input variables.

BDS600 DATASET (1962 – 2017)

SN	X1	X2	X3	…	X26
1.					
2.					
3.					
.					
.					
1160					

Key
BDS = Bachelor of Dental Surgery
X1 = Anatomy
X2 = Biochemistry
X3 = Physiology
X4 = Morbid Anatomy
X5 = Clinical Pathology/Haematology & Blood Transfusion
X6 = Medical Microbiology & Parasitology
X7 = Pharmacology
X8 = Principles of Epidemiology and Environmental and Occupational Health
X11 = Oral Maxillofacial Surgery
X12 = Restorative Dentistry
X13 = Child Dental Health
X14 = Preventive Dentistry
X15 = Oral Pathology
X16 = Preventive Dentistry
X17 = Health Management Planning and Development
X18 = Dental Surgery I (Restorative Dentistry & Child Dental Health)
X19 = Dental Surgery II (Including Oral Surgery, Pathology & Oral Medicine)
X20 = Medical Sociology

X21 = Medical Psychology
X22 = General African Studies 201
X23 = General African Studies 202
X24 = Basic Clinical Skills
X25 = Medical Statistics
X26 = Clinical Psychology

In a bid to solve the problem of shortage of manpower in the health sector, understanding hidden patterns in medical students' data with a view to repositioning medical education for increased productivity should be of paramount concern. Given these two datasets (MBBS600 and BDS600), there are two learning analytics tasks to accomplish - (1) classifying the learning behaviour of medical students and (2) predicting the performance of future students. Given MBBS600 as sample data, pattern recognition (classification) using deep neural networks will commence with an activation function that introduces non-linearity into the linear data as follows:

Neuron output ($\hat{y}$) = $x_1.w_1 + x_2.w_2 + x_3.w_3 + \ldots + x_{25}.w_{25} + b$

where $x_1, x_2, \ldots, x_{25}$ are student scores, $w_1, w_2, + .. + w_{25}$ are network parameters, b is a network constant called bias.

This neural network learning process continues with the computation of an objective (cost) function with:

$\delta = y_{target} - \hat{y}$

Since it is unlikely that the network (neuron) output ($\hat{y}$) will equal target output (y_{target}), it means $\delta \neq 0$. It implies an error in the networks attempt to exactly match the real-world data. The neural network then starts an iterative process that progressively reduces the error until it is within acceptable limit. At this point, the deep neural network is assumed to have learnt sufficiently the patterns in the medical students' data. The DNN-based LA system can then be positioned for academic advising such as predicting future students' performance based on this historical data (MBBS600).

The task of finding an error within acceptable limit is an iterative process that is same as optimizing the objective (error or cost or loss) function parameterized by network parameters. Progressively, the training algorithm finds changes in objective function w.r.t. changes in network parameters. Given m passes over sample data and n neural network parameters, the training process involving cost functions ($f_1, f_2, ..f_m$) and network parameters ($w_1, w_2, .., w_n$) is represented by the partial derivative ($\partial f/\partial w$):

$$\frac{\partial f}{\partial w} = \begin{bmatrix} \frac{\partial f1}{\partial w1} & \frac{\partial f1}{\partial w2} & \cdots & \frac{\partial f1}{\partial wn} \\ \frac{\partial f2}{\partial w1} & \frac{\partial f2}{\partial w2} & \cdots & \frac{\partial f2}{\partial wn} \\ & \vdots & & \\ \frac{\partial fn}{\partial w1} & \frac{\partial fn}{\partial w2} & \cdots & \frac{\partial fn}{\partial wn} \end{bmatrix}$$

Traditional gradient descent optimization algorithm is used for training deep neural networks though there could be variants. The algorithm manipulates learning rate and network parameters until the objective function converges to a local minimum. At this point, the deep neural network has learnt patterns in students' data sufficiently and can be relied upon to predict student performance from future input data. Interest groups and relevant stakeholders in the health sector can then rely on the DNN-based LA system for information that could be harnessed for formulating adaptive learning strategies that encourage the production of more doctors and dentists for effective and efficient UHC.

Screen shots from experiments conducted using MATLAB are shown in figures 2 and 3 below.

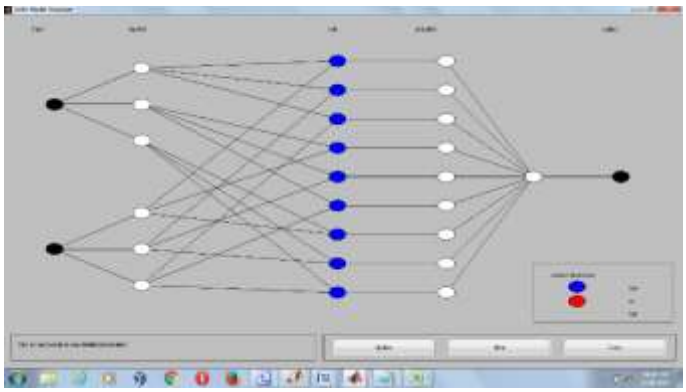

Figure 2. Deep neural network modelling of MBBS600 dataset on MATLAB

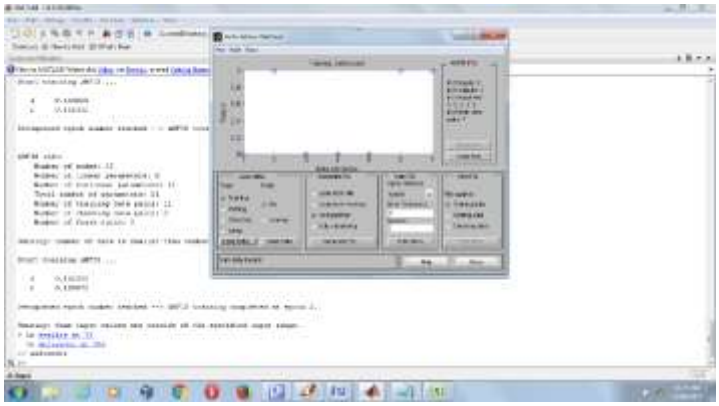

Figure 3. The training process on MATLAB

The training process transcript generated by MATLAB is presented as follows:

ANFIS info:
Number of nodes: 35
Number of linear parameters: 9
Number of nonlinear parameters: 12
Total number of parameters: 21
Number of training data pairs: 11
Number of checking data pairs: 0
Number of fuzzy rules: 9

Warning: number of data is smaller than number of modifiable parameters

Start training ANFIS ...

1 0.164825
2 0.162332

Designated epoch number reached --> ANFIS training completed at epoch 2.

- IMPROVING STOCHASTIC GRADIENT DESCENT ALGORITHM

Efforts to improve gradient descent as the key algorithm for training neural networks have resulted in variants and extensions like stochastic gradient descent, Momentum, Nesterov accelerated gradient, AdaGrad, AdaDelta, RMSProp and Adam [14]. In the literature, stochastic gradient descent (SGD) has assumed the umbrella name these algorithms [22] and will be so used this paper. The key consideration has been to achieve good and fast results from neural networks by modifying learning rates and network parameters in such a way that facilitates convergence of loss function as well as scales up learning speed of neural networks. This way, deep learning libraries such as DNN-based LA systems could be more reliable for tackling problems of poor academic performance, high drop-out rate and low student progression in medical schools. And by extension, solve the manpower problem of UHC. Table IV highlights trends in the improvement of SGD algorithm till date.

TRENDS IN SGD ALGORITHM IMPROVEMENT

Gradient Descent Variant/Extension	Approach	Strength	Weakness	Improvement
Standard Gradient Descent [23]	Computes the gradient of the entire dataset before performing parameter update	Algorithm for optimizing neural networks. Find minima, controls variance and updates model's parameters that leads to convergence.	Computation of gradient for entire dataset before performing updates slows convergence. It also calculates redundant updates for huge datasets.	Stochastic gradient descent (SGD) was developed [24]
Stochastic Gradient Descent (SGD) [24]	Performs parameter update for every training example	Network learning happens per training example. Convergence is faster.	Frequent updates complicate convergence to exact minimum. It can also lead to overshooting.	Momentum was developed [25,26]
Momentum [25,26]	Accelerates SGD by navigating along the relevant direction while discouraging oscillations in irrelevant directions.	Tackles the problem posed by high variance oscillations in SGD as it performs parameter updates for relevant examples only. Enhances faster and stable convergence as well as reduces oscillations.	High momentum as the minima (the lowest point on the curve) is reached could slow convergence. This potentially could cause the loss function to miss the minima completely and rather continue to move up.	Nesterov accelerated gradient (NAG) was developed [27]
Nesterov Accelerated Gradient (NAG) [27]	Computes the gradient after making a big jump premised on previous momentum. Thereafter, it makes a correction which culminates in a parameter update.	Prevents the loss function from decreasing too fast so that it does not miss the minima. It equally makes the convergence process to be more responsive to changes.	Though momentum and NAG adapt updates to the slope of error (loss) function thereby speeding up SGD, there is need to adapt updates to each parameter.	Adagrad was developed [28]
AdaGrad (Adaptive Gradient) [28]	AdaGrad enables the learning rate (η) to adapt based on the parameters and this ensures big updates for infrequent	It supports per-parameter learning rate and this improves performance when used on problems with sparse gradients.	The learning rate (η) is constantly reducing and decaying. This	AdaDelta was developed [29]

	parameters and small updates for frequent parameters.	Manual tuning of learning rate is not necessary	results in extremely slow convergence, prolonged neural network training time, and slow learning speed.	
AdaDelta [29]	Adadelta limits the number of accumulated previous gradients to certain constant size w	Efficient storage management as it preserves recursively definitions of the sum of gradients as a decaying mean of past squared gradients instead of storing all previous squared gradients. It doesn't require setting a default learning rate.	Though it calculates individual learning rates for each parameter, it is unable to calculate individual momentum changes for each parameter and store them separately.	Root Mean Square Propagation (RMSProp) was developed [30]
Root Mean Square Propagation (RMSProp) [30]	Adapts the parameter learning rates based on first moment (the mean)	Computes individual momentum changes for each parameter and stores them separately.	Uses only first moment of gradients.	Adam was developed [12]
Adam (Adaptive Moment Estimates) [12]	The algorithm computes an exponential moving average of the gradient and the squared gradient, and the parameters beta1 and beta2 control the decay rates of these moving averages.	Adam is a popular algorithm in the field of deep learning because it achieves good results fast.	There is room for improvement in terms of convergence rate and training time.	Aiona – proposed algorithm in this present study

- THE PROPOSED ALGORITHM, AIONA

You The above-mentioned algorithms have performed well in practice and in particular, Adam is reputed to make gains over other adaptive learning-method algorithms [12]. This is because it converges quiet fast coupled with the fact that the learning speed of the neural network model is efficient and pretty fast. Adam also rectifies all problems faced in other optimization techniques. These issues include slow convergence, vanishing learning rate, and high variance in the parameter updates which results in fluctuating loss function. Nonetheless, there is room for improvement as acknowledged by [11]. This is the motivation for our efforts toward a better SGD algorithm.

The quest for further improvement, especially with a view to fast-tracking solution to non-convex high dimensional problems like a DNN-based LA, has led to the proposal for a method called Aiona in this present study. Aiona is a modification of Adam. It calculates adaptive learning rates for each parameter. Like AdaDelta, it stores exponentially decaying average of previous squared gradients V(t). And like Momentum and Adam, Aiona preserves an exponentially decaying average of past gradients M(t). However, its unique feature is that it introduces a third parameter, β3, for storing an exponentially decaying average of past cubed gradients E(t). The pseudocode of Aiona is shown in Algorithm 1.

Algorithm 1 Aiona: Modified version of Adam algorithm. Good default settings for the tested machine learning problems carried over from Adam are $\alpha = 0.001$, $\beta_1 = 0.9$, $\beta_2 = 0.999$ and $\varepsilon = 10^{-8}$. For the introduced parameter β_3 specific to Aiona, the default value is $\beta_3 = 0.997$.

Require: α: Stepsize
Require: $\beta_1, \beta_2 \in [0, 1)$: Exponential decay rates for the 1st and 2nd moment estimates
Require: $\beta_3 \in [0, 1)$: Introduced exponential decay rate for the 3rd moment estimate
Require: $f(\theta)$: Stochastic objective function with parameters (θ)
Require: θ_0: Initial parameter vector
$m_0 \rightarrow 0$ (Initialize 1st moment vector)
$v0 \rightarrow 0$ (Initialize 2nd moment vector)
$e_0 \rightarrow 0$ (Initialize 3rd moment vector)
$t \rightarrow 0$ (Initialize timestep)
while θ_t not converged **do**
$t \rightarrow t + 1$
$g_t \rightarrow \Delta\theta f_t(\theta_t{-}1)$ (Get gradients w.r.t. stochastic objective at timestep t)
$m_t \rightarrow \beta_1 . m_t{-}1 + (1 - \beta_1) \cdot g_t$ (Update biased first moment estimate)
$v_t \rightarrow \beta_2 \cdot v_t{-}1 + (1 - \beta_2) \cdot g_t^2$ (Update biased second raw moment estimate)
$e_t \rightarrow \beta_3 \cdot e_t{-}1 + (1 - \beta_3) \cdot g_t^3$ (Update biased third raw moment estimate)
$\acute{m}_t \rightarrow m_t/(1 - \beta_1{}^t)$ (Compute bias-corrected first moment estimate)
$\acute{v}_t \rightarrow v_t/(1 - \beta_2{}^t)$ (Compute bias-corrected second raw moment estimate)
$\acute{e}_t \rightarrow et/(1 - \beta_3{}^t)$ (Compute bias-corrected third raw moment estimate)
$\theta_t \rightarrow \theta_{t-1} - \alpha \cdot \acute{m}_t / (\acute{e}_t \sqrt{\acute{v}_t} + \varepsilon)$ (Update parameters)
end while
return θt (Resulting parameters)

From Algorithm 1 above, it is apparent that instead of adapting parameter learning rates based only on first moment (the mean) as in RMSProp [30] or based on first and second moments as in Adam [12], Aiona adapts parameter learning rate based on three moments of gradients – first, second and third moments. The algorithm computes respective exponential moving averages of the gradients, the squared gradients, and cubed gradients using parameters β_1, β_2, and β_3 to control the decay rates of these moving averages. Given gradients g_1, g_2,…,g_n, the sth moment of the gradients is obtained using the formula [31]:

$$(g_1^s+g_2^s+\ldots+g_n^s)/n$$

Since the initial values of the moving averages, beta1 (β_1), beta2 (β_2) and beta3 (β_3) can give rise to bias of moment estimates towards zero, some measures are put in place in the algorithm to address this issue. In the first instance, the bias is overcome by calculating the biased estimates (m_t, v_t, and e_t). Thereafter, bias-corrected estimates ($\acute{m}_t$, $\acute{v}_t$, and $\acute{e}_t$) are computed.

To facilitate good and fast results from neural network models, the proposed Aiona stochastic optimization algorithm does not only calculate individual learning rates for each parameter, it computes individual momentum changes for each parameter and stores them separately. The introduction of a third moment is a strategy aimed at further smoothening learning rate decay so that it doesn't get so small that neural network learning begins to foot-drag. For example, prolonged network training will discourage users of DNN-based LA system from patronizing the application. In addition, the introduction of the third moment of gradients will ensure only relevant parameter updates are done with a view to giving Aiona some advantage over Adam in terms of convergence rate and network training (learning) speed.

Already, it has been established that Adam (which Aiona extends) performs well in practice and competes favourably with other established SGD algorithms [12]. It is noteworthy that Adam has addressed problems faced by other SGD algorithms such as slow convergence, vanishing learning rate, and high variance in parameter updates which can result in fluctuating loss function.

- IMPLICATIONS OF AN IMPROVED STOCHASTIC GRADIENT DESCENT FOR DNN-BASED LEARNING ANALYTICS

DNN is known for its rigorous and thorough approach towards pattern recognition and forecasting [9,10]. It is also adequate in handling large models and high dimensional datasets such as medical students' data that are highly structured. As a result, outcomes are highly reliable and the information generated could be used by critical stakeholders in higher education and health sector for high-precision decision making. Such informed decision making would result in strategic interventions such as adaptive learning techniques that promote rich learning experience, encourage student retention, and galvanize student progression.

One of the concerns of researchers and stakeholders of ANN-based LA is the training time of neural networks [7]. Prolonged training time of DNN means that DNN-based LA systems could delay in providing robust and reliable information for decision making. Hence, we proposed a new algorithm called Aiona. The aim of Aiona is to speed up convergence rate in the direction of the local minimum. The algorithm is to be tested and benchmarked against established SGD algorithms. DNN-based LA will be enhanced should outcomes of the experiment indicate that a cutting edge SGD algorithm has emerged in Aiona.

- FURTHER WORK

The study examined existing SGD algorithms with a view to improving on them in terms of convergence rate and learning speed of neural networks. In the immediate future, we would ascertain if Aiona outperforms established SGD algorithms. This will be achieved by taking turns to test deep learning models like RNNs and CNNs with these algorithms on benchmark learning analytics tasks of pattern recognition (classification of medical students learning behaviours) and predictive analytics (forecasting of academic performance) using medical students' datasets (MBBS600 and BDS600). The series of experiments will determine if Aiona has gains over popular SGD algorithms like Adadelta, RMSProp, and Adam. Also, to encourage further research in the area of continuous improvement of SGD, the study will make public the experiments and code of Aiona.

- CONCLUSION

This study identified a problem in the health sector and gathered data from a College of Medicine for survey. Specifically, Universal Health Coverage, a global health initiative, is being challenged by shortage of high-level medical personnel like medical doctors and dentists. Survey into medical education that provides these critical human assets revealed low student retention rate, poor learning experience, high drop-out rate, and low student progression rate in medical schools. As a solution, we advocated and tested, on a prototype basis, a DNN-based LA system that will enhance data-driven pedagogy through the formulation of adaptive learning strategies. Such strategic interventions will be based on the unbiased, reliable, and robust information obtainable from the system. The interventions are envisaged to promote rich learning experience, encourage student retention and student progression in medical schools. Our study also revealed that existing SGD algorithms for training neural networks could be improved upon for faster convergence rate, better training time, and richer end-user experience. In response, we proposed a new method known as Aiona, an extension of Adam algorithm. Aiona will be benchmarked against well-known SDG algorithms to ascertain its efficacy. The study also adds DNN-based LA as

an empirical deep learning application to the growing body of deep learning libraries.

REFERENCES

Figure 15.
lobal Burden of Disease Health Financing Collaborator Network, "Trends in future health financing and coverage: future health spending and universal health coverage in 188 countries 2016–40", Lancet 2018; 391: 1783–98, Published by Elsevier Ltd, Open Access article under the CC BY 4.0 license.

Figure 16.
.I. Okpani and S. Abimbola, "Operationalizing universal health coverage in Nigeria through social health insurance", Nigerian Medical Journal, Niger Med J. 2015 Sep-Oct; 56(5): 305–310.

Figure 17.
. Olawale and G. Orogun, "One doctor still attends to 6,000 patients in Nigeria – Don", The Vanguard, January 26, 2017.

Figure 18.
orld Health Statistics, World Health Organization, WHO Press 2011, Switzerland.

Figure 19.
. Okewu and O. Daramola, "Design of a Learning Analytics System for Academic Advising in Nigerian Universities", IEEE Xplore Digital Library 2017.

Figure 20.
AK 2011, 1st International Conference on Learning Analytics and Knowledge 2011, February 27-March 1, 2011, Banff, Alberta.

Figure 21.
. Okewu and P. Adewole, "Artificial Neural Network-Based Learning Analytics Technique for Employability and Self-Sustenance", The Journal of Computer Science and its Applications (JCSA), Vol.25 No.2., 2018.

Figure 22.
. Ali, M. Hatala, D. Gaševic, and J. Jovanovic, "A qualitative evaluation of evolution of a learning analytics tool", Computers & Education 58 (1): 470–489, 2012.

Figure 23.
. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks", DIRO, Universit´e de Montr´eal, Montr´eal, Qu´ebec, Canada.

Figure 24.
. Li, L. Deng, L. Tian, H. Cui, W. Han, J. Pei, and L. Shi, "Training deep neural networks with discrete state transition", Neurocomputing, Volume 272, 10 January 2018, Pages 154-162.

Figure 25.
. Koushik and H. Hayashi, "Improving Stochastic Gradient Descent With Feedback", conference paper at ICLR 2017.

Figure 26.
. Kingma and J. Ba, "Adam: A method for stochastic optimization", Published as a conference paper at ICLR 2015.

Figure 27.
.T. Tran, A. Iosifidis, and M. Gabbouj, "Improving efficiency in convolutional neural networks with multilinear filters", Neural Networks, Volume 105, September 2018, Pages 328-339.

Figure 28.
. Li, T. Zhou, and C. Wang, "On global convergence of gradient descent algorithms for generalized phase retrieval problem", Journal of Computational and Applied Mathematics, Volume 329, February 2018, Pages 202-222.

Figure 29.
. Anandkumar, "Nonconvex optimization: Challenges and Recent Successes", ICML2016 Tutorial.

Figure 30.
.F. Ipaye, "Forty Years of the College of Medicine, University of Lagos (1962 – 2002), The College through their Eyes", 2002, ISBN 978-056-277-X.

Figure 31.
. Fisher, H. Selikowitz, M. Mathur, and B. Varenne, "Strengthening oral health for universal health coverage", The Lancet, Available online 25 July 2018.

Figure 32.
. Miller, V. Toffolutti, and A. Reeves, "The enduring influence of institutions on universal health coverage: An empirical investigation of 62 former colonies", World Development, Volume 111, November 2018, Pages 270-287.

Figure 33.
. Fage-Butler, "Qualifying the promise of Universal Health Coverage", The Lancet, Volume 392, Issue 10144, 28 July–3 August 2018, Page 279.

Figure 34.
.J. Culyer and K. Chalkidou, K., "Economic Evaluation for Health Investments En Route to Universal Health Coverage: Cost-Benefit Analysis or Cost-Effectiveness Analysis?", Value in Health, Available online 26 July 2018.

Figure 35.
.R. Lu and T. Chiang, "Developing an adequate supply of health services: Taiwan's path to Universal Health Coverage", Social Science & Medicine, Volume 198, February 2018, Pages 7-13.

Figure 36.
. Mercier, F. Poirion, and J. Désidéri, "A Stochastic Multiple Gradient Descent Algorithm", European Journal of Operational Research, 31 May 2018.

Figure 37.
. Kim and J.A. Fessler, "Optimized first-order methods for smooth convex minimization", Math. Prog. 151:8-107, Sep. 2016

Figure 38.
. Mei, "A mean field view of the landscape of two-layer neural networks", Proceedings of the National Academy of Sciences 2018.

Figure 39.
. Sutskever, J. Martens, G. Dahl, and G.E. Hinton, (Sanjoy Dasgupta and David Mcallester, ed.) "On the importance of initialization and momentum in deep learning", (PDF). In Proceedings of the 30th international conference on machine learning (ICML-13), 2013, 28. Atlanta, GA. pp. 1139–1147.

Figure 40.
.E. Rumelhart, G.E. Hinton, and R.J. Williams, "Learning representations by back-propagating errors", Nature. **323** (6088): 533–536, 1986.

Figure 41.
. Nesterov, Published research paper, 1983

Figure 42.
. Duchi, E. Hazan, and Y. Singer, "Adaptive subgradient methods for online learning and stochastic optimization", Journal of Machine Learning Research, 12(Jul):2121–2159, 2011.

Figure 43.
.D. Zeiler, "Adadelta: an adaptive learning rate method. 2012

Figure 44.
. Tieleman and G. Hinton, "Lecture 6.5-rmsprop: Divide the gradient by a running average of its recent magnitude", COURSERA: Neural Networks for Machine Learning, 4(2), 2012

Figure 45.
. Davies and A. Dembinska, "Computing Moments of Discrete Order Statistics from Non-identical Distributions", Journal of Computational and Applied Mathematics, Volume 328, 15 January 2018, pages 340 – 354.

Dual Biometrics And Elliptic Curve Cryptography Based E-Commerce Security (C004)

Onuja, Abdulkarim Musa
Department of Computer Science
Federal University of Technology Minna,
Minna, Nigeria
e-mail: onuja14@gmail.com

Oyefolahan, Ishaq Oyebisi
Department of Information and Media Technology
Federal University of Technology Minna,
Minna, Nigeria
e-mail: ishaq.flhn@gmail.com

***Abstract*—This paper presents a preliminary result of an ongoing research which integrates elliptic curve cryptography (ECC) with biometrics as a methodology to improve the security of electronic commerce (e-commerce) transactions. While an existing system use the iris of bank clients to generate cryptographic keys for ECC, this paper use the iris and voice biometrics for authentication given that ECC has the capacity to generate encryption and decryption keys. The model is to be implemented on webservers that serves as electronic commerce platforms. The experimentation of the methodology shows a promising model that makes it harder for malicious hackers to compromise transactions on e-commerce platforms. It supports the drive for a cashless economy and payment for goods in instalments.**

Keywords-Biometrics; ECC; E-Commerce Security; RSA

• INTRODUCTION

E-commerce is a powerful tool for business transaction and transformation that allows companies to enhance their supply-chain operation, reach new markets, and improve services for customers as well as for service providers [20]. E-commerce websites are not only tools to support a business transaction, but also companies' channels to interact and communicate with their consumers [10]. In the retail industry, websites for business-to-consumer e-commerce (B2C ecommerce) provide more accessible, easier, faster, and cheaper methods for individual consumers to conduct their retail transactions [9]. As individuals and businesses increase information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases [20]. Consequently, the future of B2C e-commerce may well depend on the selling firm's ability to manage security threats and improve consumer perceptions of Internet security [9].

Cryptography is a process of making information unintelligible to an unauthorized person, hence, providing confidentiality to genuine users of online internet infrastructure. There are various cryptographic algorithms that can be used [17]. The most commonly used algorithms as listed by [17], this include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advance Encryption Standard (AES), Rivest, Shamir and Adelman (RSA) and blowfish. Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA [18].

TABLE I Application of Public-Key Cryptosystems [18]

Algorithms	**Table Column Head**		
	Encryption/d decryption	***Digital signature***	***Key exchange***
RSA	Yes	Yes	Yes
ECC	Yes	Yes	Yes

It is widely used to secure information channels and gateways such as the web traffic, electronic mails, scientific information about innovation and new technologies, and e-commerce transactions. Table I reveals ECC matches RSA in utilization as both cryptographic algorithms can be used for encryption and decryption, digital signature, and key exchange.

The computational effort required in the cryptanalysis of symmetric key algorithms, that includes RSA and ECC has been compared to discover that ECC use about one-eighth of the key-size used in RSA to offer the same level of security, as shown in table II. The Table presents public-key cryptography [18] such as RSA algorithm and elliptic curve cryptography (ECC), as the key length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. A competing algorithm that challenges RSA is the ECC. It is showing up in standardization efforts, including the IEEE P1363 Standard for Public-Key Cryptography [18].

COMPARABLE KEY-SIZE IN TERMS OF COMPUTATIONAL EFFORT FOR CRYPTANALYSIS (STALLINGS, 2014; NIST SP-800-57)

RSA(size of n in bits)	***ECC(size of n in bits)***
1024	160 – 223
2048	224 – 255
3072	256 – 383
7680	384 – 511
15360	512+

- RELATED WORK

  - *Literature Review*

Mahto and Yadav [14] worked on the security of One-Time Password by using the irises of bank clients for generating their cryptographic keys, and then the keys are used in ECC to provide data communication security while sending the one-time password (OTP) from OTP Transaction Server to client. ECC could have been allowed to generate its own cryptographic keys as it has the power of securely exchanging keys while the use of irises of the clients could have served as an outright addition of another security measure as proposed in this paper titled dual biometrics and elliptic curve cryptography based electronic commerce security.

Computer networks provide platform to do e-commerce tasks, online banking, and sharing of information [22]. Security is required for dual purposes; to protect customers' privacy, and to protect against fraud [7, 22]. While more than two parties communicate to each other, they worry about confidentiality, data authentication, nonrepudiation [15, 22]. In order to mitigate these issues, [22] apply cryptography with biometric features. The identification and authentication of an individual using cryptography and biometrics, provides high assurance in its security model [21, 22]. Mahto & Yadav [22] proposed an algorithm for enhancing the security of OTP using ECC with palm-vein biometric. The major influence of ECC compared to prevalent and commonly used public key cryptography such as RSA in computing devices, is that it offers higher security per bit with smaller key size [1, 22]. The proposed model is able to handle encryption and decryption technique problems such as key privacy, key storing and management as achieved from the results of implementation. However, the size of palm-vein print to be captured has an effect on the ease of use and deployment and does not support the portability of computing and capturing devices.

  - *Research Framework*

The research framework include the comparative study of two cryptographic algorithms that results in the understanding that ECC and RSA can both perform encryption and decryption, digital signature, and key exchange. The memory requirements of the two schemes were put into considerations as discussed in the introduction. The integration of iris and voice biometrics with ECC is discovered to maintain a lesser memory space requirement after implementation. The security of the system is improved with these additional security measures. Fig. I illustrate the steps involved in the research framework.

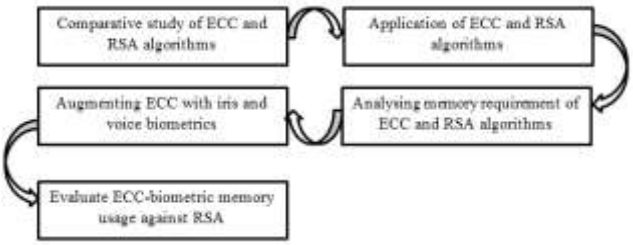

Fig. I Illustrates the steps involved in the research design

  - *Elliptic Curve Cryptography (ECC)*

Elliptic Curve Cryptography (ECC) [12] is used to establish a session-key with forward secrecy property, due to its capacity to provide a high level of security with a smaller key-size. The security of the ECC lies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), and it can achieve same security as of RSA with the key of fewer bits [23]. The elliptic curve (EC) is given by;

$Ep(a, b) : y2 = x3 + ax + b \pmod p$ … Equation (1)

Over a finite field Fp of prime order $p > 3$,

Where, $a, b \in Fp$, on the condition that;

$4a^3 + 27b^2 \neq 0 \pmod p$ … Equation (2)

  - *Iris Biometric*

The iris of the human eye is a circular portion between pupil and sclera [14]. Iris is gaining a lot of attention nowadays due to its distinctiveness, and non-counterfeiting attributes [8, 14], texture pattern [4, 14] and other minute characteristics. Iris compared to other biometrics traits provides reliable and accurate user identification method [4, 14]. Fig. II present the picture of a well labelled human iris biometric

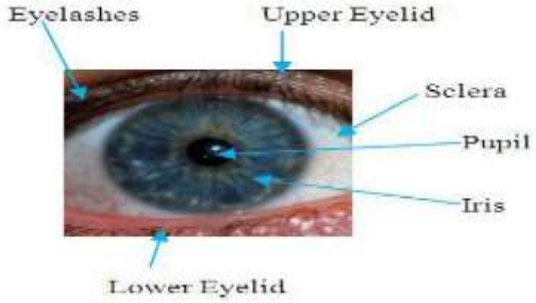

Fig. II Iris Biometric [11]

- *Voice Biometric*

Human beings have been recognized by appearance, gait, and voice for thousands of years [22]. Fingerprint-based and iris-based techniques are more accurate than the voice-based technique [16]. However, in some applications such as tele-banking applications, the voice-based technique can be integrated seamlessly into the existing telephone system [3, 16]. This informed the choice of using voice biometric to complement the use of iris in this research work. Fig.III illustrates voice biometric signal.

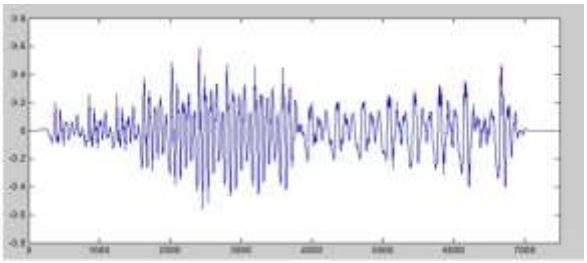

Fig. III Illustrates voice signal (https://archive.cnx.org)

- METHODOLOGY

- *Proposed Model for ECC Augmented with Biometrics*

It can be inferred from [24] that the use of ECC is more efficient since it is established that a key length size of 255 bits of ECC will have the strength of 2048 bits key-size of RSA algorithm with reference to table I. Consequently, current research in e-commerce security is interested in the use of ECC as it reduces overhead cost with respect to the memory size required for the encryption key in ECC [24]. More so, the algorithm also suits new mobile computing devices such as smart phones that can equally be used to access e-commerce websites. This work is focussed on taking advantage of the memory space afforded by using ECC to integrate another security measure in the form of iris and human voice biometrics to improve on the security of e-commerce as shown in the proposed model in fig. IV. The mnemonics used in the proposed model include customer order information (COI), that list all the items the customer want to purchase with their respective prices added to a digital cart and calculate the total cost to be forwarded to the e-commerce website server for processing. The payment order information (POI) enumerates all information required to effect online payment. Information such as Automated Teller Machine (ATM) card number, expiry date, personal identification number (PIN), amount to be paid, name of the customer, address and phone number are categorized as payment order information (POI). The proposed model also has the automated ECC encryption key as ECC_{EK} and the decryption key as ECC_{DK}. The e-commerce website server verifies customer's information by sending verification request to the bank that issues the ATM card used for the transaction and then matches it against the one on the bank account before sending feedback to the customer with the usual one time password (OTP) and then display a digital receipt to be printed for documentation after a successful transaction.

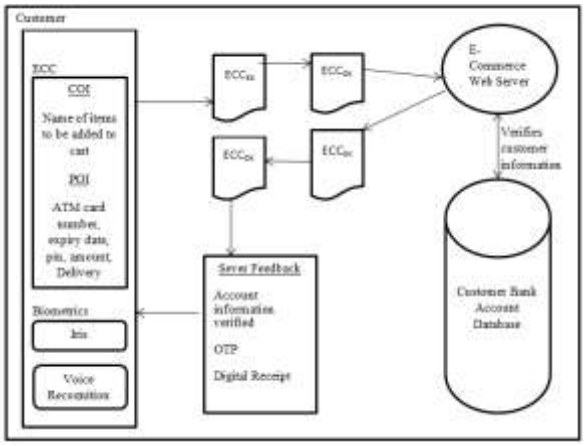

Fig. IV Model diagram for ECC Augmented with Biometrics

- *Operation of the Proposed Model*

The system requires the registration of new customers on the e-commerce platform or website to facilitate subsequent commercial transactions until the customer's user account is deleted from the database on the request of the customer. The new customer registration details include names, address, phone number, e-mail address, date of birth, capturing of iris and the recording of voice preferably a native dialect statement. The personal information of a customer already used for registration is matched against information submitted to effect transaction, including automated teller machine (ATM) card details. The customer order information (COI) and payment order information (POI) are secured traditionally by using the RSA algorithm in the mechanism of security collectively called Pretty Good Privacy (PGP) but with lower overhead cost of ECC, ECC is gaining prominence instead. And to solve the authentication problem in ECC that is not practical, this research adds biometrics in the form of iris data capturing and native language voice recognition. The online platform or websites request to capture biometrics and other personal information used for registration to be matched with those in the database. The server then allows for a successful payment if records are verified to be correct. Otherwise, it will not allow payments to be made to avoid security breach due to repudiation. Fig. V shows the flow chart describing the operation.

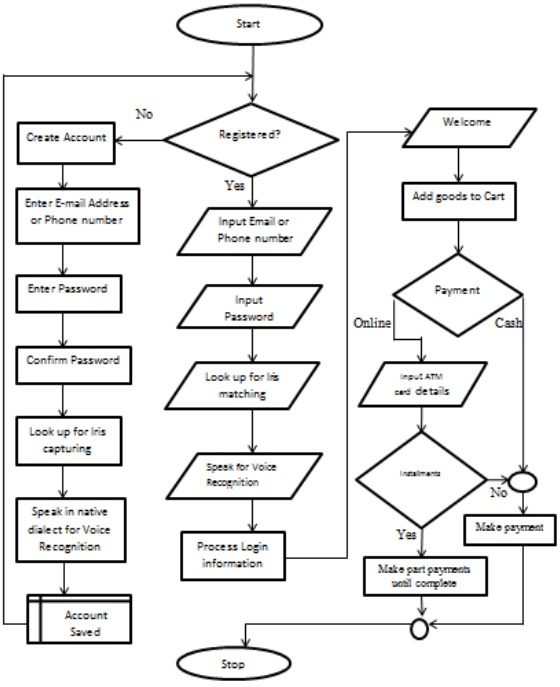

Fig. V Flowchart diagram for the model

- RESULTS

The preliminary findings of the integrated ECC-Biometric model is tabulated in Table 3, where n is key in kilobytes (kb) and $Sum_{e\text{-}iv}$ is the sum of ECC, iris data, and voice data in kilobytes (kb). NIST recommended key-sizes for ECC and RSA are minimum of 20 bytes and 128 bytes respectively [2].

ANALYSIS OF THE SIZE OF ECC-BIOMETRIC MODEL AND RSA

	ECC-Biometrics Model			
RSA (size of n kb)	ECC (size of n kb)	Iris (kb)	Voice (kb)	$Sum_{e\text{-}iv}$
8.192	1.200	6.224	9.211	16.635
16.384	2.400	6.804	7.352	16.556
32.768	4.800	7.344	6.812	18.956
65.536	9.600	8.343	7.568	25.511
131.072	19.2	5.802	6.800	31.802
262.144	38.4	6.612	6.733	51.745

The collections of dataset used for the testing of implementation focused on the use of image capturing device to capture the eyes and voices of volunteers. Image and audio processing were used to process the data to reduce noise. The sum of the key-size of ECC, Iris and Voice biometrics in the model were found to be higher when the key-size of RSA and ECC is less than 32 and 4.8 kb respectively. The key size of RSA is found to be much higher than the model when the key size is greater than 32 kb for RSA and 4.8 kb for ECC. The memory requirement for the model becomes less significant as we continue to double the key size of ECC from 19.2 kb upward while biometrics dataset maintains a normal distribution. The paper is an expression of an idea that is hoped to be updated with results from standard iris and voice capturing and matching tools in the near future. It is to be deployed practically on e-commerce webservers.

- CONCLUSION

The paper models a system that improves e-commerce security using dual biometric traits and ECC. The data used in the preliminary work can replaced with values from standard iris and voice capturing and matching tools in the near future. It is to be deployed practically on e-commerce platforms such as web applications and websites. .

REFERENCES

Figure 46. E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, ''Recommendation for key management part 1: General (revision 3),'' NIST special publication, 800(57), 1-147. 2012.

Figure 47. S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, ''An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography,'' Journal of Medical Systems, DOI 10.1007/s10916-015-0335-y, 2015.

Figure 48. A. K. Das, ''Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards,'' IET Information Security, vol. 5, no. 3, pp. 145–151, 2011.

Figure 49. J. Daugman, and C. Downing, ''Epigenetic randomness, complexity and singularity of human iris patterns,'' Proceedings of the Royal Society of London B: Biological Sciences, 268 (1477), 2001, pp. 1737-1740.

Figure 50. J. Daugman, ''New methods in iris recognition, systems, man, and cyber- netics, Part B: Cybernetics,'' IEEE Transactions, 37 (5), 2007, 1167-1175.

Figure 51. X. Fang, S. Chan, J. Brzezinski, and S. Xu, ''Moderating effects of task type on wireless technology acceptance,'' Journal of Management Information Systems, 22, 2006, 123–157.

Figure 52. R. Ganesan, and K. Vivekanandan, ''A secured hybrid architecture model for internet banking (e-banking),'' Journal of Internet Banking and Commerce, 14(1):1–17, 2009.

Figure 53. F. Hao, R. Anderson, and J. Daugman,'' Combining crypto with biometrics effectively,'' IEEE Transactions on Computers. 55 (9), 2006, 1081-1088 doi:10.1109/TC.2006.138.

Figure 54. E. Hartono, C. W. Holsapple, K. Y. Kim, K. S. Na, and J. T. Simpson, ''Measuring perceived security in B2C electronic commerce website usage: A respecification and validation Decision Support Systems 62 11–21 http://dx.doi.org/10.1016/j.dss.2014.02.006, 2014.

Figure 55. https://archive.cnx.org/contents/fcbd1f34-bb85-442c-b25d-bd5204aea692@1/speak-and-sing-time-scaling-with-wsola

Figure 56. S. P. Jogi, and B. B. Sharma, ''Methodology of iris image analysis for clinical diagnosis,'' IEEE International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), (pp. 235-240). doi:10.1109/MedCom.2014.7006010, 2014.

Figure 57. S. Kumari, X. Li, F. Wu, A. K. Das, K. K. R. Choo, and Shen, J. ''Design of a provably secure biometrics-based multi-cloud-server authentication scheme,'' Future Generation Computer Systems, 68, 320-330, 2017

Figure 58. D. Mahto, and D. K. Yadav, ''Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce,'' Applications International Conference on Computer, Communication, Control and informatics. www.springer.com 2017

Figure 59. D. Mahto, and D. K. Yadav, ''One-time password communication security improvement using elliptic curve cryptography with iris biometric,'' International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18, 2017, pp. 7105-7114 Research India Publications http://www.ripublication.com

Figure 60. S. Mohammadi, and S. Abedi, ''ECC-based biometric signature: A new approach in electronic banking security,'' International Symposium on Electronic Commerce and Security pages 763–766, August, 2008.

Figure 61. V. Odelu, A. K. Das, and A. Goswami, ''A secure biometrics-based multi-server authentication protocol using smart cards,'' IEEE Transactions On Information Forensics And Security DOI 10.1109/TIFS.2015.2439964, 2015

Figure 62. P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, ''A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,'' Procedia Computer Science, 78, 617-624, 2016.

Figure 63. W. Stallings, ''Cryptography and network security principles and practice,'' Sixth Edition, 2014.

Figure 64. Y. W. Sullivan, D. J. Kim, ''Assessing the effects of consumers' product evaluations and trust on repurchase intention in e-commerce environments,'' International Journal of Information Management 39, 199–219 https://doi.org/10.1016/j.ijinfomgt.2017.12.008, 2017.

Figure 65. S. Yasin, K. Haseeb, and R. J. Qureshi, ''Cryptography based e-commerce security: a review,'' International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012, ISSN (Online): 1694-0814.

Figure 66. P. Zhang, J. Hu, C. Li, M. Bennamoun, and V. Bhagavatula, ''A pitfall in fingerprint bio-cryptographic key generation,'' Computers & Security, 30(5), 311-319, 2011.

Figure 67. D. Mahto, and D. K. Yadav, ''Enhancing security of one-time password using elliptic curve cryptography with biometrics for e-commerce applications,'' International Conference on Computer, Communication, Control and informatics, 2015. www.springer.com

Figure 68. S. H. Islam, and G. P. Biswas, ''Design of improved password authentication and update scheme based on elliptic curve cryptography,'' Mathematical and Computer Modelling, 57(1112), 2703-2717, 2013.

Figure 69. K. Ahmad, and M. S. Alam, ''E-commerce security through elliptic curve cryptography,'' *Procedia Computer Science, 78,* 867-873, 2016

Implementation of Modified Pull-All Data Migration for a Java-based Mobile Agent Using Coloured Petri Net (CPN) (C005)

K. Adewale, O. O. Deji-Akinpelu and O. Osunade
Dept. of Computer Science
University of Ibadan
Ibadan, Nigeria
e-mail: kikeadewale@gmail.com;
omokehindeakinpelu@gmail.com;
seyiosunade@gmail.com

B. S. Olanrewaju
Dept. of Computer Science
Wellspring University
Benin City, Nigeria
e-mail: bs.olanrewaju@gmail.com

O. T. Olanrewaju
Dept. of Computer Science
Federal College of Animal Health and Production Technology (FCAHPT)
Moor Plantation, Ibadan, Nigeria
e-mail: ayotundetaiwo@gmail.com

A. O. Okunade
Dept. of Computer Science
National University of Nigeria (NOUN)
Ibadan, Nigeria
e-mail: okunadeoluwasogo@gmail.com

A. Omilabu
Dept. of Computer Science
Tai Solarin University of Education (TASUED)
Ijebu-Ode, Nigeria
e-mail: demmysax@yahoo.co.uk

***Abstract*— During migration process, mobile agent always carries along its current data, program code and its execution state with which it will continue its execution at the destination platform. The data migrated with the mobile agent causes performance inefficiency such as increased load and lower speed of transmission for the disrupted mobile agent. Modified migration strategies have been proposed but are yet to provide sufficient empirical evidence to support performance enhancement against existing data migration strategies. This work is aimed at examining the performance of pull-all data migration pattern in mobile agent by implementing the existing and modified pull-all data migration strategy. A Java-based mobile agent with Object tool command language (Otcl) and Coloured Petri Net (CPN) in a network simulator (NS2) was used to evaluate the performance, with network load and transmission time as performance evaluation metrics. Existing mathematical models were used to represent the three stages of the pull-all data migration process including a dispatch from the home host, migration from one host to another and return to the home host. A pull-all data migration strategy was simulated using the Otcl and CPN tools in NS-2 on Ubuntu operating system. In all the evaluations, the modified pull-all data migration strategy showed a 2 second improvement over the transmission time and 100bytes lesser in terms of the network load.**

Keywords- *data migration, mobile agent, simulation, coloured petri net, performance*

• INTRODUCTION

• Mobile agent is a software program that moves from one node to another while performing given tasks. The advent of mobile agent systems signifies the beginning of one of the most important paradigm shifts in computing [1]. Mobile agents are computer programs, which are autonomous, proactive and reactive, and have ability to learn. They move from one node to another, interact with each other, and share information to achieve their goals[2]. They facilitate user's tasks in distributed systems and improve applications such as Internet, Mobile Data Computing, E-Commerce and many mobile computing areas.

•

Mobile agents are defined as objects. These objects have their state, location and behavior. Mobile agents are used in many areas such as networking, information retrieval, military, distributed systems, distributed database, and so on [3]. One of the most attractive applications for mobile agents is the notion of "distributed information processing". This is particularly clear in the mobile computing scenarios where users have portable computing devices with only intermittent, low bandwidth connections to the main network. Moreover, the mobile agent can carry on a task while the connection to the portable device is temporarily lost and then continue once the link returns to send the found result. Mobile agents can exploit the high processing power available in the server machines by shifting the computations into the server side. A large number of mobile agent systems, which differ in

mobility, implementation language, execution, communication and security, have been developed to support and provide mechanisms for the pervasive and ubiquitous computer networks that have emerged [4]. Notwithstanding, a number of data migration patterns exist in practice for code, data and execution state for a mobile agent moving from one mobile agent system to the other and consist of several steps which can be implemented using either the push or pull strategy [4].

Current data migration patterns are inefficient for mobile agents due to little empirical evidence to support performance enhancement with other data migration patterns. However, a number of modifications to the pull data migration pattern exist in principle, which needs to be ascertained for performance efficiency. In addition, most of the existing modifications are java-based and so needs further evaluation using other evaluation tools. This research work is therefore expected to implement the existing and modified pull data migration pattern in a Java-based mobile agent using a network simulator 2 and evaluate the performance of these patterns using network load and transmission time as performance evaluation metrics.

- LITERATURE REVIEW

Migration Strategies is a method to ship mobile code, execution state of the mobile agent and data the agent carries along over the network. Mobile agent migration can be used instead of communications between a server-side and a client-side program. It enables the development of distributed systems, the movement of an agent to another location in the network [5]. A mobile agent can transport or migrate its state from one environment to another with its data intact and is capable of performing appropriately in the new environment [6, 13]. A Mobile Agent is a type of software system which acts "intelligently" on one's behalf with the feature of autonomy, learning ability and most importantly mobility. More specifically, When a Mobile agent moves, it saves its own state and transport this saved state to the new host and then resumes execution from the saved state [7, 12].

- Some mechanisms and facilities have been designed and implemented to support the migration of code among the nodes of a network. Two types of code migration have been identified: Process and Object migration according [8]. Process migration is the relocation of a process from the processor on which it is executing to resume its execution seamlessly in the remote environment. Process migration facilities have been introduced at the operating system level to achieve load balancing, fault resilience and data access locality across network nodes [9]. Therefore most of these facilities provide transparent process migration, that is, the programmer has no control or visibility of migration [11].

- There are various migration strategies. One possibility is to send the complete program over the network. Another choice is whether to push code over the network, that is code will be sent over the network in advance, or to pull (download) code from a reachable location, that is the mobile agent (the execution unit) loads code from some suitable source. If the push code variant is used, code could be sent to the next location only, or to all locations on the agent's itinerary. There are two main discerned categories to transfer the code and data to the destination platform in a mobile agent technology. These are "push" and "pull". The strategy used in migration has a great impact on the mobile agent performance. One of the pitfalls of the "push strategy" is that it drives classes that could not have been used in the next locations or could never have been used at all. On the other hand, a "pull strategy" requires a fast reliable retained connection or at least a fast way to reconnect to the agent source through the agent lifetime [10].

The pull-all code migration strategy is characterized by the request for code by the mobile agent on each host it visits. The mobile agent requests for all the code units whether or not they are all required on that host [4]. The mobile agent can migrate from host to host on its itinerary with the data generated on each host.

- The need for increased access by applications and users to the data being collected by the mobile agent and the need to improve the transmission time of the mobile agents during migration necessitated the development of an alternative data migration pattern. In the modified migration strategy, the mobile agent can migrate from host to host on its itinerary without the data collected on each host. The data is transmitted to the home host before migration to the next host in an iterative manner until the mobile agent finally returns to the home host. While the transmission time comprises the time to migrate the mobile agent to the next host and the time to transfer the data collected to the home host; consequentially, the network load at an instance of time on a host is composed only of the data collected by the mobile agent on that host. For this strategy, the mobile agent migrates to a host then requests for all necessary code from a code server or agent server before execution. On migration to the next host with data, it sends the same request for code again.

[4] developed mathematical models based on the size of information transmitted across the network called network load and the time it takes the mobile agent to complete its migration from one host to the next host on the network called the transmission time or execution time. Three mathematical models were used to represent the three stages of the pull-all data migration process including a dispatch from the home host, migration from one host to another and return to the home host.

The migration process is divided into three basic stages representing distinct stages of the migration process that can be modeled. The three basic stages are:

- ***lve*:** The migration of the mobile agent from the home host (mobile agent system) to the first host on the mobile agent's itinerary i.e. the agent leaves (*lve*);
- ***mig*:** The migration between hosts on the itinerary following the specified order from the home host i.e. the agent migrates (*mig*);

- ***home:*** The migration of the mobile agent back to its home host (mobile agent system) after completion of the itinerary i.e. the agent returns home (*home*);.

This model used the network load (B) and transmission time (T) as the metrics for performance evaluation to an ordered set of hosts, represented as $L = L_1,\ldots\ldots L_m$. The agent consists of some class files which can be dynamically loaded during execution from the agent's home host. The decision on which class files must be loaded is influenced by the communication of the agent to the local agent server.

To model the network load (B), the following assumptions were made

- an agent consists of *n* units of code or *n* class files,
- each unit of code has a length or size B_c^k, k=1,…n,
- the sum of all code units is B_c
- an agent has a data of length or size B_d,
- an agent's state information is of length or size B_s
- a request to load a specific code unit has a length or size B_r
- The probability of dynamically loading code unit k on a host is P^k.
- On a host the agent's data increases by d_L bytes.

The migration is from L_a to L_{a+1} where a = 1,…..,m-1. is a host on the itinerary that is not the home host.

The migration process consists of marshalling data and state, transmitting data, state, and code to the destination host, and unmarshalling of data and state information. Marshalling is the process of suspending the mobile agent operation on a host and preparing it for migration to the next host. Unmarshalling is the reverse process where the received agent is instantiated on the receiving host.

To model the roundtrip time (T), the following simplifications are assumed:

- Marshalling and unmarshalling of data on each host is linear in time and modeled by μ: IN → IR.
- For each pair of platforms we know throughput τ: L x L → IR
- For each pair of platforms we know delay δ: L x L → IR in advance

With this information the equation for the migration strategy for the modified Pull All pattern is presented.

The models for the network load are:

$$B_{lve}(L,S) = B_c + B_r + B_s + B_d \quad \ldots\ldots 1$$

As the mobile agent moves from one host to the next host on the itinerary, it migrates with the results of its activities on each host. The network load at this stage is thus

$$B_{mig}(L,a,S) = B_d + \sum_{i=1,\ldots a} d_{Li} + B_s + B_r + B_c \quad \ldots\ldots\ldots 2$$

$$B_{home}(L,S) = B_d + \sum_{l=1,\ldots m} d_{Li} + B_s \quad \ldots\ldots\ldots\ldots\ldots 3$$

The models for the transmission time are described for the first stage, the migration from one host to another and for the last stage when it returns back to the home host.

$$T_{lve(L,S)} = 2\mu(B_d + B_s) + \delta(L_h, L_1) + \frac{B_d + B_s}{\tau(L_h, L_1)} + \delta(L_1, L_h) + \frac{B_r + B_c}{\tau(L_1, L_h)}$$

$\ldots\ldots\ldots 4$

When the mobile agent migrates from host to host on the itinerary, it migrates with the accumulation of results generated by the activity of the mobile agent. Thus, the transmission time is represented as

$$T_{mig}(L,a,S) = 2\mu(B_d + B_s + \sum_{i=1,..,a} d_{Li}) + \delta(L_a, L_{a+1}) + \frac{B_d + B_s + \sum_{i=1,..,a} d_{Li}}{\tau(L_a, L_{a+1})} + \delta(L_{a+1}, L_h) + \frac{B_r + B_c}{\tau(L_{a+1}, L_h)}$$

$\ldots\ldots\ldots\ldots\ldots 5$

$$T_{home}(L,S) = 2\mu(B_{home}(L,S) + \delta(L_m, L_h) + \frac{B_{home}(L,S)}{\tau(L_m, L_h)})$$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 6$

- METHODOLOGY

The Object tool command language (OTcl) and CPN toolboxes in NS–2 were used to model and simulate the existing and the modified migration patterns. NS-2 is a discrete-event network and packet level simulator for Internet systems, targeted primarily for research and educational use.

The model and the simulation for the existing mobile agents' pull-all migration strategy are presented in Figure 1 and Figure 2 respectively. In addition, the model and the simulation of the modified pull-all data migration strategy of the mobile agent are presented in Figure 3 and Figure 4 respectively. The models consist of 4 nodes (HostA, HostB, HostC, HostD). Each node uses a DropTail queue, of which the maximum size is 10. A "tcp" agent is attached to Home HostA, and a connection is established to a tcp "sink" agent attached to HostD. As default, the maximum size of a packet that a "tcp" agent can generate is 1KByte. A tcp "sink" agent generates and sends ACK packets to the sender (tcp agent) and frees the received packets. A "udp" agent that is attached to HostA is connected to a "null" agent attached to HostD. A "null" agent just frees the packets received. A "ftp" and a "cbr" traffic generator are attached to "tcp" and "udp" agents respectively, and the "cbr" is configured to generate 1 KByte packets at the rate of 1 Mbps. The "cbr" is set to start at 0.1

sec and stop at 4.5 sec, and "ftp" is set to start at 1.0 sec and stop at 4.0 sec.

- RESULTS AND DISCUSSION

The results generated for the existing and the modified Pull All data migration patterns are summarized and presented in Table 1. Table 1 presents the transmission time and network load for both the existing and modified Pull All migration strategy when four (4) hosts are visited with no marshalling factor at a selectivity constant ranging from 0 to 1 with a variance of 0.1. As observed, there is a very little change in the transmission time as the selectivity constant increases for both migration strategies. The network loads for both data migration strategy in the two (2) migration strategies are significantly different in value from each other. The network load decreases as the selectivity constant increases. This reduction is proportional for both data migration patterns and the migration strategies. As lower network load and transmission time interpret into better performance of the migration pattern; the results obtained from all the evaluations conducted in this research work reveal that in general, the modified data migration pattern developed produced lower network load and transmission time than the existing pattern. Consequentially, the modified data migration pattern performed optimally and efficiently in a significant manner over the existing data migration pattern.

Table 1: Transmission Time when four (4) hosts are visited with no marshalling factor

	Transmission Time		**Network Load**	
Selectivity constant (Σ)	**Existing Pull All**	**Modified Pull All**	**Existing Pull All**	406.00
0	56.91	54.67	527.00	402.50
0.1	56.87	54.61	508.00	399.00
0.2	56.69	54.598	493.00	396.50
0.3	56.46	54.56	479.50	393.00
0.4	56.225	54.52	462.00	389.50
0.5	55.98	54.496	444.00	386.00
0.6	55.86	54.43	430.00	382.50
0.7	54.735	54.405	414.00	379.50
0.8	54.48	54.399	395.50	376.00
0.9	54.32	54.38	381.00	372.50
1.0	54.20	54.346	364.00	389.36
Mean	55.703	54.492	445.27	406.00

- CONCLUSION

Network migrations are typically studied using system-dynamics and agent-based models. In this research work, the agent-based model approach was considered in which the system consists of an ensemble of agents, each trying to increase its own utility. In this research work, a Pull all data migration pattern was modified and simulated using the OTcl and CPN tools in NS-2 on a Linux operating system. In all the evaluations, the modified pull all data migration strategy showed significant improvement over the existing strategy in terms of the network load and the transmission time. Two quantifiable measurable quantities were used as evaluating metrics. The results of the simulation for the existing and new data migration patterns obtained showed that increase in the number of hosts visited for each migration strategy resulted in a significant difference between the network load and transmission time. However, when no marshalling factor is used, the results obtained showed that the modified data migration pattern had a better transmission time. When the full data collected on the host is migrated, the modified pull all data migration pattern showed a better performance over the existing one. As a result, this research work can be instrumental in the creation of more mature network applications. This set of modification and simulation can be conducted for other migration strategies to help confirm that modified versions can produce lesser network traffic and response time. In addition, Java Network Simulator (JNS), a Java-version of the Network Simulator 2 can be used to model and simulate the modified patterns to achieve standardization of results.

REFERENCES

Figure 70. Thomsen, L. L. and Thomsen, B. (1997). Mobile Agents—The new paradigm in computing Research & Advanced Technology, ICL, Bracknell, Berkshire, UK. pp. 14-40

Figure 71. Shamila, M., Subbarao, V., Wunnava, M. (2006). Application of Mobile Agents in Managing the Traffic in the Network and Improving the Reliability and Quality of Service. IAENG International Journal of Computer Science, 32(4)

Figure 72. Khalid, K. (2015). Mobile Agent: A Comparison Review. International Journal of Computer Science and Mobile Computing, Vol.4(7). pg. 122-127.

Figure 73. Osunade, O. 2007. Data Migration Patterns for Java Based Mobile Agents. PhD. Thesis, Department of Computer Science, University of Ibadan.

Figure 74. Oyediran, M. O., Fagbola, T. M., Olabiyisi, S. O., Omidiora, E. O. and Fawole, A. O. (2016). A Survey on Migration Process of Mobile Agent. Proceedings of the World Congress on Engineering and Computer Science Vol I,. San Francisco, USA.

Figure 75. Adnan, S., Datuin, J., Yalamanchili, P. (2000). A Survey of Mobile Agent Systems. http://www.cs.ucsd.edu/classes/sp00/cse221reports/dat-yal-adn.pdf,

Figure 76. Singh, Y., Gulati, K. and Niranjan, S. (2012). Dimensions and Issues of Mobile Agent Technology. International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3(5).

Figure 77. Fuggetta, A., Picco, G. P. and Vigna, G. (1998). Understanding Code Mobility. IEEE Transactions on Software Engineering. Vol 24(5).

Figure 78. Milojicic, D., Douglis, F., Paindaveine, Y., Wheeler, Y. and Zhou, S. (1999). Process Migration. University of Toronto and Platform Computing, Toronto, Canada.

Figure 79. Erfurth, C.; Braun, P. and Rossak, W. 2001. Migration intelligence for mobile agents. Retrieved July 20, 2005 from ftp.minet.unijena. de/pub/ips/cen/aisb01.ps

Figure 80. Powell, M. L. and Miller, B.P. 1983. Process migration in DEMOS/MP. Proceedings of the 9th ACM Symposium on Operating Systems Principles. ACM Press, 110-119.

Figure 81. Silva, A. and Delgado, J. (1998). The Agent Pattern for Mobile Agent Systems. 3rd European

Figure 82. Al Shrouf, F., Turani. A., Abu Baker, A. and Al Omria, A. (2014).Analysis of Mobile Agent

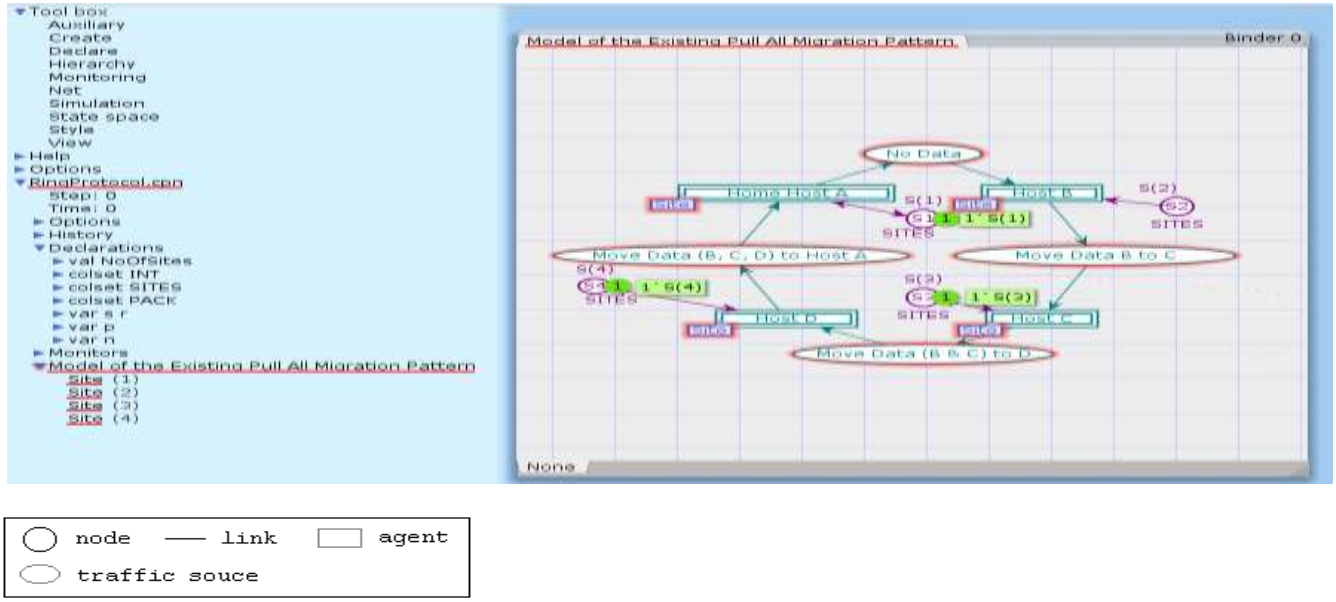

Figure 1: Model for the Existing Mobile Agent Pull All Migration

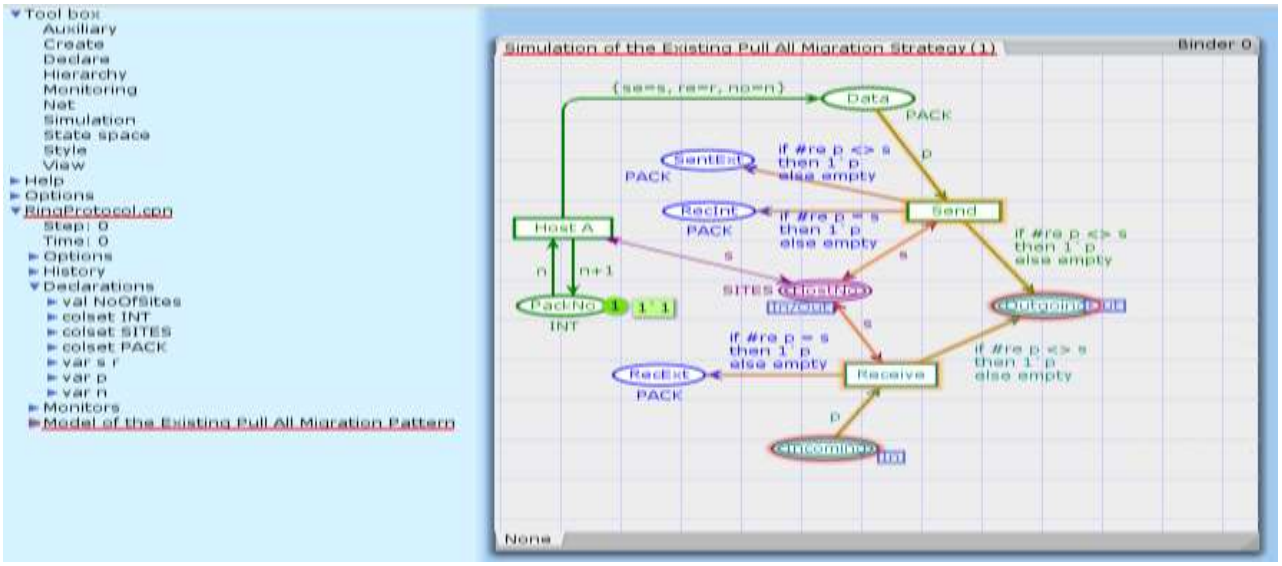

Figure 2: Simulation Interface for the Existing Mobile Agent Pull All Migration

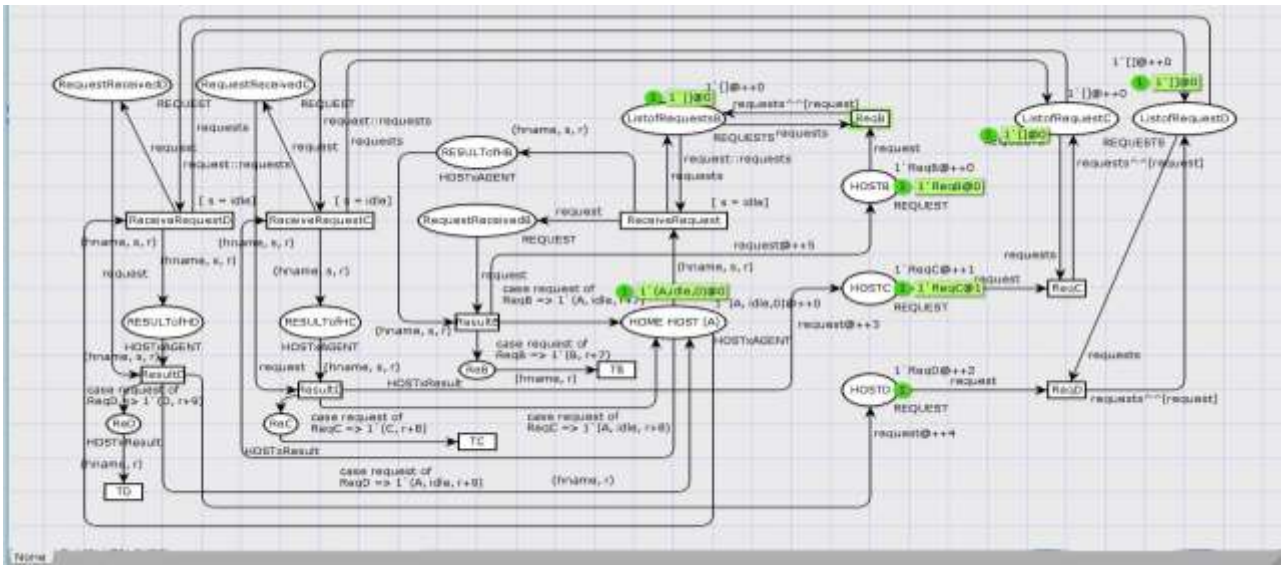

Figure 3: Model of the Modified Mobile Agent Pull All Migration

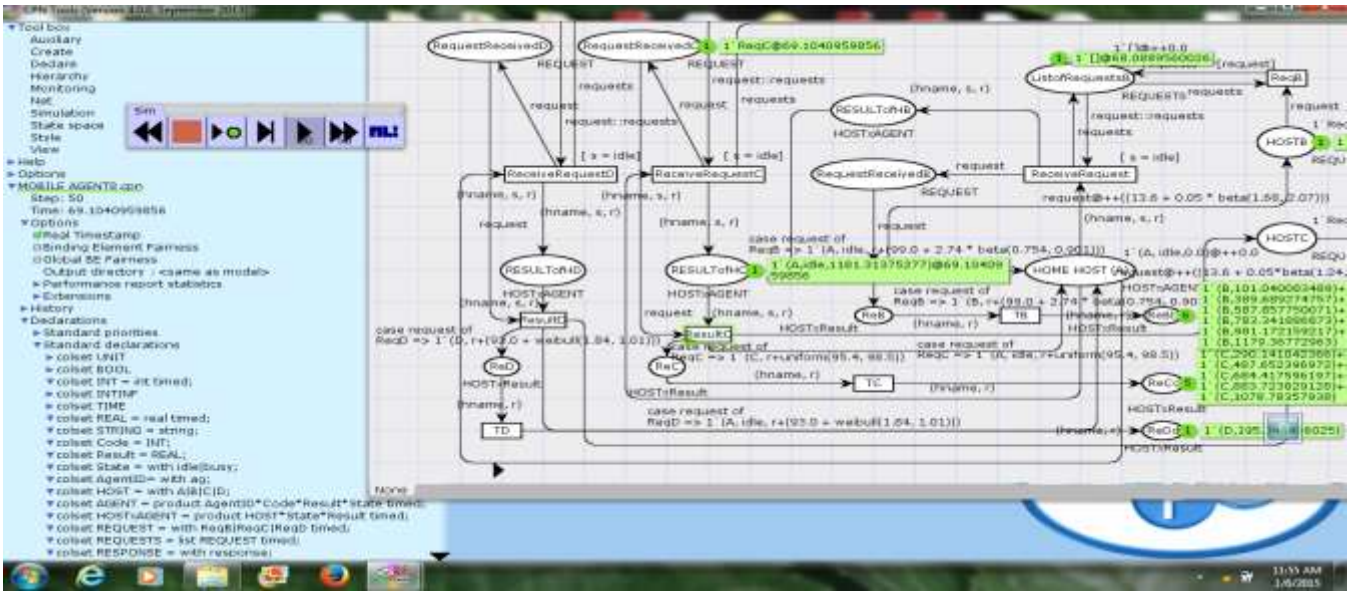

Figure 4: Simulation Interface for the Modified Mobile Agent Pull All Migration

Detection of a Real-time Cyber-attack using Locator Agent Algorithm (C006)

Isah, Abdulkadir Onivehu[1]
Idris, Ismail[3]
(1, 3) Department of Cyber Security Science
Federal University of Technology Minna,
Minna, Nigeria
ao.isah@futminna.edu.ng1
ismi.idris@futminna.edu.ng3

Alhassan, John Kolo[2]
Adebayo, Olawale Surajudeen[4]
(2, 4) Department of Cyber Security Science
Federal University of Technology Minna,
Minna, Nigeria
jkalhassan@futminna.edu.ng2
waleadebayo@futminna.edu.ng4

***Abstract*— This paper presents a preliminary result of an ongoing research work on attack prevention and location of attacks on the cyberspace. The methodology combines the preventive encryption and locative algorithms. This paper in particular, present the reviews and methodology used in achieving the first objective of the said ongoing research. The existing systems duels on methodologies that attempt mostly postmortem solutions. Whereas, this research uses advanced encryption standard as prevention against compromising confidentiality. The methodology and objective obtained so far present a promising solution of unified model algorithm for real time solution of the ongoing research problem.**

Keywords- Realtime; Cyberspace; Locator agent; Detection

- Introduction

As cyberspace based technologies are being utilized by different individuals, there is a propensity that they would be exposed to increasingly security dangers. Since network systems are utilized by various individuals, there are expanding number of security issues and security of data on transition [1] which required the improvement of various intrusion detection frameworks; such attacks are DOS attacks. SYNflood, smurf, and User Datagram Protocol (UDP) storm assaults [13]. IP traceback [14] is a strategy that is very effective to absolve attacks

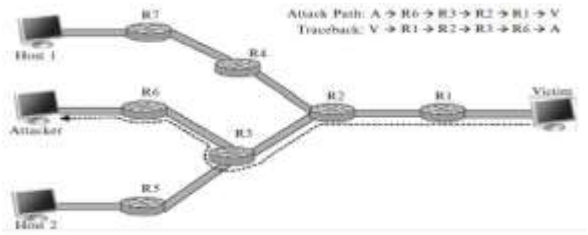

Fig. I IP Traceback Mechanism [14]

and to examine and attribute the attacks during the post-mortem analysis. The traceback system is shown in Fig. I IP traceback issue is characterized as distinguishing the real source of traffics sent over the Internet [14].

The attacks cannot be prevented or mitigated by the techniques of IP traceback. However, in this paper, other network security measures such as

public key cryptosystems, and feedback alert system are to be combined to form a hybrid system that is able to prevent, mitigate and reveal the source of attack.

- Related Work

For malicious programs or malicious packets to be detected, proper monitoring of particular activities is undertaking [8]. Anomaly detection is part of active monitoring techniques [3], detection of signature scan [10], intrusion detection systems [15], access control list [12], and honeypots [13]. Anomaly detection techniques can be utilized to create the behavior of users' pattern and network resources. Any behaviour that moves away from these particular patterns (traffic patterns that are irregular) is malicious [3]. Signature scan method is utilized to keep the mark of the activities in a database. A passive checking is performed on the system activity [10] for informal sample recognition. If the sample matches including the saved signature, it is regarded malicious. It is generally done because of recognized attacks within the network. Intrusion detection systems commonly discover intrusion based totally of pattern matching or statistical anomaly [6]. However, statistical violation identifies malicious activities based totally concerning deviations from the usual utilization pattern. The usual utilization pattern is normally established firstly before deciding a deviation within the network activities. Access control list is utilized to recognize malicious activity by coordinating packets headers with pre-characterized rules [12]. Honeypot is a trap put to screen and keep interlopers from going into secured zone of the system [10]. Honeypot is a camouflage that recreates to secure server and instigates intruders to cooperate. Along these lines, an assault is identified by checking unapproved examining of open ports in the honeypot. The authors are basically concerned with detection and not proactive in the location of the source of attack.

Identification of the source of packets within a particular network is called traceback or IP traceback [7]. It is utilized to detect origin of packets that are being generated by identifying attacks [2]. Traceback is a proper NFT used to detect packets sources by checking the path of attacks especially for DDoS and IP spoofing attacks [10]. Due to botnet, Traceback is significantly more [11] and DDoS attacks [4, 5] that are seen in various distributed systems of network. Distributed systems of network which work together with Internet give likely atmosphere and pull in bot-master for network attacks [9]. To beat these assaults, it is important to keep the system framework anchored by consolidating different traceback systems in an effective way. Although, the improvements made by the various research works are commendable, none is able to effect real-time detection of position of intrusion or attacks; it is rather a post-mortem approach. This is what the ongoing research work seeks to achieve, although, this paper covers the first objective of the research.

- Methodology

The method employed by this paper is formulation of the mathematical relationships which involves functions and variables required in the achievement of the very objective under consideration. The algorithms arising from the mathematical considerations shall be stated and the model shall be drawn out of the final unified algorithm.

  - *Mathematical Considerations*

Logically, the operations and the activations of any of the algorithm is discretely represented. The positive S_{pc} is the Systems positive communication while S_{nc} is the Systems negative communication.

$S_{pc} = 1$…….. (1)

$S_{nc} = 0$…… (2)

The unified model algorithm U_{ma} proposed is achieved by the combination of Encryption algorithm E_a and Locator agent algorithm L_{aa} where the encryption type is the AES.

$E_a + L_{aa} = U_{ma}$……. (3)

But

For equation (i),

$E_a = M_s = V_s = 1$……... (4)

$L_{aa} = M_s = V_s = 1$…….. (5)

M_s is the malicious system and the victim system is V_s

For equation (ii),

$U_{ma} = 0$…… (6)

- *General AES Algorithm*

AES algorithm is traditionally known as encrypting algorithm but it can be adapted to a wide range of data security solutions.

START

SELECT FILE

ENTER AES ENCRYPTION PASSWORD

GENERATE CIPHER USING PASSWORD

READ IN FILE

FIGURE OUT FULL SIZE OF FILE

ENCRYPT FILE DATA

WRITE ENCRYPTED DATA TO NEW FILE

STOP

- *Locator Algorithm*

The algorithm below is the locator algorithm that serves as the locator agent within the cyberspace.

START

INPUT:

ACTIVATE MALICIOUS SYSTEM

VICTIM SYSTEM:

ACCESS SYSTEM CONFIGURATIONS

MALICIOUS:

MALICIOUS AND VICTIM SYSTEMS CONFIGURATION COMMUNICATION LINK

IF ACTIVE

LOCATOR AGENT ACCESS GPS API

SEND LOCATION TO ADMIN

END

- *Algorithm of unified model that can prevent and locate attacks position A*

The algorithm below captures the objective of having a unified solution that is realtime and can be implemented by the programming language that is employed in the ongoing research as stated above.

START

INPUT:

VICTIM SYSTEM FILES

ENCRYPT VICTIM SYSTEM FILES

IF MALICIOUS SYSTEM ACTIVATE

THEN ACTIVATE VICTIM SYSTEM CONFIGURATIONS

ACTIVATE MALICIOUS AND VICTIM CONFIGURATION LINK

IF COMMUNICATION LINK ACTIVE

LOCATOR AGENT ACCESS MALCIOUS SYSTEM

LOCATOR AGENT ACCESS API GPS OF MALICIOUS SYSTEM

LOCATOR AGENT SENDS REPORT TO ADMIN

END

- *Algorithm of unified model that can prevent and locate attacks position A*

Fig. II 2 show the proposed model of the preventive and attack location system, the model shows the communications between each sector of the model with the cyberspace as indicated by the arrows.

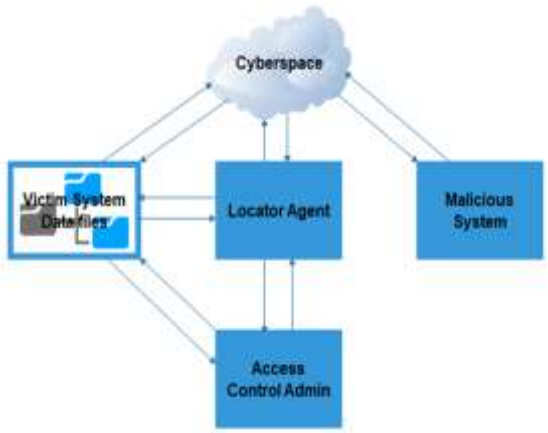

Fig. II Proposed unified model that can prevent and locate attacks position.

- Discusion

The general attacking pattern of cybercriminals as illustrated in fig. I, is by routing through network systems on the cyberspace to get to particular would be victim systems, gain access, maintain access and then get to particular data of interest. There are several tactics employed by cybercriminals and several activities ensues before and during attacks as shown by the mathematical relations.

Gaining of access by unauthorized entity is premised on equations 1 and 2, equation 3 defines the unified algorithm which is active when equation 1 is true and it is not active when equation 2 is true. Equation 3 will readily perform its functions and achieve the mentioned objective when equations 4 and 5 equals discrete value 1 respectively. Equation 6 is non active when equation 2 equals discrete value 0.

The algorithms of *B*, *C* and *D* represent the general AES algorithm, Locator algorithm and algorithm of a unified model that can prevent and locate attacks position respectively. The algorithms of *C* and *D* are the algorithms of interest as they are combined to form the unified model to achieve the objective of the ongoing research as mentioned earlier.

In fig. II, the host system otherwise known as the Victim system, that host the data files of interest, the locator agent and access control admin systems are all communication with the cyberspace. Although the malicious systems used by cybercriminals to access the victim system is not normally in direct communication with the host systems, They also have access to the cyber space from any location across the globe, this makes the victim system accessible to the malicious system. In the proposed solution, the data file on the host system is encrypted against any attack coming from the malicious system, the locator agent monitors the activities of the host system and the location of potential malicious systems since the locator agent is also interacting with the cyber space which is the channel through which the malicious activities can pass through to the host system.

- Conclusion

This paper has been able to achieve the objective which is to design a unified model of detection and locative solutions of the ongoing research work on the problem of malicious attacks. It is hereby recommended that the objective achieved as presented in this paper, is to be considered with

other objectives of the ongoing research work for the desired data security.

REFERENCES

A. O. Isah, J. K. Alhassan, S. S. Olanrewaju, and E. F. Aminu, ‘’Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition,’’ International Journal of Cyber-Security and Digital Forensics, 6(4), 162-179, 2017.

T. Akyuz, and I. Sogukpinar, ‘’Packet marking with distance based probabilities for IP traceback,’’ Networks and Communications, First International Conference on pp. 433-438, December, 2009, IEEE.

V. Chandola, A. Banerjee, and V. Kumar, ‘’Anomaly detection: A survey,’’ ACM computing surveys, 41(3), 15, 2009.

S. Chen, Y. Tang, and W. Du, ‘’Stateful DDoS attacks and targeted filtering,’’ Journal of network and computer applications, 30(3), 823-840, 2007.

W. Dou, Q. Chen, and J. Chen, ‘’A confidence-based filtering method for DDoS attack defense in cloud environment,’’ Future Generation Computer Systems, 29(7), 1838-1850, 2012.

V. M. Igure, and R. D. Williams, ‘’Taxonomies of attacks and vulnerabilities in computer systems,’’ IEEE Communications Surveys & Tutorials, 10(1), 2008.

S. Khan, E. Ahmad, M. Shiraz, A. Gani, A. W. A Wahab, and M. A. Bagiwa, ‘’Forensic challenges in mobile cloud computing,’’ International Conference on Computer, Communications, and Control Technology, pp. 343-347, 2014, IEEE.

S. Khan, M. Shiraz, A. W. Wahab, A. Gani, Q. Han, and Z. B. A. Rahman, ‘’A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing,’’ The Scientific World Journal, 2016.

J. Kok, and B. Kurz, ‘’Analysis of the botnet ecosystem. 10th Conference of Telecommunication, Media and Internet Techno-Economics, pp. 1-10, 2011, VDE.

P. Li, M. Salour, and X. Su, ‘’A survey of internet worm detection and containment. IEEE Communications Surveys & Tutorials, 10(1), 2008.

S. Mizoguchi, K. Takemori, Y. Miyake, Y. Hori, and K. Sakurai, ‘’Traceback framework against botmaster by sharing network communication pattern information,’’ International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, (pp. 639-644), 2011, IEEE.

B. Yu, and R. Wang, ‘’Research of access control list in enterprise network management,’’ Informatics and Management Science VI (pp. 121-129), 2013, Springer.

F. N. Ogwueleka and M. N. Okoye, ‘’Hybrid Incident Response Digital traceback technique in network-based intrusion source detection,’’ IUP, 2016.

R.C. Joshi, E.S. Pilli, ‘’Fundamentals of network forensics, computer communications and networks,’’ DOI 10.1007/978-1-4471-7299-4_7 Springer-Verlag London, 2016.

H. J. Liao, C. H. Richard, Y. C. Lin, K. Y. Tung, ‘’Intrusion detection system: A comprehensive review,’’ Journal of Network and Computer Applications, 36, 16–24, 2013.

PERFORMANCE ANALYSIS-BASED PARAMETER TUNING OF CLONAL SELECTION ALGORITHM FOR ANOMALY DETECTION (C007)

[1]Sule Aishat Aladi, [2]Oyefolahan Ishaq Olabisi., [3]Muhammed Bashir Abdullahi

School of Information & Communication Technology

Federal University of Technology

Minna, Nigeria.

[1]suleaishat990@gmail.com, [2] o.ishaq@futminna.edu.ng, [3]el.bashir02@futminna.edu.ng

Abstract — Intrusion detection has become paramount in the field of network security owing to the fact that network data are being compromised on a daily basis. To this effect, several algorithms have been made available to detect intrusion in the network environment. The Clonal Selection Algorithm (CSA) is one of such algorithms for intrusion detection. Often times, the detection capability of this algorithm are limited by incorrect settings of the parameters involved. Thus, tuning some of the parameters involved in CSA is sacrosanct in determining the performance analysis of the algorithm. Hence, this paper is aimed at tuning the parameters of CSA and analysing its performance for anomaly-based intrusion detection using KDDcup'99 dataset as benchmark for the evaluation. The findings showed that CSA is a good intrusion detection algorithm.

Keywords: *Intrusion Detection; Artificial Immune System; Clonal Selection Algorithm KDDcup'99 Dataset.*

1.0 INTRODUCTION

Artificial Immune System (AIS) algorithms have received much attention from researchers in the past years owing to its increased popularity in solving computational problems. This algorithms is composed of four major algorithms: artificial immune Networks (aiNet); danger theory and Dentritic Cell Algorithm (DCA); Clonal Selection Algorithm (CSA) and Negative Selection Algorithm (NSA) according to Dasgupta, Yu & Nino (2011). Their application areas are in intrusion detection, fault detection, numerical function optimization, image processing, bio-informatics, robotics, web mining etc.

A category of the AIS algorithm which is inspired by the clonal selection theory is the clonal selection algorithm that produces candidate solutions by means of selection, cloning and mutation process. Diverse problems are being solved by this algorithm and it has been reported by Ulutas & Kulturel-Konak (2011) to perform better in cases such as pattern recognition, and function optimization as compared to its counterpart genetic algorithm and neural network.

Literatures regarding CSA have not witnessed its performance evaluation by

tuning the parameters. Hence, this paper is geared towards tuning some parameters of the CSA algorithm to determine their effect on the performance of the algorithm under such performance metrics as true positive rate, false positive rate, precision, recall, F-Measure and ROC Area.

2.0 LITERATURE REVIEW

2.1 Intrusion Detection

With the increase in system complexity, the traditional intrusion detection system such as firewall finds it difficult to provide the system with the needed security. This has given rise to the development of more efficient mechanism for providing the needed protection as a second layer defense. Intrusions are malicious activities that compromise system security; the process of detecting such activities is termed intrusion detection (Farnia, 2017). Intrusion detection systems monitor network traffic for possible malicious activities, raising an alarm when there is any compromise relating to confidentiality, integrity and/or availability of a system resource. There are two classification of intrusion detection approach: misuse detection and anomaly detection

2.1.1 Misuse detection

The misuse detection which is also referred to as the signature-based approach has a predefined rules or patterns (signature) in the database in which identified packets are compared with. Whilst a signature is a pattern or string that corresponds to a known threat or attack; these attack signatures pass specific activity or traffic that is based on known intrusive activity (Liao, Lin, Lin & Tung, 2013). The process usually involves comparing patterns against captured activities for identifying possible attacks. This technique is simple and efficient in the processing of audit data. However, the false positive is minimal in this approach.

2.1.2 Anomaly detection

In network intrusion detection where this work is based, anomaly detection is able to detect attacks that are unknown previously without the need for any programming of the system to signatures of attacks that can possibly occur. Unlike the misuse approach, the anomaly based IDS uses rules or heuristics rather than signature or patterns and is able to detect any compromising activities that deviate from normal system operations. Here, normal profiles are compared with observed events in order to recognize possible intrusions (Liao, Lin, Lin & Tung, 2013).

2.2 Clonal Selection Algorithm

In 1954, immunologist Niels Jerne puts forward her original idea of clonal selection theory which explains how B and T lymphocytes improve their response to antigens. Later in 1958, Joshua Lederberg and Sir Guster reviewed that only one antibody is always produced by the B cell which forms the first evidence for clonal selection theory. The clonal selection theory states that the occurrence of a clonal expansion of the original lymphocytes is triggered by the activation of the original lymphocytes by binding to the antigen and that any clone of the activated lymphocyte with antigen receptors specific to molecules of the body of the organism during the development of the lymphocyte is eliminated. The clonal selection theory forms the basis on which CSA was introduced by Castro & Zuben (2000). The algorithm was later known as CLONALG

(Cai, Gong, Ma & Jiao, 2015) implementing the affinity maturation of immune response and the clonal selection principle.

The clonal selection algorithm is highlighted below (Ulker & Ulker, 2012):

Step 1: Generate a set of antibodies (generally created

in a random manner) which are the current candidate solutions of a problem.

Step 2: Calculate the affinity values of each candidate

solutions.

Step 3: Sort the antibodies starting from the lowest

affinity. Lowest affinity means that a

better matching between antibody and antigen.

Step 4: Clone the better matching antibodies more

with some predefined ratio.

Step 5: Mutate the antibodies with some predefined

ratio. This ratio is obtained in a way that

better matching clones mutated less and weakly matching clones mutated much more in order to reach the optimal solution.

Step 6: Calculate the new affinity values of each

antibody.

Step 7: Repeat Steps 3 through 6 while the minimum

error criterion is not met.

The CSA is useful for recognition of antigen, propagation and discrimination of cell into the memory cell (Fathima, 2017).

2.3 Performance Metrics

The metrics used for the performance analysis of anomaly detection algorithms are: true positive, false positive, false negative, true negative, precision, recall, receiver operating characteristic (ROC) score, and F-measure. It is true positive (TP) when a true and predicted class of the observation is positive. When an instance that is negative is classified as positive, then it is termed a false positive (FP). Similarly, when a negative observation is classified as negative, then it is named a true positive (TN). Finally, if a positive instance is classified as negative, then it is called a false negative (FN).

In the area of anomaly-based intrusion detection, FN shows the attacks that are not detected by the intrusion detection system and FP shows the false alarm rate. Consequently, TP shows the rate of detecting attacks, and TN shows the rate of accepted non-attack observations.

Recall, also known as *sensitivity* or *TP rate*, is the percentage of detected positive instances. When the algorithm detects all positive instances, the recall value will be equal to one (Ting, 2011). This is depicted formally in equation 1.

$$Recall = \frac{TP}{TP + FN} \quad (1)$$

Precision describes the success of an algorithm in detecting real positive observation as depicted in equation 2, (Ting, 2011).

$$precision = \frac{TP}{TP + FP} \quad (2)$$

F-measure is an evaluation model on which the weighted harmonic mean of recall and precision is calculated, as shown in equation 3, F-measure is a compromise between precision and recall. A value close to one indicates that the classifier is proper to use, whereas an F-measure value close to zero, indicates that the classifier has failed in detecting the intrusion, detecting non-attack observations or both.

$$F - Measure = \frac{2}{{}^{1}/_{precision} + {}^{1}/_{recall}} \quad (3)$$

ROC is the most widely used measure to compare the performance of different algorithms. ROC curves are graphical plots which show the trade-off between false positive (FP) and true positive (TN) rates (Diaz, Lopez & Sermiento, 2016). AUC is a portion of a unit square that has a value between 0 and 1. This is depicted in equation 4.

$$AUC = \frac{FPR * TPR}{2} + \frac{(1 - FPR)(1 + TPR)}{2} \quad (4)$$

Where FPR is False Positive Rate and TPR is True Positive Rate respectively. The ROC curve is a 2D plot that shows the TP rate on the Y axis versus the FP rate on the X axis, and they are plotted in a unit square called ROC space.

2.4 Previous Studies

The performance of algorithms are analysed in a number of ways most times comparing the performance of one with another. A study conducted by Ehsan, Hossein & Alireza (2018) using a version of the negative selection algorithm known as Real-valued Negative Selection Algorithm (RNSA) for intrusion detection varied two parameters of the algorithm: the normal radius and the anomaly radius. At each run, different values of the two parameters were used for intrusion detection. After 20 runs, the value 0.2 and 0.2 for normal radius and anomaly radius respectively, provided the optimum performance. The parameters of CSA were varied in the work of Chaudhary & Kumar (2018) and it was found that there was no significant effect in their result except test tolerance which was varied from 0.6 to 1.0; as the tolerance value increases, accuracy and specificity increases while sensitivity decreases. Furthermore, Chan, Prakash, Tibrewal & Tiwari (2013) showed in their work how the accuracy of the clonal selection algorithm for classification (CSCA) is affected by the number of antibodies. In their experiments, they varied

the number of antibodies between 0 and 100 and accuracy was found to decrease as the number of antibodies tends towards 100.

3.0 METHODOLOGY

3.1 Data Acquisition

The dataset utilized in these experiments is the KDDcup'99 dataset downloaded from the UCI repository (http://kdd.ics.uci.edu). The dataset is known to be the most widely used dataset and the only publicly available dataset for anomaly-based intrusion detection since 1999 (Zekrifa, 2012). The 10% of the whole dataset was used due to its large nature. The 10% consist of 494021 connection records with 41 features and a label of either normal or an attack. The 10% was split into two: 70% for training the model and 30% for testing.

3.2 Parameter Tuning

The parameters involved in the algorithm experiment are:

I. Antibody pool size (N): This describes the total number of antibodies maintained in the memory pool and remainder pool.

II. Clonal factor (beta): This parameter is used to scale the number of clones created by the selected best antibodies

III. Selection pool size (n): This describes the total number of best antibodies selected on each iteration, for cloning and mutation.

IV. Number of generations (G): this describes the total number of times that all antigens are exposed to the system.

V. Remainder pool ratio: This is the percentage of the total antibody pool size allocated for the remainder pool.

This paper considers tuning three parameters that have very high effect on the performance of the algorithm which are N, beta, and number of generations. The simulation environment used is Weka platform using the weka.classifiers.immune.clonalg.CLONALG software developed by Castro & Zuben (2002).

3.2.1 Test case 1

Experiments were conducted by varying the three parameters aforementioned one at a time while keeping others constant. The initial values for each parameter are: N = 30, Beta = 0.1, n = 20, number of generations = 10, remainder pool ratio = 0.1 and total replacement = 0. Subsequently, the N value is varied incrementally by 5; Beta by 0.1; and number of generation by 10 on each iteration. Remainder pool ratio and selection pool size were not varied because they have little effect on the performance of the algorithm.

3.2.2 Test case 2

The values that generated the best results in test case 1 were selected and used to carry out another experiments to see the behaviour of the system whether it performed better or worse.

4.0 RESULTS AND DISCUSSION

4.1 Case 1

The result obtained from tuning the antibody pool size is depicted in figure 1 and it shows that as the number of antibody pool size increases, TPR increases and FPR decreases.

Optimum performance of the algorithm is achieved at N = 70.

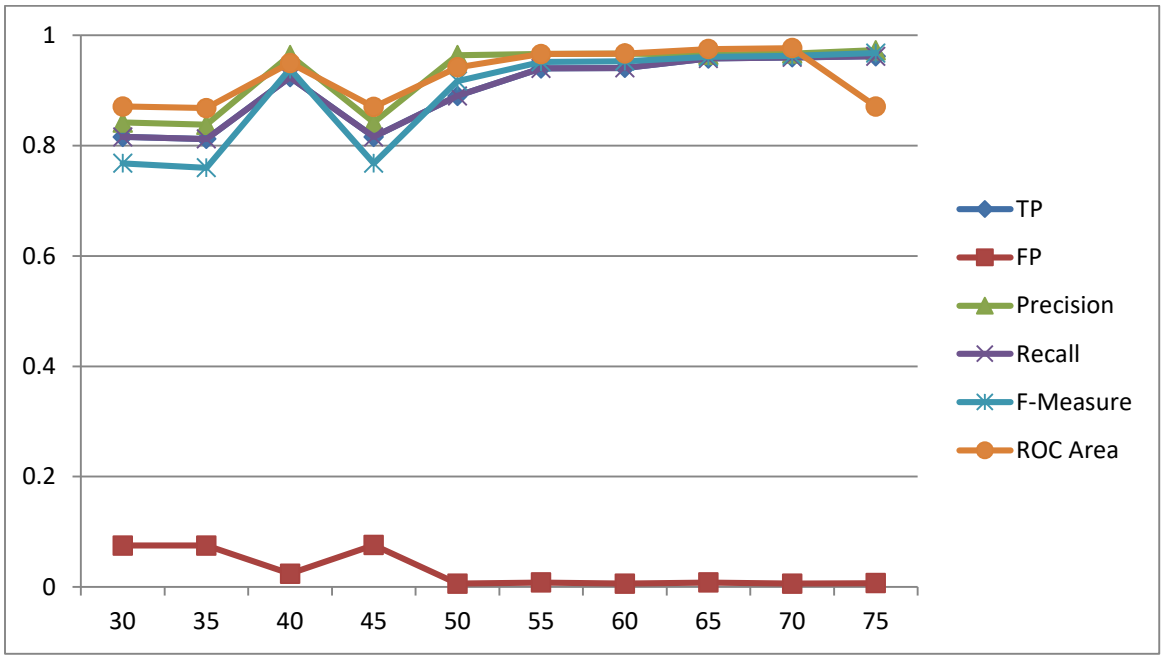

Figure 1: Results obtained from tuning antibody pool size (N).

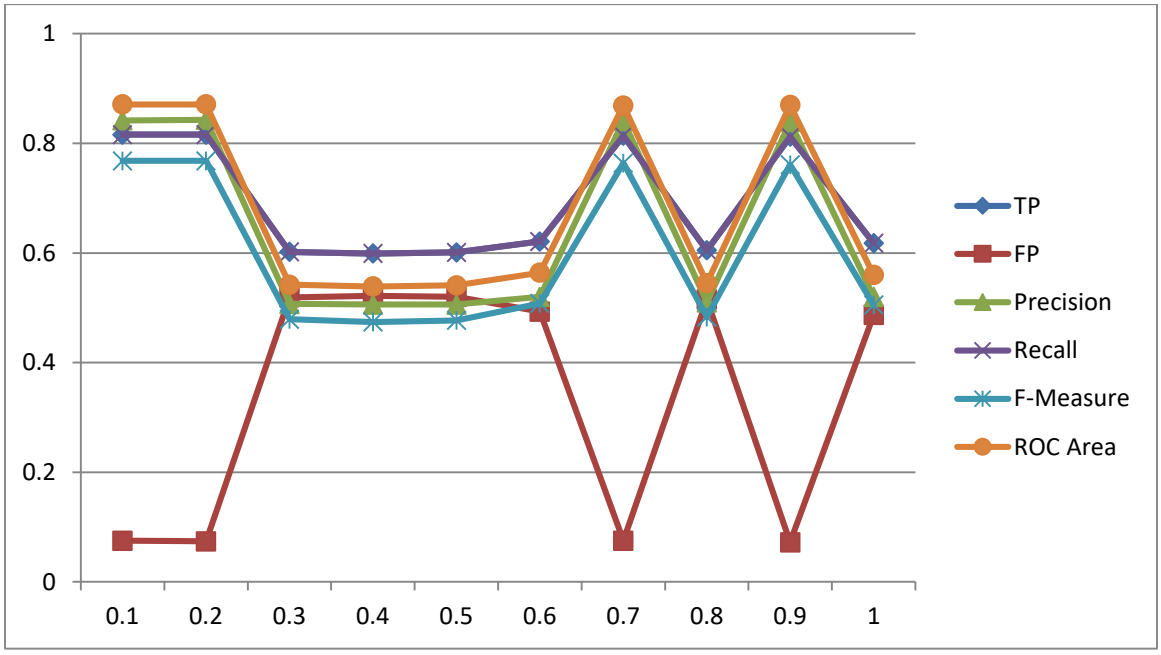

Figure 2: Results obtained from tuning clonal factor (Beta).

The result obtained from tuning the clonal factor parameter is depicted in figure 2. The effect of clonal factor on the algorithm is not stable. At 0.2, it maintained same value of true positive rate while decreasing the false positive rate; along the line, the effect was seen much as it was decreasing true positive rate and increasing false positive rate.

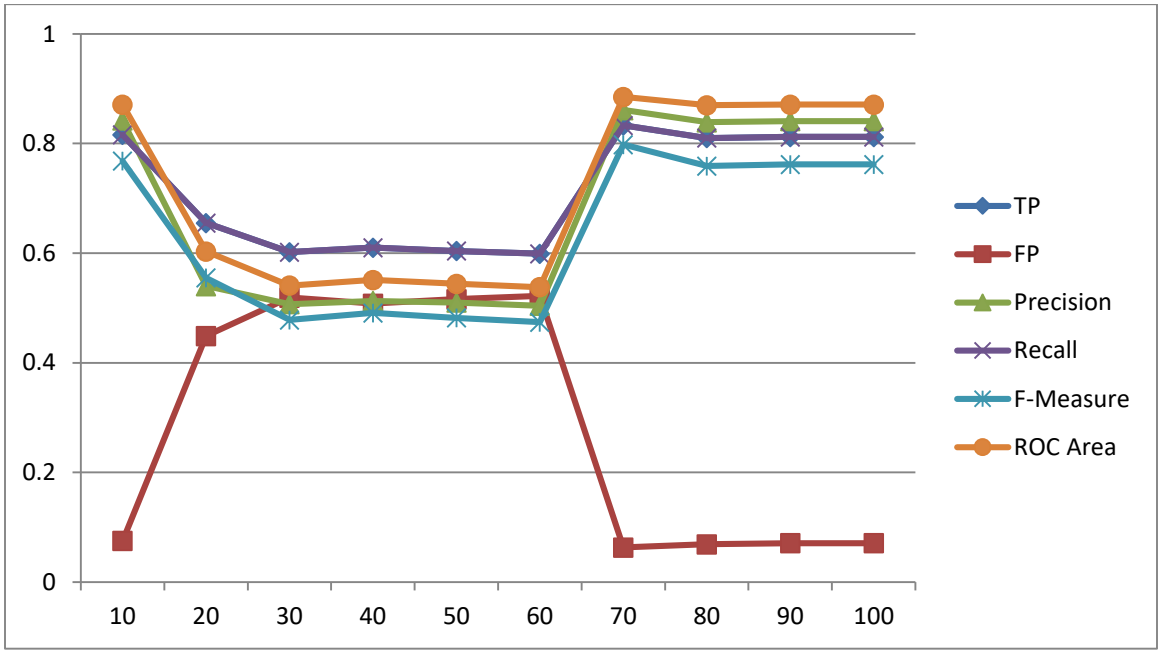

Figure 3: Results obtained from tuning Number of generations (G)

The behaviour of the system is not stable with increase in the number of generation; its effect is seen much in false positive rate as shown in figure 3.

4.2 Case 2

The antibody pool size decreases the performance of the algorithm as it tends towards 100 for a selection pool size of 20. Therefore, the antibody pool size of 70 which achieved the highest true positive rate and lowest false alarm rate was selected for test case 2 experiment. Similarly, the clonal factor of 0.2 generated the highest true positive rate and lowest false positive rate and was selected as the clonal factor value of test case 2. In the same vein, the number of generations of 10 was selected.

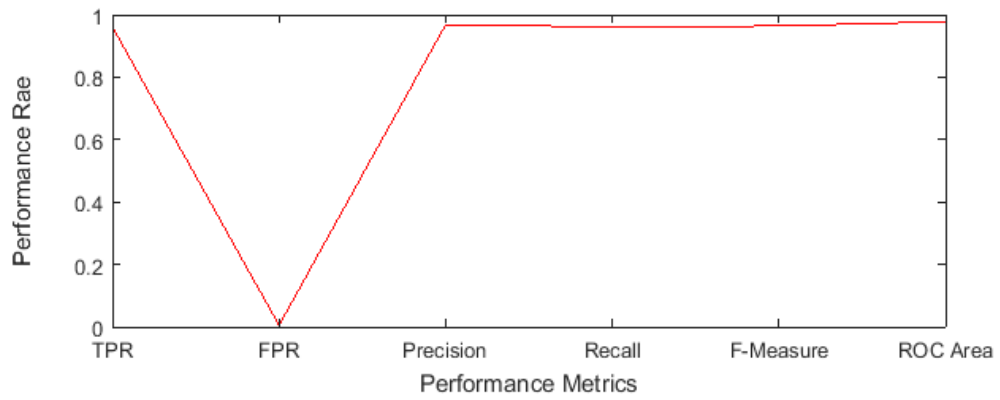

Figure 4: Results obtained from selecting best parameter values from N, Beta and G

Table 1: Results obtained from selecting best parameter values from N, Beta and G

TPR	FPR	Precision	Recall	F-Measure	ROC Area
0.961	0.005	0.968	0.961	0.964	0.978

The system achieved a higher true positive rate and a lower false positive rate as compared to other parameter settings in test case 1 with a true positive rate of 0.961 and a false positive rate of 0.005. The result of the experiment is depicted in figure 4 and summarized in table 1.

5.0 CONCLUSION

The parameters tuned include the antibody pool size, the clonal factor and the number of generations. TPR was seen to increase with increase in N value but later decreased as N tends towards 100 whilst FPR was seen to decrease with increase in N. The effect of Beta on TPR is not stable, it increases at one point and decreases at another point. Same was seen on FPR. The effect of tuning G on FPR and TPR was also not stable. However, a higher TPR and lower FPR were achieved with the following parameter value: N = 70; n = 20; Beta = 0.2; G = 10; remainder pool ratio = 0.1 and total replacement = 0.

The analysis of the performance of CSA has been done in a way that broadens our knowledge on the performance of CSA in intrusion detection and the effect of CSA parameters on each performance metrics investigated. Therefore, it can be concluded that CSA performed considerably well in the detection of intrusion. Future research can look into optimizing the parameters to improve on the detection rate.

REFERENCES

Castro, L. N. D., & Zuben, F. J. V. (2000). The clonal selection algorithm with engineering applications. *In* Genetic and Evolutionary Computation Conference, Las Vegas, Nevada.

Chan, F. T., Prakash, A., Tibrewal, R. K., & Tiwari, M. K. (2013). Clonal selection approach for network intrusion detection. In *Proceedings of the 3rd International Conference on Intelligent Computational Systems, ICICS*.

Cai, Q., Gong, M., Ma, L., & Jiao, L. (2015). A novel clonal selection algorithm for community detection in complex networks. *Computational Intelligence*, *31*(3), 442-464.

Chaudhary, P., & Kumar, K. (2018) Artificial Immune System: Algorithms And Applications Review.

Dasgupta, D., Yu, S., & Nino, F. (2011). Recent advances in artificial immune systems: models and applications. *Applied Soft Computing*, *11*(2), 1574-1587.

Diaz, M., López, S., & Sarmiento, R. (2016). A new comparison of hyperspectral anomaly detection algorithms for real-time applications. In *High-Performance Computing in Geoscience and Remote Sensing VI* (Vol. 10007).

Ehsan, F., Hossein, S., & Alireza, N.,(2018). The Real-Valued Negative Selection Algorithm (RNSA): A Matlab Simulation.

Farnia, F. (2017). *Low-Rate False Alarm Anomaly-Based Intrusion Detection System with One-Class SVM* (Doctoral dissertation, École Polytechnique de Montréal).

Fathima H. (2017) Anomaly Detection in Wireless Sensor Networks using Immune based Bio-inspired Mechanism

Castro, L. N. D., & Zuben, F. J. V (2002) Learning and Optimization Using the Clonal Selection Principle. IEEE Transactions on Evolutionary Computation, Special Issue on

Artificial Immune Systems. 2002; 6(3): 239-251.

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.

Ting K. M. (2011), "Precision and recall," in *Encyclopedia of machine learning*. Springer, 2011, pp. 781–781.

Ulutas, B. H., & Kulturel-Konak, S. (2011). A review of clonal selection algorithm and its applications. *Artificial Intelligence Review*, *36*(2), 117-138.

Ulker, E. D., & Ulker, S. (2012). Comparison study for clonal selection algorithm and genetic algorithm. *arXiv preprint arXiv:1209.2717*.

Zekrifa, D. M. S. (2014). *Hybrid Intrusion Detection System* (Doctoral dissertation, School of Information Technology & Mathematical Sciences).

DIGITAL SECURITY CONSIDERATIONS FOR DEVELOPMENT: WEARABLES PERSONAL EMERGENCY RESPONSE SYSTEMS (WPERS) FOR SAFETY, SECURITY, AND HEALTH (C008)

ATANSUYI, N.[1] and LAWSON, M.O. [2]
1. Dataplus Global Services Limited, 2, Akinola Street, Ogba-Aguda, Lagos.
nathansuyi@gmail.com
2. Milestone Technical Institute Inc., 9800 Centre Parkway Suite 870 Houston, Texas 77036.
Bunmi7@hotmail.com

Abstract:
Rapid urbanization is a global phenomenon, according to the UN; just over half of the world's people live in urban areas with a projection that two-thirds of the global population will be city dwellers by 2050, amounting to an urban influx of 2.5 billion people in the next few decades. As urbanization intensifies and public sector technology initiatives advance quickly, the once-futuristic promise of "smart cities" is coming to fruition, the increased demand for resources such as energy, water, sanitation and services such as education, healthcare delivery and quick response to security concerns is a major requirement in a connected world. Cities have always been "smart" to a degree, using technology to boost the productivity and efficiency of municipal services. But today, the proliferation of digital connectivity and big data explosion are creating new opportunities for beneficial smart-city projects across a range of sectors. Responding to these needs, there are currently hundreds of smart city projects worldwide in both developed and developing countries. Examples abound, such as Lagos, Amsterdam, Barcelona, Beijing and a 100 smart cities initiative recently launched by the Government of India. The speed and stability with which our cities optimize for efficiency, sustainability and safety will broadly impact the quality of life issues around the world.

In Nigeria, security concerns is high and the security apparatus seems overwhelmed, response time to emergency situations is appalling, either security or health related issues is very sluggish hence with Wearables Personal Emergency Response Systems (WPERS), response can be immediate and a bad situation can be salvaged. WPERS is electronic devices that enable individuals at high risk to secure help at a push of a button in an emergency situation; these products will be marketed through Securekare Global Limited.

[Keywords: urbanization, cyber-physical, WPERS, securekare, wearables]

1.0 Introduction

Human and economic activities are the main attraction to the cities thereby creating synergies that allow great development opportunities to the citizenry. However, they also generate a wide range of problems that can be difficult to tackle as they grow in size and complexity. Urban areas need to manage their development, supporting economic competitiveness, while enhancing social cohesion, environmental sustainability and an increased quality of life of city dwellers. With the development of new technological innovations -mainly ICTs- the concept of the "Smart City" emerges as a means to achieve more efficient and sustainable cities. Since its conception, the Smart City notion has evolved from the execution of specific projects to the implementation of global strategies to tackle wider city challenges. Thus, it is necessary to get a comprehensive overview of the available possibilities and relate them to the specific city challenges.

Cities and infrastructures will dominate the majority of human development for the foreseeable future and science, technology and innovation (STI), including information and communication technologies (ICT) can enable them as smarter and cleaner habitats. Accordingly, cities can be planned, designed,

constructed and operated more holistically as crucibles of political power, commerce, education, and innovation with enormous potential for addressing sustainable development needs.
Here are two possible security concerns, where, emergency help is needed.

1. When someone is attacked at gun point either for a dispossession cause, kidnapping or abduction or invasion or even for ritual purposes and so on and so forth, experience has shown that one of the things taken away from the victims is the phone; this incident has led to losing some precious lives and or valuables.
2. When someone is frail, unsteady on their feet or experiencing memory or thinking problems or even the weak aged ones, same thing goes for our children, we are often worried when they are at home alone or on an errand or in their schools or at play. For the weak (aged, women and children) there is need for constant monitoring and contact.

A smart city is a future, better state of an existing city, where the use and exploitation of both tangibles (e.g. transport infrastructures, energy distribution networks, and natural resources) and intangible assets (e.g. human capital, intellectual capital of companies and organizational capital in public administration bodies) are optimized. While the IT systems of critical infrastructure providers face the same level of risk from cyber-attacks as do other enterprises in the private and public sectors, a cyber-attack on critical infrastructure can have much broader and deeper consequences for society and the economy. This put an added pressure on IT decision makers and influences how they design, implement and maintain their cyber securities. Accepting the fact that the threats are both constant and, in terms of the means and methods, constantly evolving, the key to successful mitigation is the development of a proactive strategy of monitoring and detection.
As a matter of fact, in this country our level of vulnerability demands viewable recorded instant security solutions. Our initiatives of WPERS devices, has taking into cognizance of our unsecure environment. These are designed with security and health check in mind with a button to push for immediate assistance. This button connects wirelessly to a configured emergency number somewhere in the home or a designated person that alerts a central dispatch or security officer or health personnel as the situation demands. The personnel at the PERS dispatch centre communicate with the wearer, asking if s/he needs assistance. When the wearer does not respond to the dispatcher's question, the dispatcher calls the person's primary responder. That primary responder is identified at the time the system is set up. It may be a family member, a next door neighbour. If the primary responder is unavailable, the dispatcher calls the backup responder.
This technology contain some newer high tech programs that provide fall detection systems or safety camera systems that monitor and predict usual patterns of daily activity and note unexpected activities.

Not everyone will be willing to participate in close and frequent observation. They may be willing to begin with the least invasive option if it can assure a subscriber's peace of mind and their ultimate wellbeing. There are varying monthly costs and installation fees for any of these programs. Also, worthy of considerations are the varying levels of remote connectivity and technical sophistication for all the possibilities, this initiatives is powered by Securekare Global Limited which is an affiliate of DMI Technologies Nigeria Limited in collaboration with Dataplus Global Services Limited, specialize in the provision of Security, Safety and Health (SSH) devices as a service in a seamlessly connected world.

2.0 Product's Literature Review

Recent developments in sensor and communication technologies have provided novel applications for the betterment of people in daily life especially in smart city development. WPERS technology is one of among such recent technology trends adopted by users in order to get various services in

safety, healthcare, fitness etc. The central idea of this paper is to provide the overall viewpoint of WPERS technology towards our society and explain the recent developments and how securekare innovative products and taken cognizance of the best practices towards developing how it can be socially adopted in various sectors.

In recent years, WPERS technology is one of the hottest topics in the technological field. This area is still in the beginning phase, but it is growing rapidly and capturing the market with great success and marvelous speed. They are small computers, which can be integrated into different objects. Also these devices can do multiple tasks which are similar to what could be provided by mobiles and laptops. But in some cases, these devices can give outstanding performance compared to hand-held devices especially in the healthcare. These devices have tendency to provide sensory and scanning features, such as bio-feedback and tracking of biological functions.

Furthermore, WPERS allow humans to access information in real-time because they have some form of communication capabilities. Also link up with an app which can work with smartphone sensors. This app can track and acts like a personal trainer. It monitors the daily activities of consumers and based on these activities it will suggest the suitable workouts for the consumer and sends inspiring texts. For example, message like if user didn't sleep well last night therefore tracker will suggest that it is essential that user should go to sleep earlier today.

Location based services (LBS) are one of the applications available in WPERS devices which are providing services and information to their users. LBS have different viewpoints and it has application in various domains such as entertainment, health and personal life among other activities. An important feature of the WPERS is that it also provides location based services to their users. Location based services collects the real-time data from their users. Based on that data, it monitors the current location of their users and based on that suggest the user relevant services.

2.1 Healthcare Application - Researchers from National Science Foundation's Center for Advanced Self-Powered Systems of Integrated Sensors and Technologies (ASSIST) at North Carolina State University have created a health and environmental tracker, which is used to prevent and predict the attacks of asthma (Wearable 2016). WPERS devices consists of sensors to track the environmental as well as health characteristics, such as ozone in the air, ambient temperature and humidity, heart rate, motion, percentage of oxygen in the blood and some other aspects. On the other hand, some types of sensors which is able to monitor the movement of the patients, respirational system, skin impedance, oxygen amount in the blood and so on.

Nowadays, patients who suffer from asthma also use the peak flow meter to examine proper functioning of lungs daily. However, the health and environmental tracker (HET) is a modified and self-powered spirometer which gives almost exact information about lung functioning and also it has the ability to store the data in it. Further, HET is a low-power WPERS devices and low-power utilization is essential to increase the battery life. Further, researchers at the University of California have designed such WPERS device which can observe both electric and biochemical signals. The device comprises with a small electronic board and a set of sensors. It can transfer information from electrical and biochemical signals through Bluetooth technology.

2.2 Military Applications - WPERS technologies are those types of technologies or gadgets which can help individuals to carry some of their functions more freely. WPERS are providing some form of protection to the individuals when they are wearing such equipment. WPERS devices and displays have significant role in the war and battlefield. These technologies can help pilots to track their foes from long distance. It detects the wind, weather,

real-time and evaluates the optimal time of the flight.

However, firearms are also using LCD screens to look their target easily instead of traditional scope. Armed forces are using smart biosensors for monitoring and sensing injuries of soldiers. The soldier's performance is completely dependent upon their physical conditions. However, there are some other sensors which can be attached on their clothes to monitor the breathing, heart rate and hydrations. On the other hand, WPERS device can sense head injury in the skullcap. It provides a warning to soldier's, when helmet is starting to weaken. Georgia Tech University has developed the FIDO System (facilitating interactions for dogs with occupations) which allows military dogs to use WPERS devices to communicate with their handlers.

Further, there are various sensors in the wearable device which emits different sound or notifications for the handlers, when dog is tugging, biting and doing other activities. It also alerts their trainer when it detects bombs and other threats.

Moreover, electronics is becoming an important part in the battle field and batteries are considered as essential as bullets. But due to the heavy load, soldiers have to put great effort on it. Therefore, BAE systems, is a global defence, aerospace and security company which has created the Broadsword spine. It is a smart textile device which is integrated into the soldier's clothes. Also, it works as invisible data bank network and also supplying power with help of conductive materials. They are used to monitor vigorous signs and ecological hazards. Further they have wireless communication facility which helps them to give current situation to authorities.

2.3 Fitness Applications - Wearable devices for fitness prevent injuries and improve physical activities of users by tracking and viewing accurate information of oxygen level, breathing rate, heart rate and acceleration. Also, professional and home athletes can share their fitness progress with their coaches and friends with the help of Bluetooth connectivity. They also get motivation when they are receiving positive feedback from their colleges and trainers.

2.4 Some Risks Associated With WPERS

- Lack of password or passcode usage on devices or applications that store company information.
- Devices lost or left unattended.
- Employee's not regularly updating or installing malware and antivirus software.
- Incompatibility of devices with company equipment or security.
- WPERS communicating with other personal devices that are left unsecured.
- Uncertainty of who owns data stored on devices.
- Lack of monitoring and usage of wearable technology.

3.0 Products Innovation for Nigeria Market

In Nigeria, security is one of the major concerns, our security issues ranges from kidnapping, abduction, rituals, inter - tribal and religious "wars" etc., hence there is urgent need for WPERS and of utmost important for both public and private institutions to start embracing this innovative technology towards aiding and supporting the various security apparatus to be effective at their job roles. Most importantly, as Lagos State moves towards achieving its smart city goals and the hope that other states of the federation will adopt this soonest, there is need to adopt smart protection for the citizens. Based on the foregoing, Securekare Global Limited and in collaboration with Dataplus Global Services Limited has introduced WPERS devices for Security, Safety and Health (SSH) where you can trigger, track, view, communicate and monitor the affected individual at the push of a button, designed purposely for Nigeria environments and the above stated risks were duly put into considerations in our model designs and not only that, it has the capability to monitor and guide on basic health status and fitness check capability such as the blood pressure, pause etc.

3.1 Research Methodology

One of the challenging tasks is to localized

technology to ones environment with numerous infrastructure deficits. On the basis of this localisation, most of technology needs must be reviewed without losing the basic features of the intended purposes at the same time benchmarking with the global best practices. End users were categorized because a single product cannot meet the needs of users and optimized with their functionality. In order to meet users' needs, we apply usability testing method, complete survey about the different levels of categorization and compatibility tendencies with both Android and Apple iphone technologies. The testing method and survey are also supported with heuristic loom to design product models that helps to resolve sufficient requirements of users in Nigeria and its environment. However, the appropriateness of this model needs more focus and contemplation.

3.2 Setting Goals

We took time to study on the applicability nature of most WPERS and making the technology
conspicuously present and accessible within seconds with the study of almost all features of Android and Apple iPhone technology that help to build new app interface for the devices and apps that runs on these technologies. The features of these WPERS consist of operating system, integrated technology, running applications, multitasking /multimode support and compatible framework just like mobile phones technology. On the basis of the survey, we conduct the usability testing, we also analyze main features of both leading mobiles and arrange these features into five categories to build better model for app interface with android, IOS technologies and WPERS devices. The various skin types' sensors were considered with different age brackets, environmental conditions such as making it water resistant. These considerations help to understand and erect this new model. Our newly developed model is highly compatible with the needs of end users in Nigeria and Africa.

3.3 Data Gathering

The collection of data follows the standards of fieldwork research, several data sources are applied that covers interviews, observations and literature. We did some research capability in the industry to trigger the data to navigate the interview process. At first stage, we collect the relevant features of Android and Apple iPhone. In second phase, we sort out the best features that our device required for optimal performance. Finally, we get feedback through observation, interviews and coordination with skilful persons of related field in order to obtain helpful suggestions.

3.4 Interviewing process:

Interviews are performed with administrative staff, experts, student-researchers, and industrialist. The time duration for each interview consists of approximately 20 minutes and performed on a one-to-one basis.

3.5 Power of Case and Evaluation of Study

The use of data collections, observations, interviews and documentary sources are purely based on scientific reliability. The validity of each foundation must be highlighted. Each interview is recorded and then transcribed. It is done on the basis of testing methods. We finish the process of testing then make observation. In our case, we give the questionnaire to students for obtaining feedback given in table 1. Each student gives feedback based on the relevant categorized model with the compatibility of the features of android and apple smart phone.

We hereby combine the best features of Apple and Android smart phones and recommend the design of new WPERS devices with sophisticated apps that can operate on 2G, 3G, and 4G internet connectivity, respectively.

Table 1: Showing feedback obtained from 22 students and 22 working adults.

S/N	Name of features Name of Mobiles		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	Is operating system supporting	Android	19	18	6	1	0
	several types of developed	Apple Iphone	8	12	20	4	0
		Android	17	15	12	0	0
2	Is dual core A5 chip available?	Apple Iphone	23	12	9	0	0
	Can we get faster page loading	Android	16	20	8	0	0
3	and improved graphical	Apple Iphone	26	14	4	0	0
	Is this providing faster page	Android	18	20	6	0	0
4	transfer from Iphone to computer?	Apple Iphone	20	14	10	0	0
		Android	36	4	4	0	0
5	Is this multitasking?	Apple Iphone	10	32	2	0	0
	Is framework compatible with all	Android	30	10	3	1	0
6	existing apps of Google and	Apple Iphone	4	20	4	16	0

3.6 Design of WPERS Devices: Integrated technology in device

The integrated device technology concerns about the system architecture. In this design, the developed system integrates heterogeneous network management technologies, which also include the Android mobile system software design. A peculiar feature of the system developed is that it can be useful as Home Gateway Entertainment (HGE), Vehicle On-Board Unit (OBU), and portable network device unit. The system provides convenient wireless internets, which can be effectively accessed by users. A typical application of Android is the HID Global is an American manufacturer of secure identity solutions. The system provides two functions; which are roaming and sharing, and the interface has been equipped with heterogeneous network interface. Roaming has the capability of searching and choosing best resources wireless network - an example is RSS and Bandwidth which are used by users, based on the pertaining conditions. When roaming is desired in the heterogeneous and homogenous network, this becomes most useful. Based on the sharing functionality of the system, the system is capable of allocating resources to all users, with the intention of the system having been interconnected with wireless multiple network. Also, with users and people who are outside home and buildings, roaming functionalities uses intelligent Mobile Internet Device (MID). User traffic demands can be met when the system has chosen more or available network resources.

3.7 Supported running features and application

The WPERS device system development also supports contents modules used for description of the supported feature, which also runs on the Android system application. An application software known as the Java Native Interface (JNI) is a programming software framework, which runs on the Java Virtual Machine (JVM), which normally display two functions: to call and to be called by native application, written in C/C++ assembly language. The Android machine also requires the Java Native Interface (JNI) for an application. When necessary, and it is required Android application developers should resort to use of Android NDK, embedded in code native libraries as the required application development platform; then the application which is running on the virtual machine in the JNI interface can be used to call the native function. An important large part in native code, written in the language C/C++ construction, which is also used to access the devices, platform specific task, which also enhances the application by use of critical code, can be developed by the JNI reuse interface.

3.8 Multi-tasking and multimode Support

We refer here multitasking and multimode support to portable lab system development of the WPERS device system application. This portable Lab system development has a main requirement which needs to be followed in our system development, which supports the architectures

and the technologies used in our system implementation. The established principles and requirements about implementing our new methodology and design for a new system will include but not limited to the following:

i. User account creation
ii. WPERS device system application connection to remote server
iii. Data extraction from server by the data acquisition board, which must include a database to store data collected.
iv. There must be a database server linked to our system application of the mobile device.
v. Information reproduction system of our WPERS device from database data Choice of Online/Offline mode made possible and is operated from the remote database.
vi. Local and remote database are synchronized together.
vii. Information visualized is at the harmonic power and voltage values level which includes graphical videos.
viii. The server side is able to search power and read which uses different criteria like date and time.
ix. It is able to annotate/comment/ and be questioned on data readings, and is made to view specific data comments.
x. It can be deployed in Android or IOS platforms.

3.9 Findings

The findings are based on testing procedure that invites the participants belonging to different background. Some are familiar and belonging to mobile and wireless communication field and fewer possess less expertise in this field but know how to use mobile devices. The performance analysis requirement or beta testing method also involves three steps. First, we introduce the testing procedure from design phase to conducting the test. Second, make all the related operations of architecture and applications and finally, we give the questionnaire to all the participants based on 5-level Likert method. On the basis of feedback, we collect the following statistical data that is applied for developing innovative WPERS mobile technologies with applications to support pedagogical activities.

3.10 Providing Proper Protection

To utilize WPERS technology at work, proper plan for protection is required beforehand. A few tips to provide proper protection:

- Create a WPERS device policy that includes information on how data will be stored and consequences if policies are not followed.
- Ensure employees use unique passwords or passcodes on devices, and stress the importance of secure Wi-Fi connections when accessing information from devices or working remotely.
- Only allow use of WPERS devices that are compatible with existing company technology, and security equipment and software.
- Secure company networks, equipment and critical data with encryption, anti-virus software and password management.
- Set a chain of command for employees to notify the appropriate individuals immediately if devices are lost or stolen.

4.0 Conclusion

The usability testing of a consumer product has more significance for introducing new technology that is better than existing technology. At the completion of usability testing, we are able to determine four categories of users; namely, fitness, kids, adults and hybrid with the following features, Anti-lost personal tracker, two way voice calling, built in speaker, emergency SOS button, take-off alert, listening mode geo fencing, fitness tracking and waterproof. In addition, we are able to produce an ideal model for each category. Results shows that the devices works in real time. By implications lots of deaths or anxiety as a result of delay in acting or lack of information to respond/assist in a dire situation will be averted or drastically reduced to barest minimum.

On the basis of the positive result and product testing, we seek partnership and patronage from public (government) and it's law enforcement agencies such as the police, FRSC etc and private organisations most especially the oil and gas, banks etc and individuals, to protect and avert unnecessary loss of lives as a result of delay response or lack of information so that we can make our environment safe again.

5.0 References

1. Steve Durbin 2015, Building Smart City Security. Available: https://techcrunch.com/2015/09/12/building-smart-city-security/. Accessed 20 July 2018.

2. Victoria Fernandez-Anez (TRANSyT-UPM); Guillermo Velazquez-Romera (TR ANSyT-UPM); Fiamma Perez-Prada; GOVERNANCE AND IMPLEMENTATION OF SMART CITY PROJECTS IN THE MEDITERRANEAN REGION Deliverable 3 https://institute.eib.org/wpcontent/uploads/2017/02/2017_0131-ASCIMER-DELIVERABLE-3-GOVERNANCE-ANDIMPLEMENTATION-OF-SMART-CITY-PROJECTS-IN-THE-MEDITERRANEANREGION.pdf Accessed 22 July 2018

3. Adelabs 2015. Using Fitbit and location based services to benefit you. Available: http://www.adelabs.com/blog/2015/12/14/using-fitbit-and-location-based-services-to-benefityou. Accessed 10 May 2016.

4. Baumann, LM. 2016. The story of wearable technology. Thesis of Master of Arts In Communication. Virginia Polytechnic Institute and State University Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/71790/Baumann_LM_T_2016.pdf?sequence=1. Accessed 16 August 2018.

5. Qualcomm Incorporated 2016. Can wearable devices keep us healthy and fit? Available: http://qz.com/467128/can-wearable-devices-keep-us-healthy-and-fit/. Accessed 16 August 2018.

6. Wearable Devices 2014. Wearable technology and wearable devices everything you need to know. Available: http://www.wearabledevices.com/what-is-a-wearable-device/. Accessed 16 August 2018.

7. Wearable Tech 2016. Researchers develop low-power wearable system to aid asthma patients. Available: http://www.wearabletechnology-news.com/news/2016/jun/14/researchers-developlow-powerwearable-system-aid-asthma-patients/. Accessed 17 September 2016.

8. Wearable Tech 2016. Researchers develop first flexible wearable monitoring biochemical and electric signals. Available: http://www.wearabletechnologynews.com/news/2016/jun/06/researchers-developfirst-flexible-wearable-monitoringbiochemical-and-electric-signals/. Accessed 17 September 2019

9. Wearable Technology - Transforms the way we experience the world. Slide number 11 on website. Available: http://www.slideshare.net/AppStudioz/wearable-technology-thefuture?qid=90159254 - 6191-4e5e-b08a-da5d40197154&v&b&from_search=1. Accessed 16 August 2018.

10. Shawn Kane, HOW TO MAINTAIN SECURITY WITH REMOTE EMPLOYEES. AVAILABLE: https://www.vectorsecurity.com/bizblog/how-to-maintain-security-with-remoteemployees. Accessed 22 August 2018

Normative Evaluation of Cyber-Attacks on a Hypothetical School Computer Network (C009)

Akinjide A. Akinola[1], Ayoade O. Kuye[2], Abiodun Ayodeji[3] and Adeyemi A. Adekoya4
[1]University of Lagos, Lagos, Nigeria, [2]University of Port Harcourt, Port Harcourt, Nigeria. [3]Nuclear Power Plant Development Directorate. Nigeria Atomic Energy Commission, Abuja, Nigeria.
[4]Virginia State University, Petersburg, VA 23806
akinjide.akinola@faculty.umuc.edu, aaakinola@unilag.edu.ng, ayo.kuye@uniport.edu.ng

ABSTRACT

This paper presents the attack tree modeling technique of quantifying cyber-attacks on a hypothetical school network system. Attack trees are constructed by decomposing the path in the network system where attacks are plausible. In this network, two possible attack paths are constructed for the network system. One path represents an attack through the Internet, and the other represents an attack through the Wireless Access Points (WAPs) in the school network. The probabilities of success of the events, that is, (a) the attack payoff, and (b) the commitment of the attacker to infiltrate the network are estimated for the leaf nodes. These are used to calculate the Returns on Attacks (ROAs) at the Root Nodes. For Phase I - the "As Is" network, the ROA values for both attack paths, are greater than 7 (8.00 and 9.35 respectively), which are high values and unacceptable operationally. In phase II, countermeasures are implemented, and the two attack trees reevaluated. The probabilities of success of the events, the attack payoff and the commitment of the attacker are then re-estimated. Also, the Returns on Attacks (ROAs) for the Root nodes are re-evaluated after implementing the countermeasures. For one attack tree, the ROA value of the Root Node was reduced to 4.83 from 8.0, while, for the other attack tree, the ROA value of the Root Node was reduced to 3.30 from 9.35. ROA values of 4.83 and 3.30 are acceptable as they fall within the medium value range. The efficacy of this method whereby, attack trees are deployed to mitigate computer network risks, as well as using it to quantitatively assess the vulnerability of computer networks is established.

Keywords: Cyber-Attack, Quantitative Vulnerability Assessment; Attack Trees, Return on Attack, Countermeasures

1 INTRODUCTION

The historic openness of higher education institutions to the public has made their computer networks more vulnerable to cyber-attacks. Such vulnerabilities have been widely discussed in literature. Assessment of negative impacts of threats/vulnerabilities in schools and academic environments has been presented in contemporary literature, however, much of the reported work have been qualitative. While qualitative research can be useful, their conclusions are often subjective and lack details that provide necessary impetus for clear and definitive actions, as the research outcomes do not readily lend themselves to risk controls and implementation. Clearly, there is a need to quantify the impacts of cyber-attacks on modern-day establishments, since the rate of cyber-attacks continue to escalate and more. Quantitative methods of modeling and analyzing cyber threats have been of great interest to a group of researchers such as Greitzer *et. al,* [1] Xynos *et. al,* [2]

WINS [3, 4] and Roger [5, 6] who have all presented innovative approaches for analyzing cyber threats.

Furthermore, some quantitative studies carried out by Dacier *et al.* [7], Balzarotti *et al,* [8], Edge *et al.* [9], Lemay *et* al. [10], Akinola *et al.* [11], Baker *et al* [15], and Peltier, [16] used attack trees and their variants to examine cyber-attack prone networks. Attack trees are used as illustrations of networks whereby, an asset, or target, may be compromised.

Attack trees present interdependencies between attack paths by breaking down the complexity of the network system and decomposing high-level parent goals into the smaller subtasks. Amenaza [12] indicates that the basic premise of an attack tree model is to provide insight into the vulnerability of a system, and ultimately, isolate what is needed to achieve desired remedial outcome/success.

Dacier *et al.* [7], approach is based on modeling a network system as a privilege graph exhibiting operational security vulnerabilities, as well as transforming the privilege graph into a Markov chain, corresponding to all possible successful attack scenarios. A set of tools has been developed to support this approach and to provide automatic security evaluations of the UNIX-based systems in operation.

Balzarotti *et al.* [8], discusses how relevant information on, the attributes of the architecture, and the vulnerabilities inherent in a distributed system can be applied quantitatively, to assess the risk to which the system is exposed. The advantage of this approach to risk evaluation is its capability to assess the extent to which one should believe in system integrity and trustworthiness, and to facilitate a comparative analysis of different evaluative outcomes.

Another line of research is studying security measures for mobile ad-hoc networks using attack and protection trees. The work of Edge *et al.* [9] indicated that Defense-trees could be used to mitigate or even eliminate vulnerabilities. There are a few limiting factors here, to the extent that some of the defense trees have overpopulated and redundant nodes. Also, the commitment of the attacker, that is, the willpower that the threat agent exhibits, and the time committed to the pursuit of the goal intended were not taken into account in these models.

Lemay *et al.* [10] calculated the State-based Security metrics of two variants of a Supervisory Control and Data Acquisition (SCADA) system architecture using the ADversary VIew Security Evaluation (ADVISE) technique. The study demonstrates how the quantitative metrics produced by ADVISE can aid system design and provide much insight on system security. Akinola *et al.* [11], quantitatively evaluated the effect of cyber-attacks on a school network system. Their work involved evaluating information security as proposed by Cremonini and Martini [13] who used the Return-on-Attack (ROA) and the Return-On-Investment (ROI) methodologies and metrics, to assess and measure how an attacker's preference changes with the selected security measure. Furthermore, Akinola *et al.* [11] established that by executing specific countermeasures, the risk of cyber-attacks on a school network could be greatly reduced. The current work builds on previously established foundations; it applies a similar method to a different environment that is, a dissimilar school

network system. It is relevant to point out that, while Akinola *et al.* [11] previous work used single values for the leaf nodes; this study extends the former by using randomly generated values to denote the leaf nodes.

2 METHODOLOGY

2.1 Network description

The network which is the test-bed for the study is a school computer network, consisting of the following elements - an Internet router (Cisco 890), a Fast Ethernet switch 1 (core switch, Cisco SFS3500)) and an Ethernet switch 2 (Cisco SFE2000), Wirelesss Access Points (Linksys WAP300N), a Web server, a database server, and a Mikrotik firewall. The Internet router is connected to the web server (Apache HTTP) in the computer laboratory on the school premises. The workstations (running on Windows 2007), are of the ring-based topology. A database server (MYSQL) houses the records of graduates and matriculated students of the school. The attacker profiled for this network is a disgruntled ex-student, whose motivation is the will to compromise the database server that hosts the students' valuable records, with the aim of modifying some of the data items including his own particular records.

2.2 The Attack Tree Model

For the attacker to commit his infamous act, and to compromise the database remotely, the attacker uses one of the wireless access points in the school vicinity. The attack trees shown in Figures 2 and 3 depict the architecture of the school's network. The Attack is initiated with the attack goal of compromising the database server - the root node. The tasks needed to achieve success on the attack are spelled out in the trailing figures below. Each task is conceptually launched at a node in the attack tree. These are wireless access points 1 and 2 in Figure 1. Figure 2 is a schematic diagram of the various tasks that are involved and it represents an attack via wireless access points, while Figure 3 represents an attack through the Internet. In Figures 2 and 3, the nodes that are conjoined by an arc must be performed simultaneously for an attack to be successful, while those that are not, requires either of the nodes for success. Mathematically, this can be represented using the Boolean notations, i.e. "AND" or "OR" respectively. Akinola *et al.* [11] have represented the Return-on-Attack (ROA) used in this work is as follows:

$$ROA = P_oCP_s \quad (1)$$

Where:

P_o = payoff; C = commitment; P_s = probability of success.

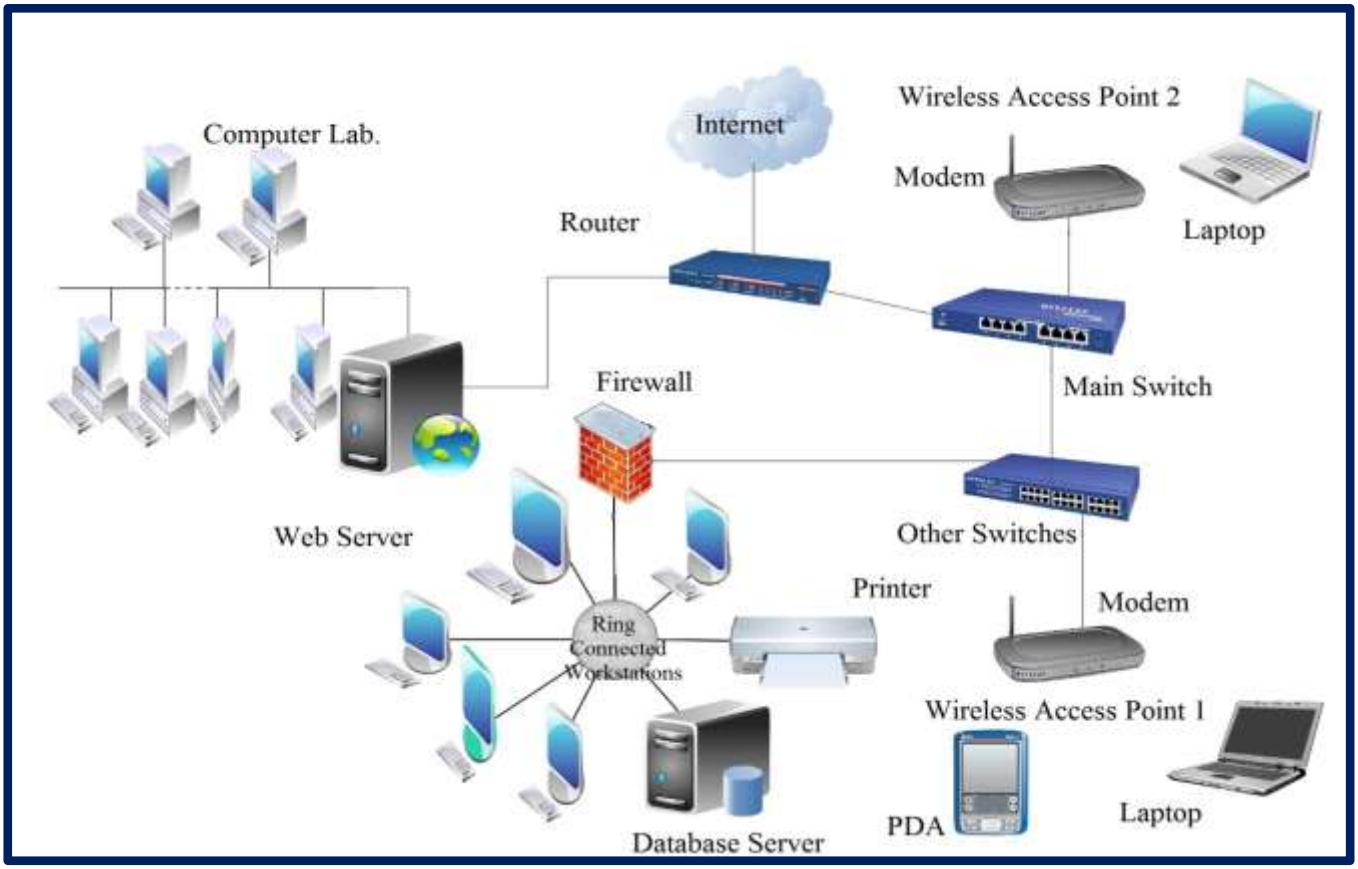

Figure 1: The School Network Topology.

The Commitment, C, is assumed to have a unit value because credible attackers have the capability and the intention to exploit a node contemporaneously. Based on [9], ROA values range from 1 to 10 with Low, Medium, High or Very High scale. Low ROA values range from 1 - 3. In such a network the attack's impact is minor, and it could easily be detected and repaired. Medium ROA values are between 4 and 6, the attack's impact on the network is usually, "Moderate"; there is typically a reduced performance or interruptions in resource availability. Furthermore, in Attack trees with moderate ROA values, the integrity, confidentiality and availability of the network require special effort to detect and repair. High ROA values are between 7 and 9. In this case, the attack's impact on the network is "Severe"; leading to a significant damage to the network system, and there are considerable informational access and disclosure to some system files. Considerable effort is required to detect and repair the damage on such networks. When the ROA value is 10, the network system is completely compromised, inoperable or destroyed. The attacker can render the asset completely unavailable.

The probability of success is calculated using the equation:

$$P_s = A_{cv} * C_A * A_u \quad (2)$$

Where

A_{cv} = Access Vector, C_A = Access Complexity, and A_u=Authentication.

The access vector (A_{cv}) shows how a vulnerability may be exploited. The access complexity (C_A) metric describes how easy or difficult it is to exploit the exposed vulnerability. The authentication (A_u) metric describes the number of times that an attacker can authenticate to a target node to exploit it. It does not include (for example) authentication to a network to gain access. For locally exploitable vulnerabilities, this value should only be set to a single or multiple values if further authentication is required after initial access. Numerical values for the access vector, access complexity, and authentication are derived from common vulnerability scoring system guide [14]. The intermediate and root nodes P_o and P_s are calculated using equation 3, 4, 5 and 6 [9]:

For "AND" nodes:

$$P_s = \prod_{i=1}^{k} \text{prob}_i \quad (3)$$

$$P_o = \frac{10^k - \prod_{i=1}^{k}(10-\text{payoff})}{10^{k-1}} \quad (4)$$

For "OR" nodes:

$$P_s = 1 - \prod_{i=1}^{k}(1-\text{prob}_i) \quad (5)$$

$$P_o = \text{Max}_{i=1}^{k}\,\text{payoff}_i \quad (6)$$

Where $Prob \in (0,1)$; $Payoff \in [1,10]$;
k=number of leaf nodes

3 RESULTS AND DISCUSSIONS

Figures 2 and 3 present the two Attack Trees A and B examined in this study. The Payoff, Access Vector, Access Complexity and Authentication values for the two Attack trees which tally with expert opinions, are presented in Tables 1 and 2. These Payoff, Access Vector, Access Complexity and Authentication values are used to calculate the ROA values for the leaf and intermediate nodes. These values are subsequently used to calculate the ROA values required to compromise the database for Attack Trees A and B (Figures 1 and 2). The ROA values obtained at the root nodes (RN) are 8.00 and 9.35 for Attack Trees A and B respectively. These ROA values fall in the High range and this implies that both root nodes can be exploited easily.

With Attack Tree A, (Figure 2), the attacker severely impacted the network system thereby, causing considerable informational disclosure and access to many system files, while with Attack tree B, the attacker can render the resource completely unavailable.

The expert opinion values presented in Tables 1 and 2 may not reflect the true or "real life" situation. Therefore, the values of the access vectors, access complexities and authentication values were varied randomly within a 5%, 10%, 20%, 30%, 40% and 50% range of the expert opinion values presented in Tables 2 and 3. The calculations for ROA were performed 10,000 times to simulate more probable situations. The results obtained are shown in Figures 4 and 5 for Attack Trees A and B respectively.

Figure 4 shows that for Attack Tree A, the maximum and minimum ROA values are 7.98 and 8.00 when the access vectors, access complexities and authentication values are varied randomly within $\pm$50% of expert opinion. The implication is that for these Attack trees the ROA value is always high even when errors are made in estimating key parameters.

Also, the maximum and minimum ROA values vary from 9.40 to 5.86 for the Attack Tree B (Figure 5)

when the Access Vectors, Access Complexities and Authentication values are varied randomly within ±50% of expert opinion values. The average ROA for the Attack path is 9.12. This implies that for half of the time, the ROA value is greater than 9.00, which is a High ROA value and is unacceptable. Clearly, the ROA values in both the Attack Trees A and B are high. The implication is that an upgrade of the two trees is needed to reduce their vulnerability. The suggested upgrades are presented in Figures 6 and 7.

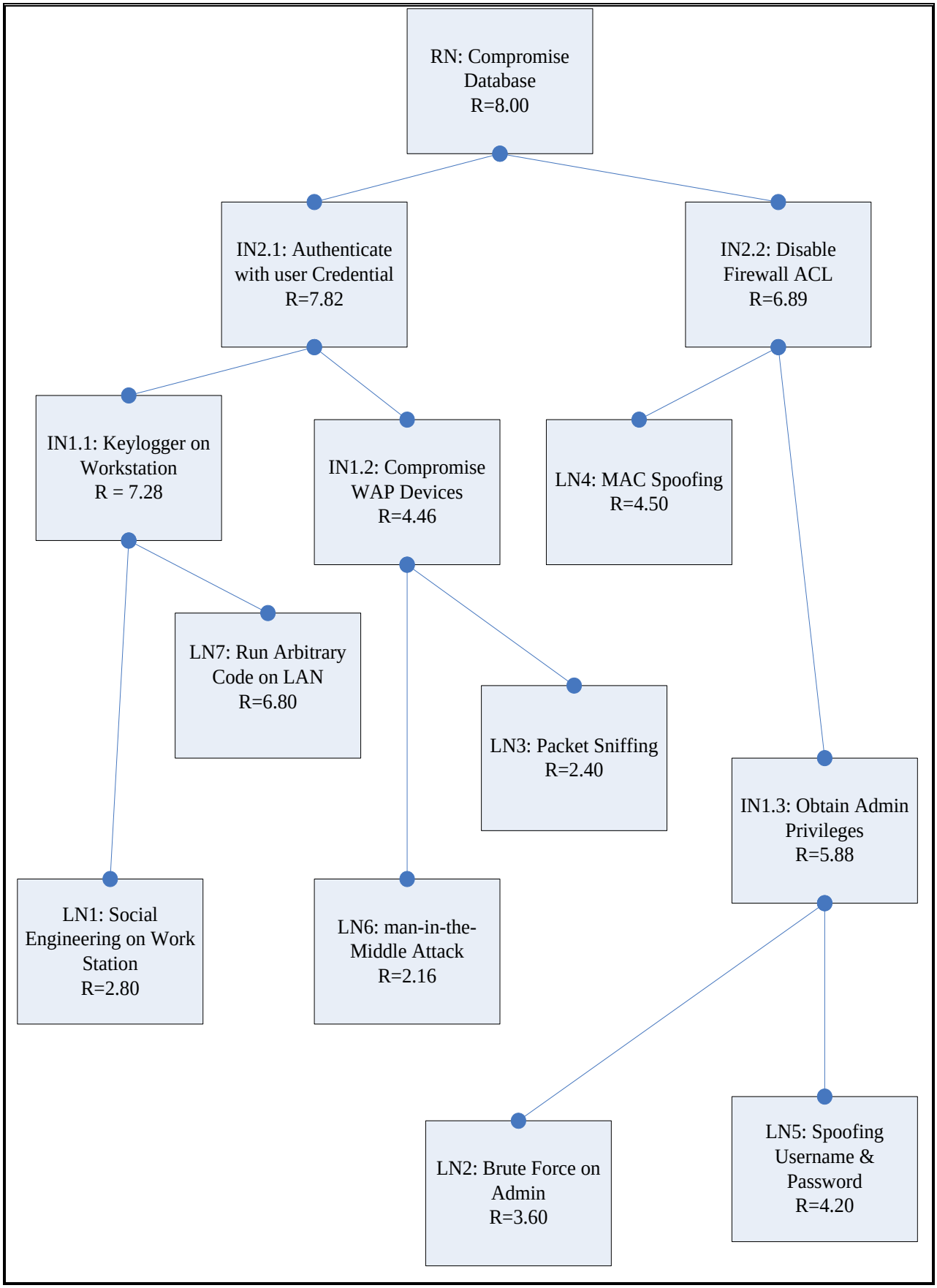
RN: Compromise Database R=8.00
IN2.1: Authenticate with user Credential R=7.82
IN2.2: Disable Firewall ACL R=6.89
IN1.1: Keylogger on Workstation R = 7.28
IN1.2: Compromise WAP Devices R=4.46
LN4: MAC Spoofing R=4.50
LN7: Run Arbitrary Code on LAN R=6.80
LN3: Packet Sniffing R=2.40
IN1.3: Obtain Admin Privileges R=5.88
LN1: Social Engineering on Work Station R=2.80
LN6: man-in-the-Middle Attack R=2.16
LN2: Brute Force on Admin R=3.60
LN5: Spoofing Username & Password R=4.20

Figure 2 Attack Tree Diagram A for the School Computer Network

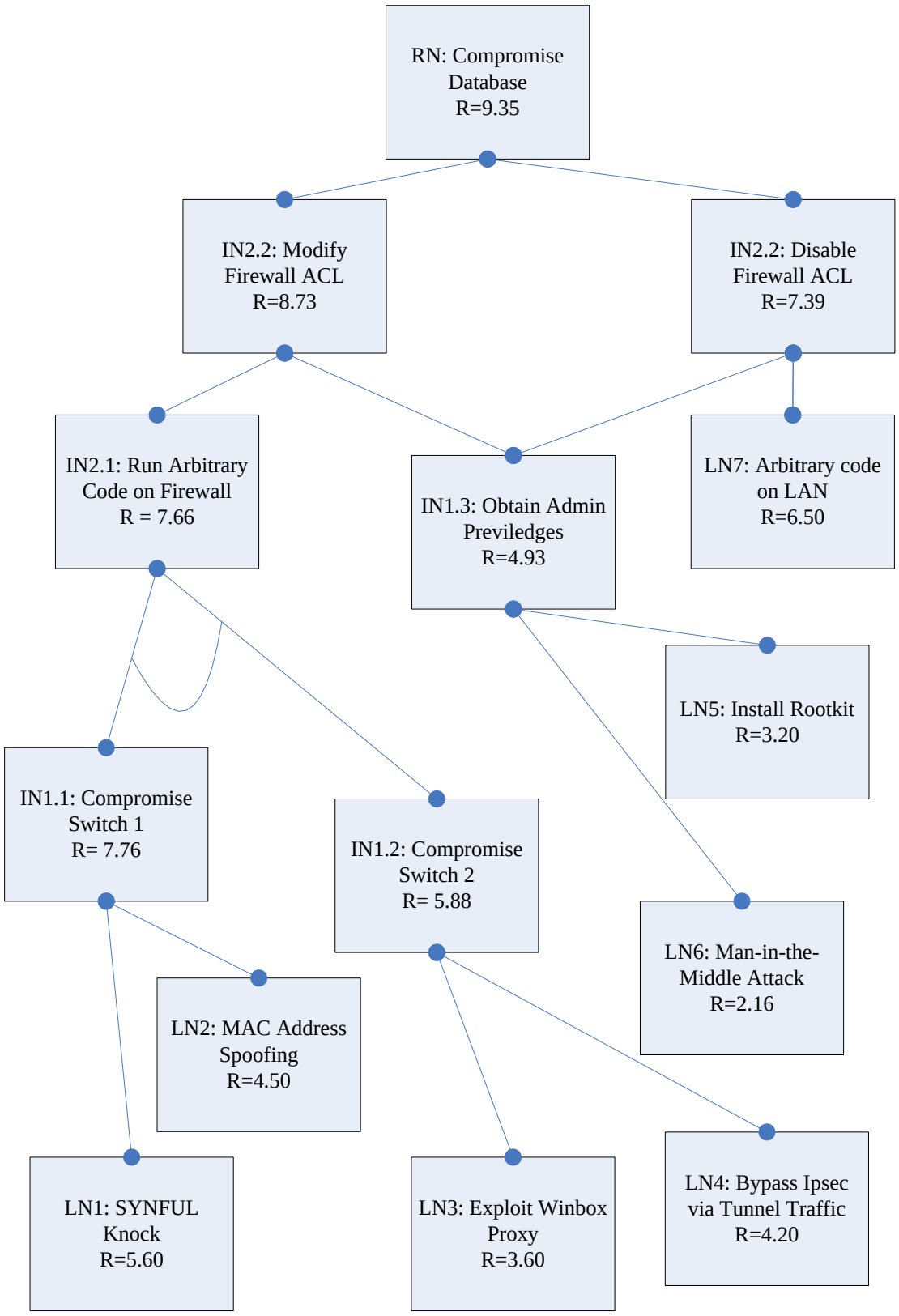

Figure 3 Attack Tree diagram B for the School Computer Network

Table 1. Parameters used in calculating ROA for Attack Tree A

Node	Task name	Payoff	A_V Access Vector	C_A Access Complexity	A_U Authentication
LN1	Social Engineering on Work Station	7	1	0.40	1
LN2	Brute Force on Admin	6	1	0.60	1
LN3	Packet Sniffing	4	1	0.60	1
LN4	MAC Address Spoofing	5	1	0.90	1
LN5	Spoofing Username & Password	7	1	0.60	1
LN6	Man-in-the-middle Attack	6	1	0.36	1
LN7	Run Arbitrary Code on LAN	8	1	0.85	1

Table 2. Parameters used in calculating ROA for Attack Tree B

Node	Task name	Payoff	A_V Access Vector	C_A Access Complexity	A_U Authentication
LN1	Synful Knock	8	1	0.70	1
LN2	MAC Address Spoofing	5	1	0.90	1
LN3	Exploit Winbox Proxy	6	1	0.60	1
LN4	Bypass Ipsec via Tunnel Traffic	7	1	0.60	1
LN5	Install Rootkit	8	1	0.40	1
LN6	Man-in-the-middle Attack	6	1	0.36	1
LN7	Run Arbitrary Code on LAN	8	1	0.80	1

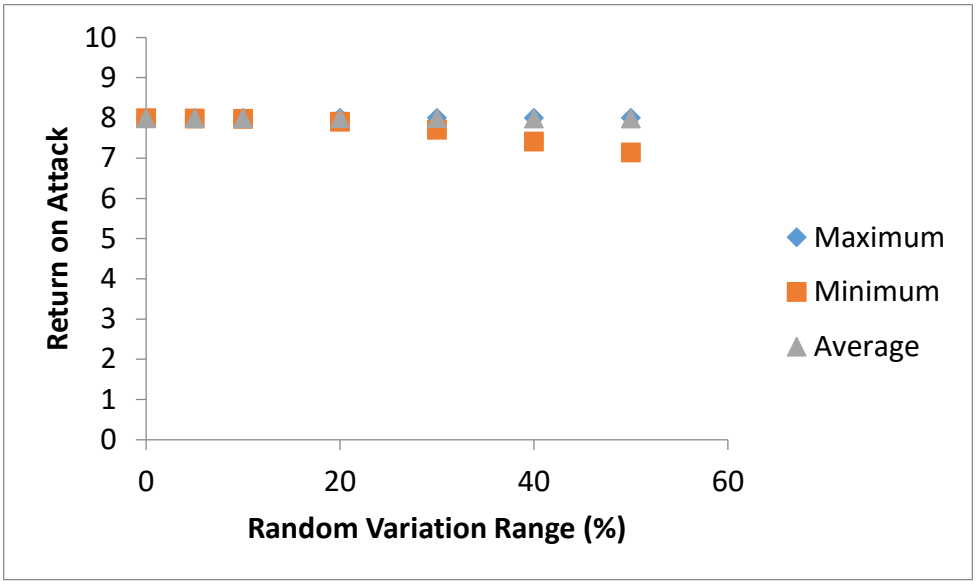

Figure 4: ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree A

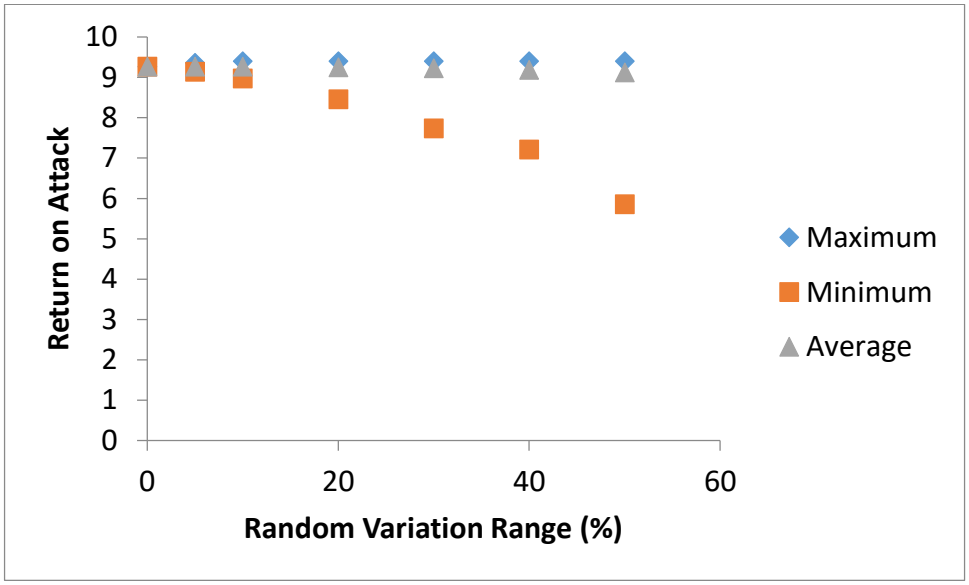

Figure 5: ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree B

All things considered, the recommended security upgrades to be implemented on leaf nodes on the Attack Trees are:

1. Adding Intrusion Detection and Prevention Systems (IDPS) at 'sensors' on the network diagram.
2. Adding Remote Access Servers (RAS) before the business processing unit of the digital Network, as all inbound and outbound traffic is routed through this unit.

Again, using expert judgment, new Access Vectors, Access Complexities and Authentication values are obtained for the Attack Trees A and B. These values are shown in Tables 3 and 4 for the Attack Trees A and B respectively. The ROA values for the nodes are recalculated, and the results are presented in Figures 6 and 7 for the upgraded Attack Trees A and B respectively. The nodes where upgrades were implemented are marked with a star in the diagrams. The ROA values at the root nodes are 4.87 and 3.30 for Attack Tree A and Attack Tree B respectively. These values are clearly lower than the reported values prior to the upgrades, and the values fall in the medium score range for ROA values. Thus, the suggested upgrades were effective, hence, they did reduce the vulnerability to compromise the Database.

To further obtain better estimates of the ROA values at the Root nodes for each Attack Tree, repeated calculations were performed by randomly varying Access Vector, Access Complexity and Authentication values up to the +50% range. The calculations were performed 10,000 times with randomly generated values of Access Vectors, Access Complexities and Authentication. A summary of the results is shown graphically in Figures 8 and 9 for Attacks Trees A and B respectively. Again, the results indicate that the error in ROA value increases proportionally with errors in Access Vector, Access Complexity and Authentication values; however, the ROA values average out to the values obtained in Figure 6 and 7 for the Attack Tree A and B respectively.

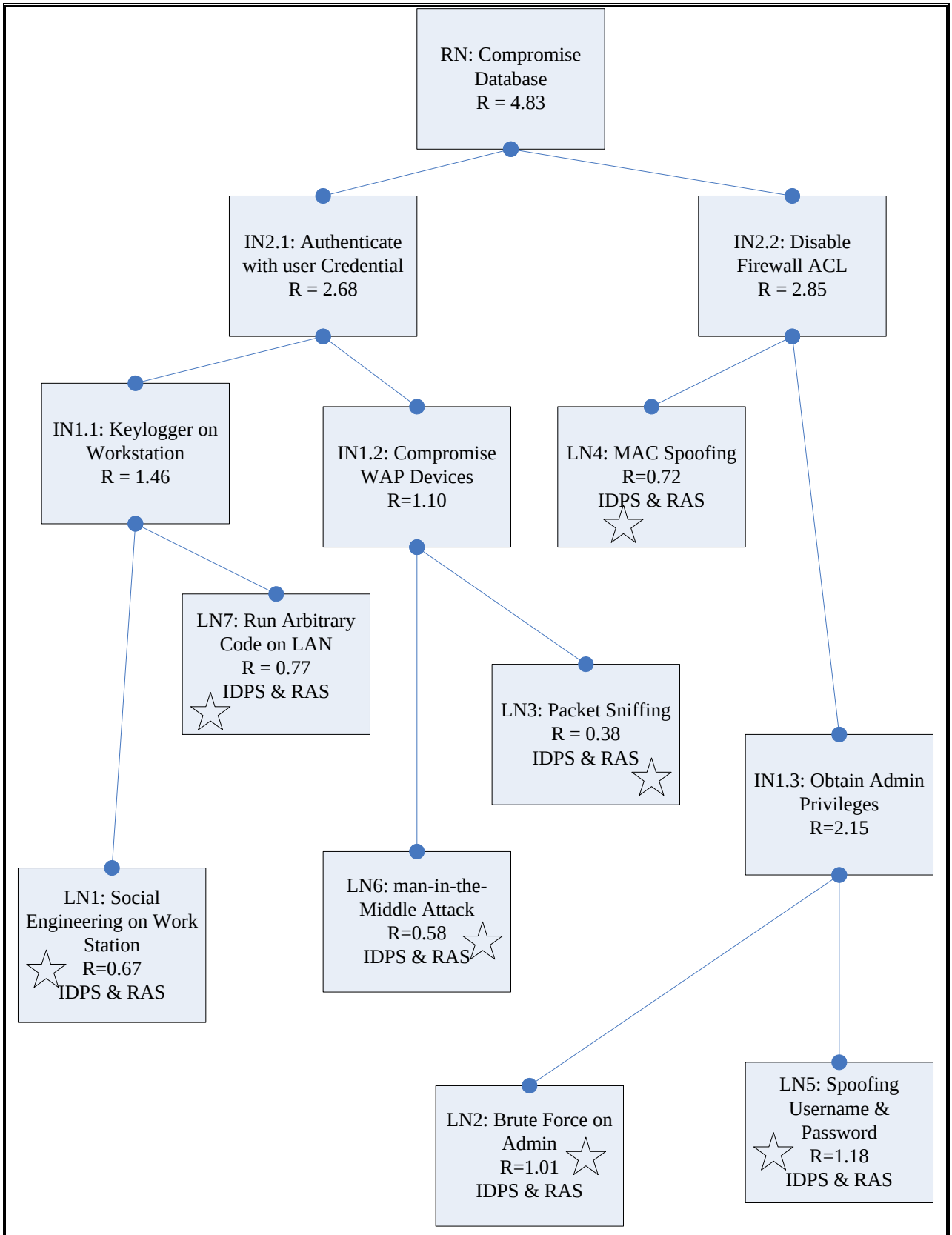

Figure 6: Attack Tree Diagrams A for School Computer Network after Upgrade

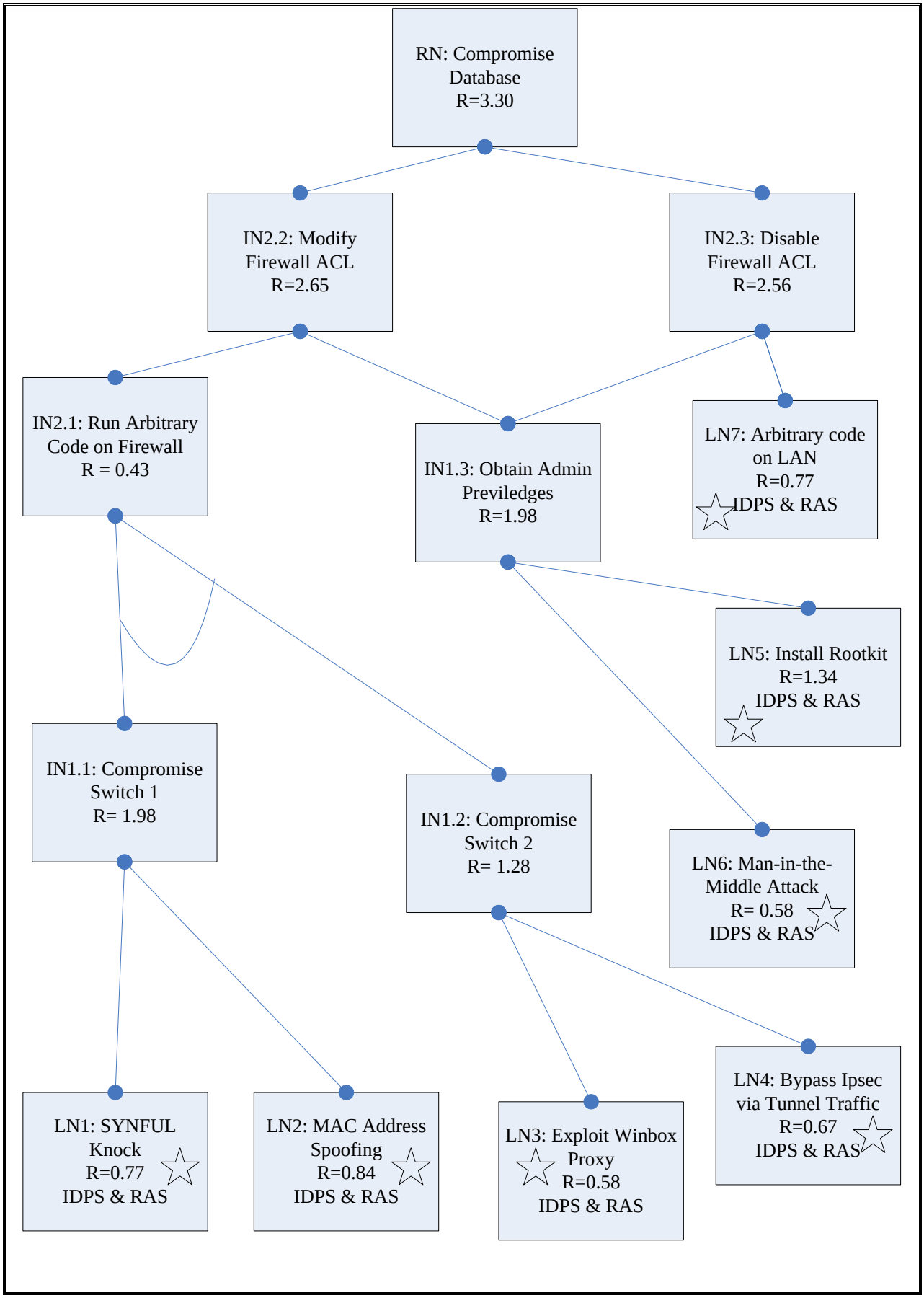
RN: Compromise Database R=3.30
IN2.2: Modify Firewall ACL R=2.65
IN2.3: Disable Firewall ACL R=2.56
IN2.1: Run Arbitrary Code on Firewall R = 0.43
IN1.3: Obtain Admin Previledges R=1.98
LN7: Arbitrary code on LAN R=0.77 IDPS & RAS
LN5: Install Rootkit R=1.34 IDPS & RAS
IN1.1: Compromise Switch 1 R= 1.98
IN1.2: Compromise Switch 2 R= 1.28
LN6: Man-in-the-Middle Attack R= 0.58 IDPS & RAS
LN1: SYNFUL Knock R=0.77 IDPS & RAS
LN2: MAC Address Spoofing R=0.84 IDPS & RAS
LN3: Exploit Winbox Proxy R=0.58 IDPS & RAS
LN4: Bypass Ipsec via Tunnel Traffic R=0.67 IDPS & RAS

Figure 7 Attack Tree Diagrams B on School Computer Network after upgrade

Table 3. Parameters used in calculating ROA for Attack Tree A after upgrade

Node	Task name	Payoff	A_V Access Vector	C_A Access Complexity	A_U Authentication
LN1	Social Engineering	7	0.6	0.4	0.4
LN2	Brute Force	6	0.6	0.4	0.7
LN3	Parket Sniffing	4	0.4	0.6	0.4
LN4	MAC Address Spoofing	5	0.6	0.6	0.4
LN5	Spoof Username & Password	7	0.6	0.4	0.7
LN6	Man- In- The- Middle Attack	6	0.6	0.3	0.53
LN7	Run Arbitrary Code on LAN	8	0.85	0.28	0.4

Table 4. Parameters used in calculating ROA for Attack Tree B after upgrade

Node	Task name	Payoff	AV Access Vector	CA Access Complexity	AU Authentication
LN1	Synful Knock	8	0.6	0.4	0.4
LN2	MAC Address Spoofing	5	0.6	0.4	0.7
LN3	Exploit Winbox Proxy	6	0.4	0.6	0.4
LN4	Bypass Ipsec via Tunnel Traffic	7	0.4	0.6	0.4
LN5	Install Rootkit	8	0.6	0.4	0.7
LN6	Man-in-the-middle Attack	6	0.6	0.4	0.4
LN7	Run Arbitrary Code on LAN	8	0.6	0.4	0.4

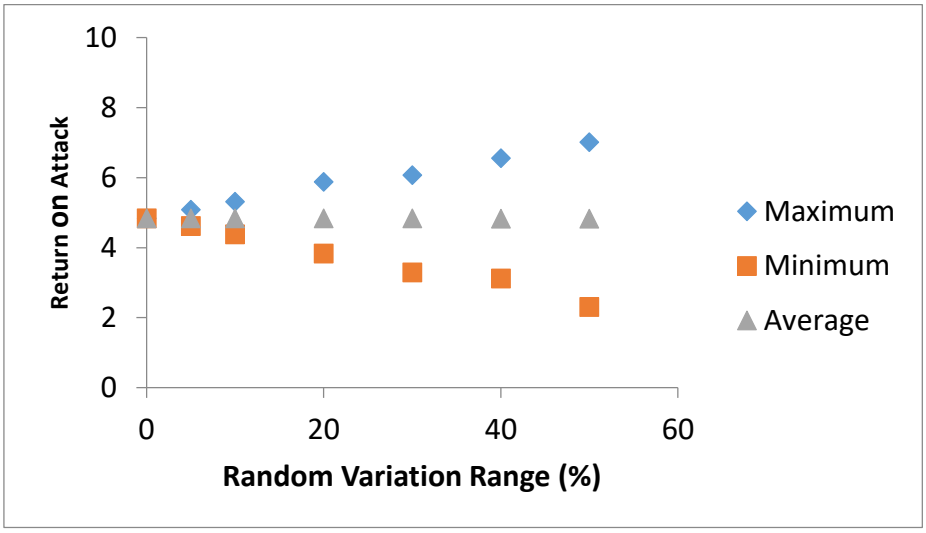

Figure 8: ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree A After Upgrade

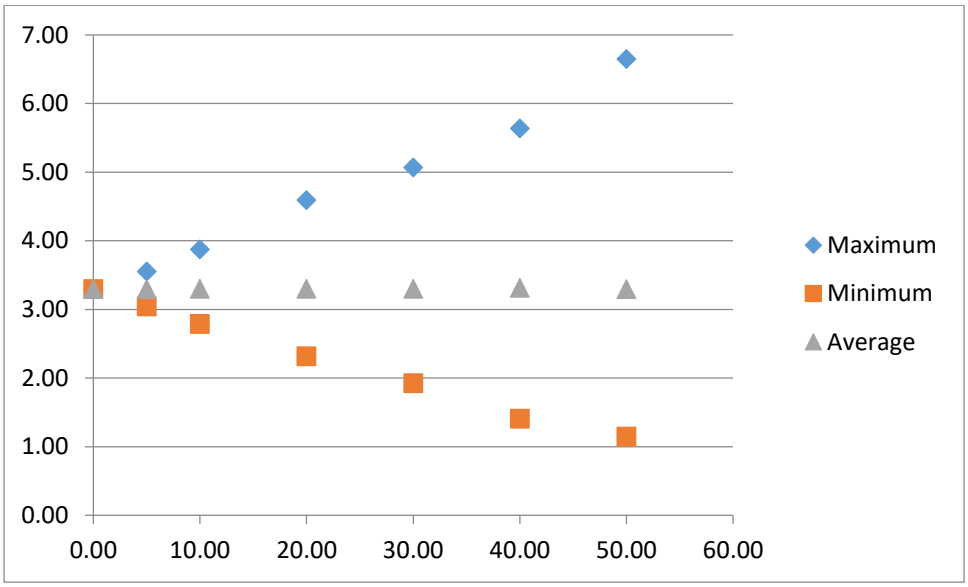

Figure 9: ROA values with random variation in A_{cv}, C_A $and A_u$ values For Attack Tree B After Upgrade

4 CONCLUSION

Two attack scenarios on compromising a database in a school network was considered in this study. The network was quantitatively analyzed using the attack tree method. The ROA for each attack scenario was calculated and in both cases, they turned out to be > 7.0; which meant there in the high range band. The implication was that the database could easily be compromised. When suggested upgrades were implemented, the ROA values reduced to 4.32 and 3.30 for Attack Tree A and Attack Tree B

respectively. The values are acceptable because they fall in the Medium range. Even when errors in the Access Vector, Access Complexity and Authentication values were used to calculate the ROA values, the values fell within the 4 – 7 range, which is an acceptable bound. The results of the study held steady. The method can, therefore, be used to mitigate and by extension, used to quantitatively assess the vulnerability of computer networks.

6 REFERENCES

[1] Greitzer, F. L., Paulson, P. R., Kangas, L. J., Franklin, L. R., Edgar, T. W., and Frincke, D.A. (2009). *Predictive Modeling for Insider Threat Mitigation*, PNNL Technical Report PNNL-SA-65204. Richland, WA: Pacific Northwest National Laboratory

[2] Xynos, K, Sutherland, I, Read, H, Everitt, E and Blyth, A, (2010), *Penetration Testing and Vulnerability Assessments: A Professional Approach*, Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23-2 August 2010.

[3] World Institute for Nuclear Security, (WINS), (2010), *Managing Internal Threat, A WINS International Best Practice Guide for Your Organization*, Vienna, Austria.

[4] World Institute for Nuclear Security, (WINS), (2012), *Human Reliability as a Factor in Nuclear Security*. A WINS International Best Practice Guide for Your Organization, Vienna, Austria.

[5] Roger, G. J., (2010a), Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities. *Journal of Physical Security*, 4(2), 30-34.

[6] Roger, G. J., (2010b), Changing Security Paradigms. *Journal of Physical Security*, 4(2), 35 - 47.

[7] Dacier, M., Deswarte, Y. and Kaâniche, M., (1996), Models and Tools for Quantitative Assessment of Operational Security, *In Information Systems Security*, 177-186, Chapman & Hall, Ltd. London.

[8] Balzarotti, D., Monga, M. and Sicari, S., (2006), Assessing the Risk of Using Vulnerable Components, *In Quality of Protection*: pp 65 - 78, Springer Science+Business Media, LLC, NY

[9] Edge, K. S., Raines, R. A., Baldwin, R. O., Grimaila, M. R., Bennington, R. W. and Reuter, C. E. (2007), Analyzing Security Measures for Mobile Ad Hoc Networks Using Attack and Protection Trees, *Journal of Information Warfare*, Vol. 6, No. 2, pp. 25-38.

[10] LeMay, E., Ford, M. D., Keefe, K., Sanders W.H. and Muehrcke, C., (2011), *Model-based Security Metrics using ADversary VIew Security Evaluation (ADVISE)*, Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems (QEST 2011), Aachen, Germany, Sept. 5-8, 2011, pp. 191-200.

[11] Akinola, A. A., Kuye, A. O. and Ayodeji, A., (2014), *Cyber-Attacks Analysis of a School Network*, 55th Annual Meeting of the Institute of Nuclear Materials Management (INMM), July 20-24, 2014.

[12] Amenaza, (2005), *Fundamentals of Capabilities-based Attack Tree Analysis*, Amenaza Technologies Limited, Suite 550, 1000 8th Ave SW, Calgary, Alberta, Canada T2P 3M7.

[13] Cremonini, M., and Martini, P., (2005), *Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)*, Fourth Workshop on the Economics of Information Security, June 2005.

[14] Mell, P., Scarfone, K. and Romanosky, S., (2006)., Common vulnerability scoring system. *IEEE Security & Privacy Magazine*, 4(6):85–89.

[15] Baker, W. H. et. Al.; Necessary measures: metric-driven information security risk assessment and decision making, *Communications of the ACM*, 50:10 P. 101-106, 2007.

[16] Peltier, T. R. *Information security risk analysis*, CRC Press, 2005.

Design and Implementation of a Knowledge-Based Authentication System (C010)

Farouk O. Adebayo, Rukayat A Koleoso
adebayofarouk@gmail.com , rajetunmobi@unilag.edu.ng
Department of Computer Sciences, University of Lagos

ABSTRACT

Authentication is the first line of defense against compromising confidentiality and integrity. In general, users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are hard for users to remember. In this paper, the design and implementation of a stronger method of authentication and easier to access mode of authentication is discussed. This method is the Knowledge-Based Authentication (KBA) method. This was done by collecting user details and storing them in a database, then training the system with this data collected. After that, designing test mechanisms to test the user if he is really a genuine user. This paper also discusses issues that surround knowledge-based authentication systems. The idea behind knowledge-based authentication is that by selecting questions that only the target individual would know the answers to, systems can verify whether the user is the legitimate owner of a secured account.

Keywords: Access, Authentication, Knowledge-based, Password, Privacy.

1. Introduction

The traditional authentication method based on combining user name and password offers a fertile ground for masquerade attacks. This is because they are based on a single piece of knowledge that can be shared or can be found using hacking tools such as password cracker [1]. More and more online systems and mobile applications are carrying valuable information from privacy or monetary perspective for the various stakeholders involved (e.g., customers, manager, online users, etc.). Examples of such systems include online paid subscriptions sites, web mails, web banks, social network websites, instant message systems, online stores, public libraries, and online tax systems. For these kinds of systems, traditional authentication schemes based solely on basic user name and password combination are not strong enough. Alternative schemes replacing or reinforcing the above schemes are needed for better cyberspace security. In this paper, we propose the Knowledge-Based Authentication solution. This solution was chosen because of the simplicity in modelling and the security strength it can offer when put in place.

According to the definition for commercial systems, Knowledge-based Authentication (KBA) is a security measure that relies on contextual and historical user information. The security measure, along with data provided and collected from the user or from other Internet sources made by the user to determine the probability of whether a user interaction is genuine or not and how the entity can confirm this information already known by the system [2]. The implementation of a KBA system consists of first knowing about the user and having a user

profile, before deciding on the appropriate level of test to put the user through in order to confirm is identity.

The aim of this paper is to create a more secure system by using KBA and applying this to an online helpdesk system. This paper shows how this authentication mode is integrated into web applications to secure the system. The objectives of this paper are providing a more secured mode of creating and assessing online web application; to create a cost effective solution for identity proofing, and, securing systems using knowledge-based authentication mode that tests what the user knows on a more complex level.

2. Related Works

Different situations call for different measures of security. Technology is moving fast and the world is changing swiftly underneath our eyes, the measures taken to ensure security in the last decade might not be applicable now, and if they are, they will have become obsolete and completely discouraging [3]. In addition, for the different situations mentioned and thought of, the level of security needed for them differ because the level of damage that can be caused and the issues at stake with a single breach is different most in different scenarios. In some cases, a little amount of money could be lost, and in some cases life is threatened, also in some cases, society, even countries are threatened and a whole level of data about people, money that can cater for multiple countries and other critical information is at stake. Indeed security breach effect could be negligible in some cases, and in some scenario, it could be hazardous and disastrous, while in other cases, it is just completely unacceptable. Knowledge-based authentication, as the name suggests, requires the knowledge of private information of the individual to prove that the person providing the identity information is the real owner of the identity. This information is more advanced than the kind of information a fraudster might be able to access through your email or computer. [4]

There are three types of KBA namely:

a. **Static KBA,** also referred to as “shared secrets” or “shared secret questions”, is commonly used by banks, financial services companies and e-mail providers to prove the identity of the customers before allowing account access, or as a fallback if the user forgets their password. At the point of initial contact with a customer, a business using static KBA must collect the information to be shared between the provider and customer, most commonly the question(s) and corresponding answer(s). This data must then be stored to be retrieved wen the customer comes back to access the account. [5]

b. **Dynamic KBA** is a high level of authentication that uses knowledge questions to verify each individual identity, but does not require the person to have provided the questions and answers beforehand. Questions are compiled from public and private data such as marketing data, credit reports, or transaction history, so it is an attractive option for e-signature users that need to be authenticated instantly [6]. We sometimes call these questions "out-of-wallet" questions

because the information cannot be found in a person's wallet if it was stolen. To initiate the process, basic identification factors, such as name, address, and date of birth or just a social security number (SSN) must be provided by the consumer and checked with an identity verification service. After the identity is verified, questions are generated in real time from the data records corresponding to the individual identity provided. Generally, the period for the person is given to respond to questions and the number of attempts is limited to prevent answers from being researched. [6]

c. **Enhanced KBA** is just like dynamic KBA, in that it presents multiple-choice questions to users. The main difference is in what is used to generate these questions [2]. It provides complete privacy protection on customer data; it also has the ability to provide unique, relevant questions to your consumers. It uses internal proprietary data behind firewalls to generate answers. It replaces shared secret questions with a safer authentication method and leverages the technology of Software as a Service (SaaS).

Where KBA is used? Most organizations across the world use KBA within their business processes to identify and stop fraud. While KBA certainly is part of the onboarding process when a new customer visits you remotely for the first time, it is also incorporated for existing customers that visit your organization via a new remote channel or engage in a high-risk activity. Government, Healthcare, E-commerce, Insurance, and Financial services are some of the sectors that use KBA.

Knowledge-Based Authentication Attacks:

As is common with all systems that are secured via one authentication mode or the other, hackers, cybercriminals and other than they will definitely try to attack the system and get data. The attack pattern of knowledge-based authentication are as follows, but are not limited to these: Password Brute Force, Spoofing attack, Physical security attacks, and Shoulder surfing attack.

3. Methodology

The new system developed is a web-based application that provides a better and adequate security to the user accounts and the system itself.

This new system serves as one with tighter security that limits and powers of intruders and provides ease of access. This new system is an online e-logging helpdesk that allows the use of knowledge based authentication to be used to gain access into the system. This application can be used at anytime and anywhere as it short words, provides better security than the username and password authentication system we are trying to improve on. It should be known that this knowledge-based authentication system is an advanced form of what the user knows. It tries to implement identity proofing in a way that it will not be too hard or too strenuous for the genuine user to get and it will be too complex for an intruder to get, thereby fulfilling its purpose of better security.

The following are the characteristics that the system possesses:

1. Easy access to information when needed as system is automated
2. Knowledge and information are well documented hence the system allows for future contributions
3. More secure and safer system cos of the increased level of authentication
4. Ease of use and ease of implementation
5. Relies on knowledge that the system has learnt about the users

The use of KBA to access the system was deployed, as well as using KBA tot eh secure the system. The security questions asked are often out of the wallet questions that are not too hard to remember and are so concise that only the genuine user will be able to answer. The procedural design of the system is shown in Figure 1 below:

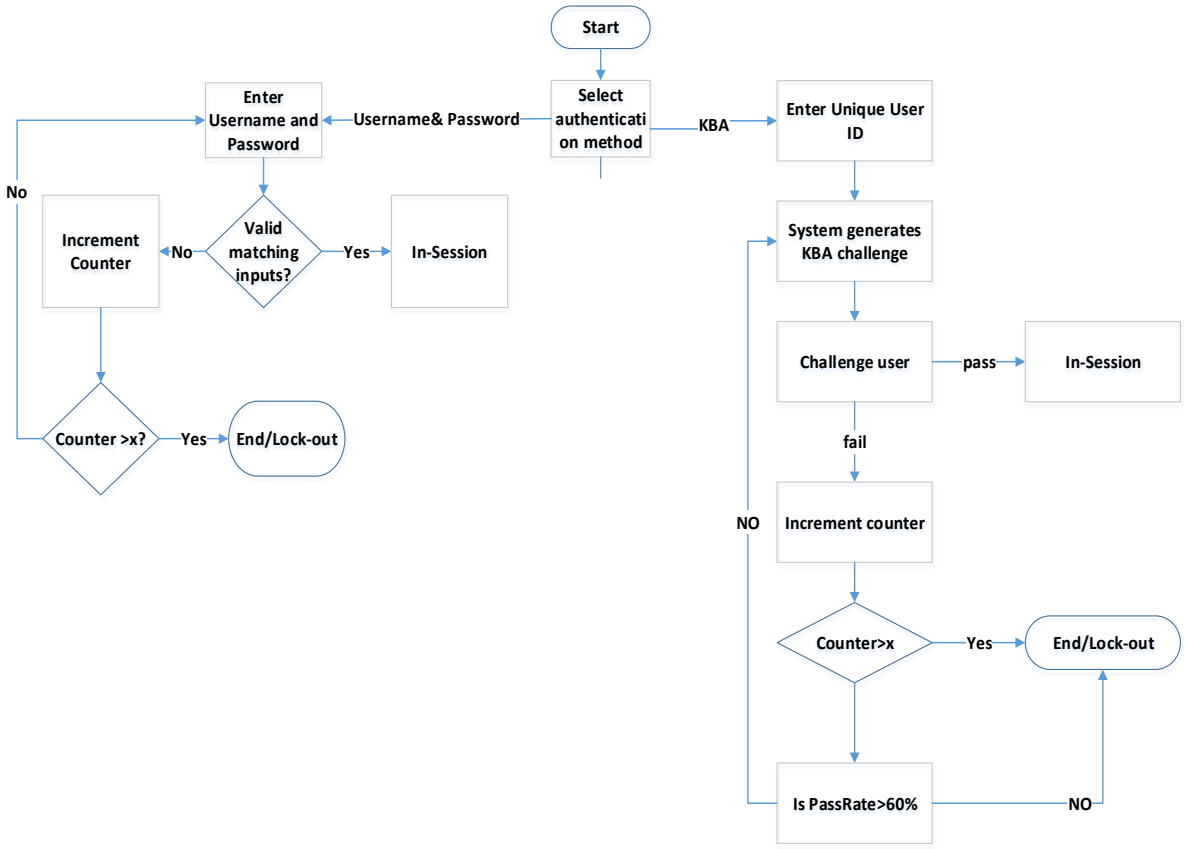

Figure 1: Procedural design for KBA

The system was designed using Unified Modelling Language (UML) via the Use Case diagram. The methodology was executed using the procedural design shown in Figure 1 above, while its database was created using phpmyadmin.

The online e-logging system using knowledge-based authentication system was developed to improve the authentication system of applications. Also, it serves as portals that need to be secured and provide fast, convenient, and more secured identity assurance and

4. Result and Discussion

provide strong authentication across channels to reduce risk and cost.

Figure 2: Output result 1(Generated from App built)

Below are figures of the developed web application for the online helpdesk system using knowledge-based authentication.

Figure 3: Output Result 2 (Generated from App built)

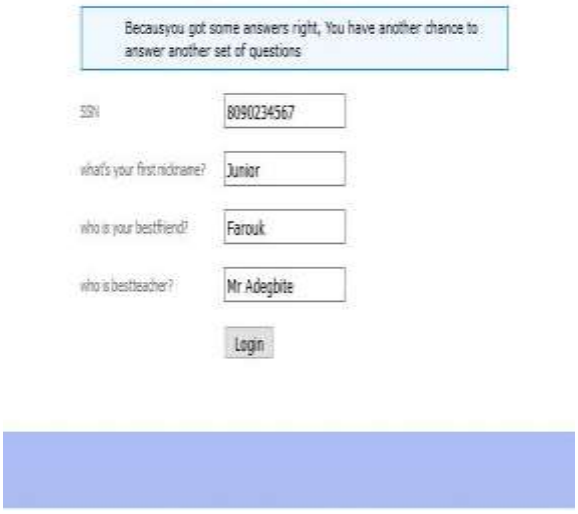

Figure 4: Output Result 3(Generated from App built)

Figure 5: Output Result 4 (Generated from App built)

Figure 2 represents the Knowledge-based authentication form and challenge questions that the user is initially supposed to fill in order to gain access into the system. Figure 3 represents an example of a user's details when he tries to use the Knowledge based authentication system. Figure 4 shows what happens when the user that tries to log in using the KBA doesn't get all the challenge questions right, the forgiveness protocol allows him to attempt to log in again giving him alternative challenge questions. Figure 5 shows the result when the user fails the second set of challenge questions generated for the user. At this stage, the user is locked out of the system.

5. Conclusion:

The aim of this paper is to discuss how to provide a solution to the traditional authentication method of username and password by implementing a knowledge-based authentication method to log in to an online helpdesk portal. This knowledge-based authentication manner of authentication is more secure than the traditional username and password manner that is fast becoming dead and obsolete. Even though knowledge-based authentication has its own flaws and it is not the perfect manner of authentication, it has its merits and understandable demerits, it is better than the traditional username and password method we are trying to improve on. The system is easy to use, convenient and has a higher level of security. Some of the qualities of this system are ease of use, convenience, and high level of security.

Though the system is not perfect, it serves as a basis from which other KBA can be developed upon, particularly via the use of Expert systems.

6. References

1. Rika Butler, (2007) "A framework of anti-phishing measures aimed at protecting the online consumer's identity", The Electronic Library, Vol. 25 Issue: 5, pp.517-533.

2. David Jablon (2004*), Methods of Knowledge Based Authentication*, KBA Symposium, pp2.2

3. Thorpe, J. (2008), *On the predictability and security of user choice in password*, in *Computer Science*. CARLETON UNIVERSITY: Ottawa, Ontario. p. 197.

4. Jain, R. Bolle, and S. Pankanti, (1999) *"Introduction to Biometrics," Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers.

5. Biddle, R., S. Chiasson, and P.C.v. Oorschot (2009), Graphical Passwords*: Learning from the First Generation:* Ottawa, Canada

.

6. Usha T., Tara H., Shidaganti, G. (2013) "*Knowledge Based Authentication Mechanism using Persuasive Cued Click Points"* International Journal of Engineering Research and Technology (IJERT), Vol. 2(6) pp. 258-266

Web-based Employee Management System for Nigerian Institute of Medical Research (C011)

Ijoga E. O[1]* and Adewole A .P[2]

[1]ICT Unit, Nigerian Institute of Medical Research, Yaba, Lagos

[2]Department of Computer Sciences, University of Lagos, Akoka-Lagos

eo_ijoga@yahoo.com

ABSTRACT

A computerised information system utilizes different kinds of software in the management process of human resource related data in organisations. As employees in organisations continue to add values as individuals, the traditional approach in the management of human resources is no longer adequate, hence, the need to adopt a different administrative method. Also, there may be a panic situation if personnel data is lost as well as the need to have a speedy access to employee information, even from remote locations. This paper focused on the design and implementation of a web-based Employee Management System (EMS) for Nigerian Institute of Medical Research (NIMR). The system was developed using Agile Model, a user friendly Interface and a Microsoft SQL relational database. The programming tool includes Microsoft visual studio 2017 platform and C Sharp (C#) as the language. The developed system filled the missing gaps in the electronic management of employee information in the Institute. The system is used among other things to manage staff leave request, profile, designation, holidays etc. based on individual access priority.

Keywords: Web-based, Personnel information, System, Institute, Nigeria.

1.0 INTRODUCTION

Employees are the most important and valuable resources in any organization. They play major roles in deciding the achievement of the organization. Thus, their knowledge and skills must be used to the maximum so as to create values in the organization. Consequently, Organizations need to devise strategies on the best way to recognize and motivating staff performance at work. In view of this, EMS has come to play an essential role in assisting organizations to attain their goals of productivity. An EMS consists of essential work-related and important personal information about employees. This was study done with respect to Nigerian Institute of Medical Research, Lagos. The selected Institution is the foremost health research Institution in Nigeria. It is an Agency under Federal Ministry of Health with staff strength of about 320.

1.1 Problem Statement

Careful inquiry from the department of Administration of the Institute reveals that the Institution does not have any software for managing her employee information. Thus, the need to develop an advanced EMS to address the under listed issues:

i) Manual management of personnel information which poses a lot of challenges.
ii) Speedy access to personnel information from remote places
iii) Database backups; panic situation of data loss.

1.2 Specific Objectives of the Study

i) To develop web-based software that will effectively manage employee information.
ii) To implement a functional database management system that will contain specific employee information as captured in staff record of service.

iii) To develop a system that can provide full database backups for the Institute

iv) To develop a user friendly front-end for interaction between the users of the application and the developed system.

2.0 RELATED STUDIES

Employee management systems have been studied extensively by many researchers across the World. However, a brief review of some studies will shed more light on why Institutions and Organizations acquire and manage their personnel information using EMS. Noronha, Aquinas and Maneze (2016) reviewed many literatures on personnel management system and compiled the various challenges experienced in the implantation of personnel management system. The literatures used in the study were obtained from organizations across different paper businesses. Though, such study ought to be done at each organization separately so as to identify such organization's peculiar challenge. Noronha, Aquinas and Maneze (2016) did not capture the feedback gotten from the managers of these Organizations where the studies were done knowing fully well that not in every case that academic perception is the same with realities. Zhang, Xiang, and Wang (2014) studied related literatures on human resource management and came up with a position that there exist an encouraging relationship between performance of an Organization and that of personnel. Zhang, Xiang, and Wang (2014) reported that concentrating on the arrangement of human resource system and discovering how such a system could accomplish high performance by different systems have significant theoretical and practical applications. Nevertheless, the conclusions from the study did not clarify why Organizations that do not adopt high performance approach also achieved outstanding performance. Huang (1995) studied the conditions of human resources in higher vocational Colleges and based the discussion of the article on the findings. Huang (1995) describes the fundamental idea behind human resource management, the main function of human resources management as well as the developmental goal a system. Bansal (2014) opined that globalisation and the advent of Multi-Nationals that employ large number of staff, warranted Organizations to computerise her employee record so as to have access to such information from any location. Bansal (2014) stated other reasons such as turnover rates, non-attendance and new enrolments etc. happening in the global marketplace calls for effective and efficient management of employee information system. Similarly, Zhang (2016) explained that the SSH fuzzy mathematics technique is optimistic in developing enterprise human resources management application. Through the assessment of production ration of an enterprise, Zhang (2016) made a systematic contrast at the level of management of human resources in different establishment using SSH fuzzy mathematics method. This method made the assessment index analysis more detail and demonstrated that SSH fuzzy framework can actually improve the performance of human resources management system. Xu, Yue, and Kai (2014) designed a smart personnel management solution that uses an Android phone. The system was used to solve security monitoring challenge and management of aged, kids and employees of companies. Suraj, Aquinas and Aruna, (2016) compiled different literatures on the difficulties confronted with usage of performance management system. Utilization of the guide discussed by Suraj, Aquinas and Aruna, (2016) will help minimize problems in the implementation of a new application or modifying the existing one. The work of Aribisala and Olusuyi (2014) relates to database management system for staff of the National Iron Ore Mining Company, Kogi State, Nigeria. Achola (2013) developed a system that determined the efficiency of the human resource management at Kampala International University (KIU). Achola (2013) adopted the Quasi-experimental approach using Sloven's formula with a sample size of 350. Using descriptive and inferential statistics for analysis, the study showed that management information system for personnel of the Institution seem to be poor. In the context of Syed et al. (2013), management of Administrators of human resource Department in Organizations was the focus. The study of Syed et al. (2013) combined the management of human resource and fundamental activities with information technology. The specific objective of the paper by Syed et al. (2013) was to lessen the job of an

Administrator to keep records of daily activities like attendance, works, appointments, etc. Staff records, hourly attendance e.t.c were used for performance appraisal for employee.

3.0 MATERIALS AND METHOD

The model preferred for this study is Agile Software Development Life Cycle (SDLC). Agile is flawless for a paper of this kind since it will go through series of iterations so as to give opportunity for enhancement. The other reasons for this choice are:

i) Agile model creates room for continues learning from each iteration process.
ii) Prototype can be delivered and modify in each cycle
iii) Agile Model encourages frequent and collective troubleshooting.
iv) The intrinsic collaboration in Agile Model increases visibility.
v) Agile Model does not allow papers to get stalled due to its feedback mechanism

Table 3.1 minimum hardware and software requirements

Components **Specifications**	
Processor IV and above	Pentium
Main Memory (RAM size) and above	2Mb
Network Component card	interface
Operating System and Linux	Windows
Hard Disk capacity Minimum	80GB

The front page tool is html. The html is one of the major languages used for creating web pages and it is fairly easy to study and manipulate. The programming language is C-Sharp (C#) because of its consistency, extremely rich syntax coupled with reliability and flexibility platform provided by .net Framework. The Database Management System selected for this study is Microsoft SQL Server. This was due to the efficiency and affordability of this Server. The researcher consulted with the Administration department of the Institution to discuss and gather all necessary information regarding employee of Institution. In addition, the Institute annual report as well as personnel record was studied in detail to know the functions, requirements and possible new features that will enhance the system. Also, to create relevant use cases for the system, the following actors were identified:

i) Employee
ii) Head of Department
iii) Head of Administration

3.2 Procedural Design

Administrator Algorithm

Step 1: Open the Institutional website

Step 2: Click on EMS icon to login

Step 3 A: If you are a registered user, your profile will be traced

Step 3A-01: after successful login, then the desired access is granted

Step 3A-01: can add new employees

Step 3A-01: can see detail profile of each employee

Step 3A-01: Accept/Reject leave requests.

Step 3A-01: Edit user role

Step 3A-01: View user activity log

Step 3A-01: Create Departments/Units

Step 3A-01: View his/her own profile

Step 3A-01: Delete profile

Step 3A-01: Add holidays

Step 3A-01: Add designation

Step 3B: you are not a registered user

Step 3B-01: Contact the administrator for you username and password

4.0 DISCUSSION OF RESULT

The application is web-based and it is accessed via the institutional website as shown in figure 4.1. For the purpose of testing, the application was hosted on a laptop computer running Windows 7 operating system, Visual studio version 2017 and SQL Microsoft management server. The black box testing approach was used by a potential user (Administrator) to access, register and view staff profiles.

The system comprised of many sub-programs ranging from designation, leave management, holidays, employee profile and many more. Access priorities are based on three different levels; administrator, head of department (HOD) and employee, each with their own limitation. The administrator of the Institute is given the super user access which is the highest access level on the system to perform all functions built into the system. On the system, only the administrator has the exclusive right to create, delete and update any record provided on the system. The administrator creates a user name with the Institute domain email and password for each user of the system. Another category of user of the system is the head of department who is given the right to view only the details of employees in his or her department and unit. The HOD also has the right to make recommendations on staff leave request from his or her department. The last category of user is the employee who has the least access priority to login, view his or her personal profile, holidays, and request for any type of leave and views the leave status; whether the leave has been approved, denied or pending. The use of this system provide opportunities for administrators to access any information about their employee as captured on the system any time and from different location on the globe once there exist internet access. Hence, it could serve as an online inventory of all employees in an Organization. Performance and simplicity were some of the issues considered in the development of the system. The system provides a dependable, simple to use and large data repository for the Institute. Hence there will be no record manipulations, irregularity and redundancy in the Institute.

The fallout of the new system is cost reduction and minimal paper work and the will be more transparency in operations. Also, it is important to recall that only the administrator has the exclusive right to the portal. Thus, any information obtained from the system will be truthful because it is coming from the Management. The Administrator updates employee record regularly if the need arise, hence out-dated information is seldom found on the system. Employees can track their records at any given time and from all locations around the globe once internet access exists. The developed system will provide a centralized record management for employees in the Institute. It overrides the difficulties dominated in the existing manual approach and reduced to the barest minimum the hardships confronted with the use of manual method. The system is built in its simplest form so as to minimize likely errors that may arise while inputting data. This research has provided an efficient way to handle most personnel challenges in the Institute and it will go a long way to boost staff morale. This study is part of the researcher's commitment to contribute his quota to Institute development and bring about an efficient way to manage personnel information.

5.0 CONCLUSION AND RECOMMENDATION

The study gives a perfect understanding on the development and use of EMS. The software solution developed is unique and it replaces manual and paper based approach used to manage employee information in the Institute. The system achieved all the user requirements. The user interface is excellent and is easy to navigate. Those with little skill about computer can find their way around the application. The system will be useful in the management of the internal operation of employee details, Leave, etc. The simplicity in the use of this EMS will reduce daily workload of the Administration department, increases productivity and employee satisfaction. The study will contribute to the existing literature in this

area and serve as a guild for other researchers. Regardless of the fact that the specific objectives of this research were fully met, there were some constraints in carrying out this study. These include non-availability of financial support and non-disclosure of useful information by personnel of Administration department. Having mentioned the challenges, this system can be improved upon by integrating functionalities such as:

i) Biometric attendance.
ii) Payroll
iii) employee Performance module

REFERENCE

Achola, A. (2013). Management information system design on human resource management of Kampala international University*: design and implementation. Information and Knowledge Management, 3*(6), 22-27.

Alshamrani, A. and Bahattab, A. (2015). A comparison between three SDLC models waterfall model, spiral model, and incremental/iterative model. *International Journal of Computer Science, 12* (1), 106-111

Annual Report of Nigerian Institute of Medical Research, 2016.

Aribisala, A. and Olusuyi K. (2014). Design of an employee management system (a case study of National iron Ore mining company, Itakpe). *International Journal of Mechanical Engineering and Information Technology, 2 (11),* 832-841

Bansal, A. (2014). Computerised human resource information system– an emerging trend for managing human resources. *International Journal of Innovative Technology and Exploring Engineering*, 3, (10), 33-35

Huang, G. (1995). Fuzzy mathematics method's application to economic analysis. *Financial Research,10, 65-68.*

Noronha, S.F, Aquinas, P.G. and Manezes, A. D. (2016). Is job performance better

attributable to performance management system through work engagement: *Indian*

Journal of Commerce & Management Studies, 2, (18), 2-6.

Staff Record of Nigerian Institute of Medical Research, 2018.

Suraj F.N., Aquinas P.G. and Aruna D.M. (2016). Implementing employee performance management

system: a scoping review. *International Journal of management and applied science,* 2, (5),

85-89.

Syed, N. A., Syed Fiaz A.S, Prabhadevi C, Sangeetha V and Gopalakrishnan S. (2013)

Human Resource Management System. *Journal of Computer Engineering, 8(4) 62-71.*

Xu X, Yue, L. and Kai, Z. (2014). Design and implementation of intelligent personnel management system. *Applied Mechanics and Materials, 602-605,*

Zhang, J. (2016). Design and implementation of human resources management system using Ssh fuzzy framework. *International Journal of Simulation: Systems, Science and Technology, 17* (15), 19.1-19.6.

Zhang, W. Xiang, L. and Wang, X. (2014). The partitioned management model for large data and its application. *Journal of Harbin Technology University, 5, 353-360.*

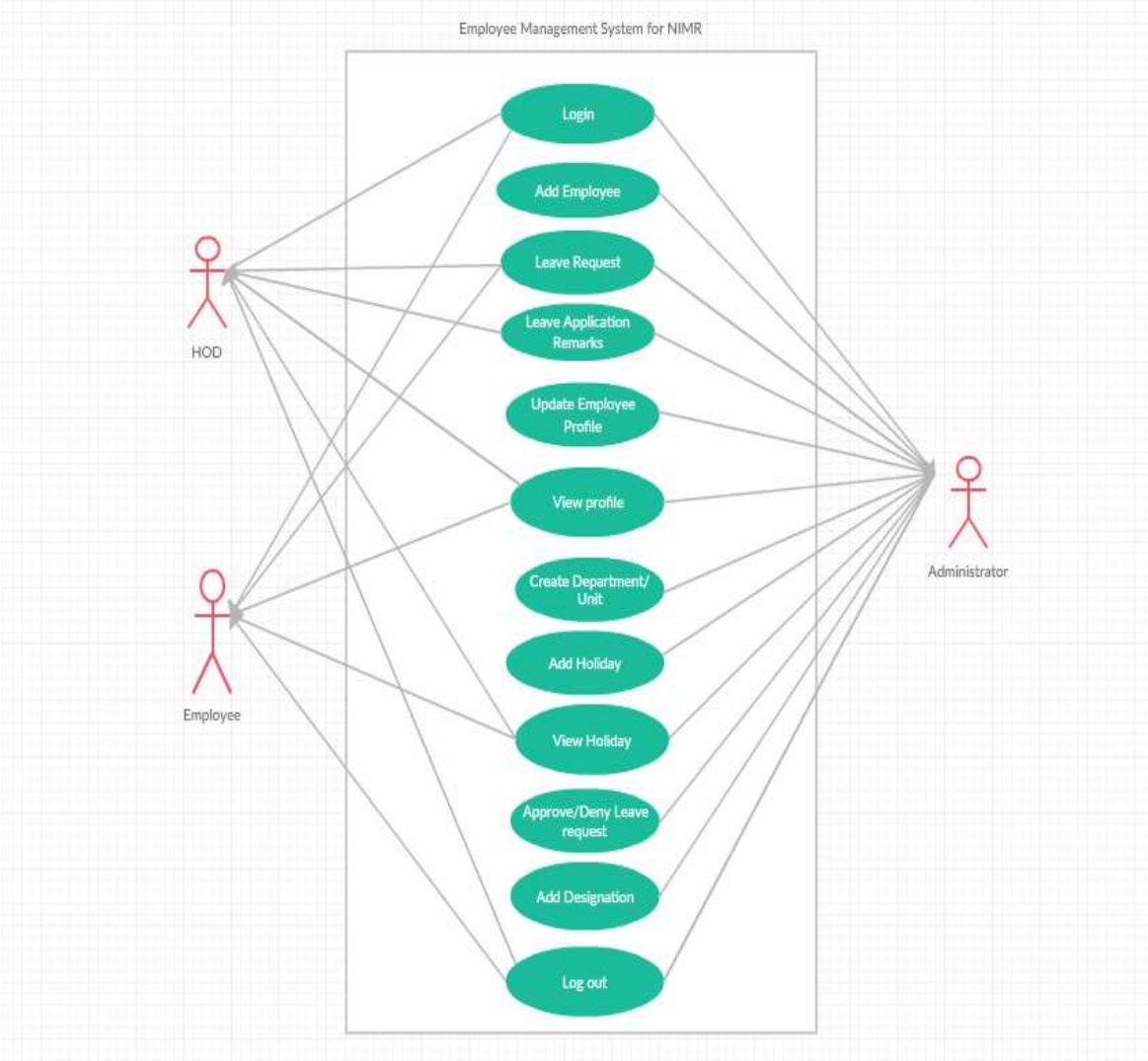

Fig. 3. Employee Management System Use Case Diagram

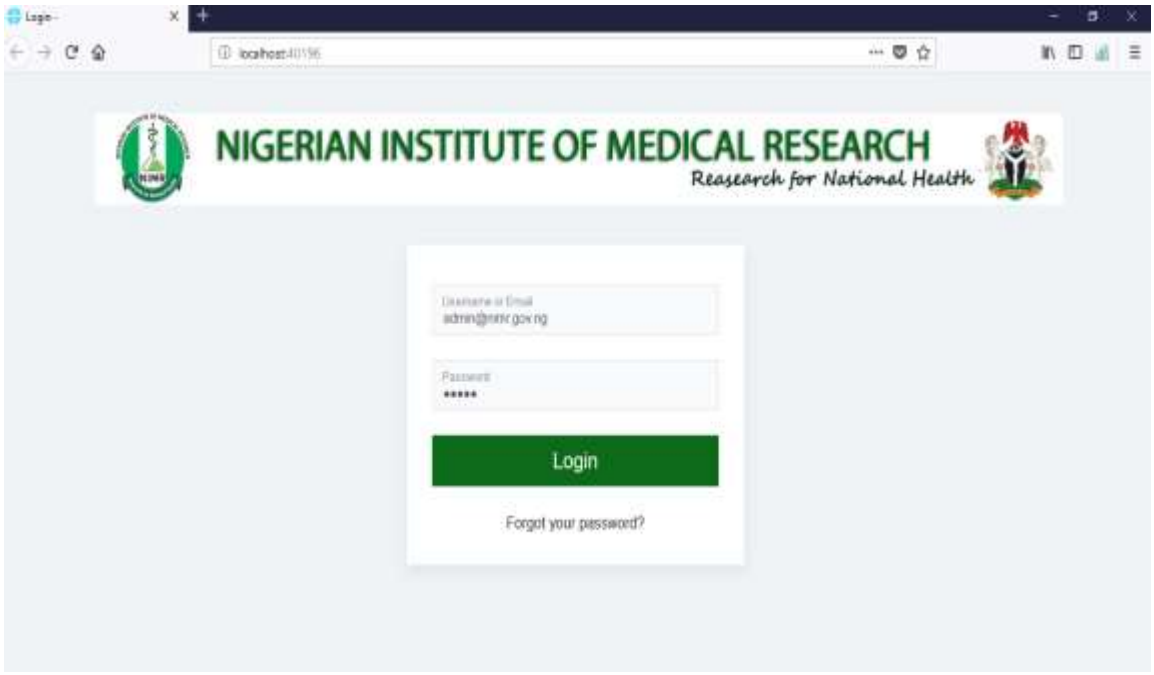

Fig. 4 Login page

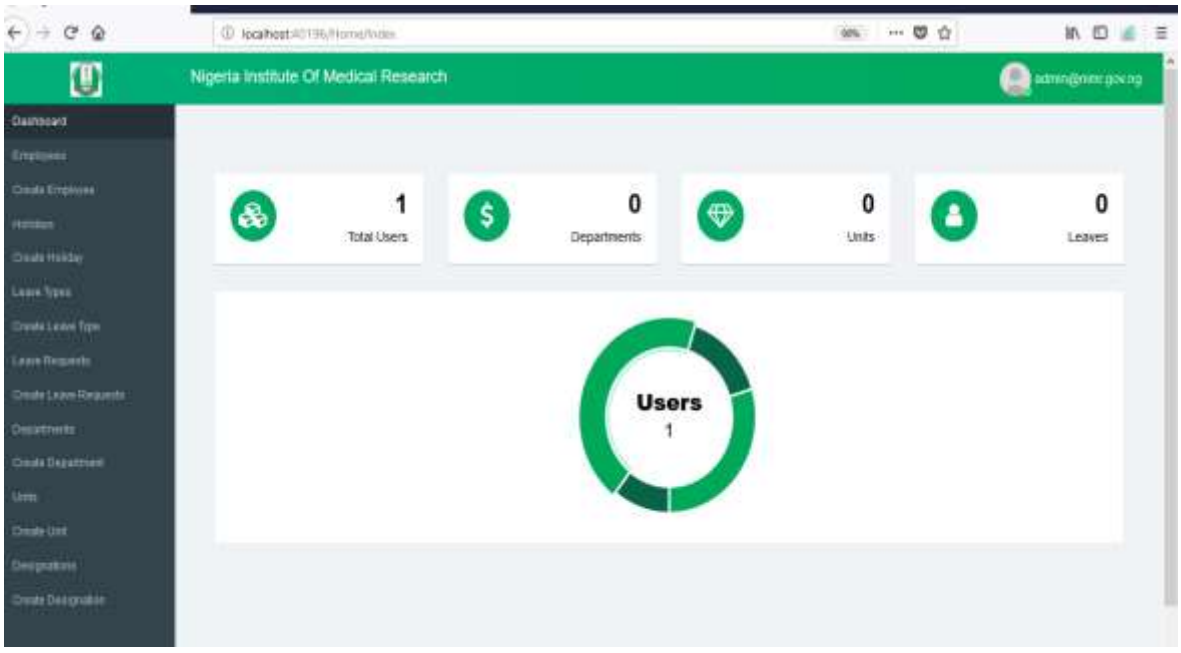

Fig. 5 Dashboard

Password Authentication and Staff Awareness Training: Towards Security of Enterprise Users (C012)

Achunike, Victor U.

Dept. of Computer Science, Institut Bilingue libre Du Togo, IBLT,

(Liberal Bilingual Institute of Togo) Lome, Togo uachus@gmail.com

ABSTRACT

The importance of securing users cannot be overemphasized in today's networked corporate world. Major factors in reducing security breach are ensuring password authentication and implementing an effective security awareness program in enterprises. The study examined these two security solutions typically deployed in managing user systems security challenges in enterprise networks. Data was obtained through secondary sources. The data collected were analysed using Analysis of Variance (ANOVA) technique. Findings review that the success level of the two security measures towards a comprehensive systems protection in organizations is significantly low. The study recommends their adoption notwithstanding and deployment of other security solutions for prevention of Information and Communications Technology, ICT security-related incidents within networked environment.

Keywords: security, information & communications technology, password authentication, staff awareness program, enterprise networks.

I. Introduction

Organizations, either big or small cannot afford to permit classified data to be accessed by unintended persons. Theoretically, a person that hacks into an enterprise network, can monitor data traffic, and take control of the critical business applications and the enterprise operating system services. In order to ensure confidentiality, integrity and availability (CIA) of data and information systems, relevant measures, controls and procedures applied by enterprises. The CIA triad is one of the core principles of information security. *User* or client system refers to personal computer, PC that uses the services offered by the servers. These users or client workstations can send requests to servers and equally process information from servers in a networked environment.

Securing user-systems requires that individual users be authenticated before access can be given to use system resources. User identification (user Id) refers to the systems' ability to identify and distinguish between every PC user. Authentication seeks to proof the identity and genuineness of a certain user. This can be realized with the aid of passwords, or with auxiliary devices like smart cards and hardware tokens [9].

The password is a secret sequence of characters only known to the authorized user for enabling computer access. Strong password authentication typically consists of at least eight alphanumeric characters mixed with special symbols, having a maximum duration of days or weeks and encrypted.

In this decade of the 21st century, the venerable password is no longer adequate. The combination of username, the public identifier for the user account, and the password, the secret key which unlocks access to that account, is enough security for most people on stand-alone computer systems. But for systems on a network, an additional protecting factor is useful and demanded. The hardware token is a physical device provides this extra level of security to complement the previous. The device permits the token's owner access to a computer or a network, by generating a number which uniquely identifies the user to the service, and allows logging in.

While security tools are seen as essential part of an enterprise security program, it is also imperative that cultural change through security awareness be incorporated. Zink, L., (2017) stated that this can be implemented by ensuring every employee is equipped to play a role in securing oneself, her company and its assets from both a logical and physical security vulnerabilities. Security awareness will enable all employees to work together to guarantee a successful sustainable security posture for the company. M. Drolet (2018) argued that an organization could have the most robust security program, stringent policies, and the latest and greatest security software tools. Yet, employees should have the right training and a working understanding of the policies and the potential risks, for safety of data.

1.1 Statement of the Problem

Most users feel that Security is someone else's job. When left on to their choice, client users habitually selected simple and obvious passwords, such as "password" or "qwerty". Others used *easy-to-guess* passwords like family members' name, or an important date [12].

With the rapid growth of the internet and the reality of electronic commerce; many corporations have become highly dependent on digital information systems for ease of business. Many businesses are now conducted over online platforms. The situation where an intruder with a compromised password of an enterprise user gains unlimited access to all his online service accounts is worrisome. Identity theft takes many forms -- exploiting weak passwords, keystroke capture, phishing, Trojan software, social engineering, password sharing, and so on [9].

Nowadays, computer networks constitute the core component of governments and private enterprises' IT infrastructures globally [6]. The trust of this study is on the impacts of two internal security mechanisms (strong password authentication and staff security awareness training) towards optimal safekeeping of business operations. Analysing the strength of these security procedures is sure approach in combating systems threats within working environments. It is increasingly recognized that user authentication and adoption of security awareness programs for staff are among key factors in securing computers in industries. In this study, it became pertinent to find out if the selected security tools are capable of offering maximum protection against most ICT-related incidents and destruction of data in enterprises.

1.2 Objectives of the Study

a. To offer theoretical and empirical insight into security of user systems via password authentication of users systems.

b. To assess modern trends that involved training companies' employees on security

Details.

c. To analyse the effectiveness of the two selected system security measures of password authentication/user Id and staff security awareness training in enterprise networks.

1.3 Research Questions

In view of the above highlighted issues, the following research questions were relevant:

[1] To what extent can password authentication and staff security awareness training provide security to user computers in companies?

[2] What is the relationship between the two internal security mechanisms (of password authentication and staff security awareness training) and ICT security-related incidents in enterprise networks?

1.4 Hypothesis Formulation

For the purpose of the study, some hypotheses have been formulated and tested:

i) H_o: The implementation of both password authentication/user identification and staff security awareness training do not

offer significant protection against ICT security-related incidents in enterprises.

H_A: The implementation of both password authentication/user identification and staff security awareness training offer significant protection against ICT security-related incidents in enterprises.

ii) H_o : The levels of the two internal security mechanisms have no significant impact on the destruction or corruption of data in companies.

H_A : The levels of the two internal security mechanisms have significant impact on the destruction or corruption of data in companies.

1.5 Delimitation of The Study

The study will focus primarily on the effects of strong password authentication and staff security awareness training in enterprises across various sectors, such as manufacturing, real estate, electricity, transportation and storage, information and communication, in twenty-six European Union, EU countries. The size of employee ranges from large enterprises of 250 persons and above, to small enterprises, with at least ten persons employed.

II. Review of Related Literature

Different sectors of the economy—both public and private amass a great deal of confidential information about their employees, customers, products, research and financial status. As the threat landscape mutates, IT security professionals must to adapt to the evolving threats with the assumption that users are vulnerable—whatever PC type or brand. Therefore, protection of the users in the networks from malicious intrusions is critical to the economic progress of our nation.

User System security is concern with processes and mechanisms by which sensitive and valuable information and services are protected from unauthorized usage or non-trusted individuals. In UNIX and similar operating systems, only the "root" user account had full system privileges. All other users held lesser degrees of privilege, and were assigned access to files and resources based on their username and/or group membership. Access required authentication with a username and password that was typically assigned by the system administrator not the user [12]

Management of Passwords Security

As many as 81% of hacking-related breaches over the last year leveraged stolen or weak passwords, according to Verizon's *2017 Data Breach Investigations Report.* Also, according to *Ovum's 2017 report,* 23% of employees are using social media credentials to sign in to business systems and applications in the workplace. Popular apps such as Google, Dropbox, Evernote and so on. People store or share sensitive company data on these apps. But when they are poorly managed pose a threat.

Going by the *Intel World Password Day Survey 2016* [3], an average business user keeps track of 27 passwords to remember. However, marketers, systems administrators, sales representatives manage several accounts. Beyond the enterprise-level apps, individual employees have dozens more. Furthermore, *Psychology of the Password 2016 Report* estimates that the average 250-employee size company would now have some 47,750 passwords in use across their entire organization. Businesses are currently experiencing password proliferation and failing to manage them securely can have dire consequences. Single Sign-On (SS0) allows a user to unlock access to all other logins or applications they use at work with a single password or authentication device. An SSO solution, in comparison, allows IT to reduce the number of passwords in use across the organization, but requires more investment of IT time and resources to execute.

A password manager, a new approach to password security benefits employees, IT departments, and the company by building faster and creating better solution. It helps IT personnel identify and prioritize the services that should be managed and deployed through an SSO solution, without preventing employees from using their apps of choice in

the meantime. Also, it helps by randomizing every password for every account, applying role-based permissions to passwords and adding protection with multi-factor authentication wherever possible.

Password sharing is common. In the workplace, though, sharing of credentials and other sensitive data is also an essential part of getting the job done but in turn creates *loopholes* for illegal access to applications and sensitive data-files. There are some best Practices in Password Management, especially for online authentication and transactions. These techniques increase the chances of keeping online accounts secure from hackers.

i. Use a randomly generated complex and unique password -- a unique password for every online account. The password should be complex and of a greater length. A *strong password* must meet basic features. It should consist of:

- At least eight characters
- A mixture of upper and lowercase characters
- A mixture of alpha and numeric characters
- A special symbol such as + ! @ # $? % & *

ii. Enable multi-factor authentication -- helps prevent unauthorized access of online accounts and could sometimes send alert for compromised password.

iii. Change passwords regularly -- Passwords should, ideally, be changed every 60-90 days.

User Systems Authentication

Authentication is the process that attempts to establish the identity of a user and is followed by an authorization process that grants whatever privileges may be appropriate to that identity. Common examples of authentication include logging on to a workstation in a corporate network (using a username and password), withdrawing cash from a bank cash dispenser (a bank card and personal identification number, PIN), and online shopping (an email address and password) [9]. Several firms these days have moved from simple authentication, which uses only a password, to advanced authentication. Generally, advanced authentication describes two forms of authentication. First, a password: that the system user knows and employs to authenticate. Second, a token or smartcard: that works as the authentication device. P. Wood (2015) suggested implementing stronger authentication through smart USB keys and mobile phone short messaging service, SMS texts for all remote users and for all privileged users and accounts. The most common forms of card readers are the proximity and contactless readers. A typical proximity card operates at a frequency of 125kHz using embedded antenna wires. With contactless technology, a smart card is wireless, has an embedded microchip and operates at 13.56MHz. The term "smart card" is used to describe cards with integral microprocessing and read/write data storage capability. They store huge amounts of data, like access transactions, qualifications, and biometric templates. Biometric Readers—verify personal biological metrics (biometrics) of an individual. Biometrics includes fingerprint, facial image, hand geometry, handwriting, voice recognition and iris patterns. While a password, a passphrase, an encryption key, a multi-factor token are all subject to compromise when transmitted over the internet, on the other hand, a thumbprint or a retina scan is more secure [13].

Security Awareness Program

Everyone has a role in protecting the organization and their own job functions. A program aimed at training employees to help them make smarter security decisions within an organization, and also to improve the organization's security posture and mitigate risk. The program assists the enterprise with the education, monitoring, and ongoing maintenance of security awareness within the organization.

According to Verizon's *2017 Data Breach Investigations Report*, as many as 81% of

hacking-related breaches over the last year leveraged stolen or weak passwords.
According to a research done by Computing Technology Industry Association, CompTIA – 96% of those surveyed recommended user training, due to the raising rate of breaches resulting from user error [2]. Providing employees with effective training will enable them to become better cyber security partners.

M. Drolet (2018) reviewed that employees are the weakest link in your cyber defenses, due to their vulnerability and possible mistakes. Sometimes they lack understanding of compliance requirements and sensitive data handling. Yet, they can be a huge asset to any security team if they are given the right tools and trained properly.

From a business perspective, Zink, Lauren, 2017 enlightened that Security awareness requires managing people, groups and projects and creating a plan to disseminate pertinent information to employees who all need to understand that they are stakeholders when it comes to the security of the company and its people. It involves equipping your employees with the knowledge they need to spot the threats and take appropriate action that aligns with your company policies. .

Give extra security training to security guards, helpdesk staff, receptionists and telephone operators, all of whom have a vital role to play in blocking identity theft [9]. Establishing and maintaining security awareness through a security awareness program is vital to an organization's progress and success.
Training goals for staff awareness program should be to [1]:

- Build human firewalls
- Reduce insider threats from employees
- Enable easy access while protecting the network and organization
- Measure effectiveness of program.
- Regular reporting and continue to find ways to communicate security awareness.

For meaningful security awareness training programs, enterprises have to assess company needs, develop content, schedule and deliver training, and also test and track the impacts of the training.

III. Methodology

The Data presented in this study were based on surveys conducted by National Statistical Authorities on 'ICT Usage and eCommerce in Enterprises' in 2010. Thus, data source is from secondary data. The survey covered various sectors operating within the EU.
The total number of enterprises of the European Union 27, EU27 member states (without Estonia) formed the population of the study. Available record put the total strength at 1.6 million in the EU27 (K. Giannakour, and M. Smihily, 2011). The Sample size surveyed for the study was 149 900 enterprises having adopted simple random technique.
Data collected from the study was classified into different groups with the aid of tables. The Analysis of Variance (ANOVA) was used to test the hypotheses.

IV. Data Presentation And Analysis

The data obtained from the study are presented below. The data in Table 1 shows the percentage of enterprises that adopted Staff security awareness and password/user authentication respectively and the percentage of ICT security-related incidents admitted in each member state of the EU in 2010.

Table 1
Data of EU-27 Enterprises (%age of Enterprises)

EUROPEAN COUNTRIES EU-27	ICT SECURITY INCIDENTS	STAFF TRAINING/ SECURITY AWARENESS	STRONG PASSWORD AUTHENTICATION /USER IDENTIFICATION

	ICT	SA	SP
Belgium	15	52	52
Bulgaria	10	41	33
Czech Republic	26	54	40
Denmark	29	56	56
Germany	11	50	46
Ireland	20	64	64
Greece	29	52	33
Spain	26	50	63
France	9	29	33
Italy	19	67	66
Cyprus	29	84	43
Latvia	10	58	42
Lithuania	22	65	42
Luxembourg	12	36	62
Hungary	5	25	24
Malta	18	43	52
Netherlands	22	33	53
Austria	10	44	39
Poland	10	18	53
Portugal	40	57	55
Romania	19	53	29
Slovenia	9	62	64
Slovakia	20	53	20
Finland	28	80	53
Sweden	19	65	58
United Kingdom	6	48	53

Source: Eurostat (http://ec.europa.eu/eurostat/product?mode=view&code=isoc_cisce_ra)

Calculation is based on the aggregates statistics of each European member state. The size of employee ranges from large enterprises of 250 persons and above to small enterprises, with at least ten persons employed.

4.1 *ICT Security-Related Incidents*

This section of the study evaluated the factors associated with ICT-related security incidents reported by employees. From the analysis, we found that there were considerable variations in incidents among the member states represented in the study. Table 4.1 column 2 shows the percentage, % of enterprises that have experienced at least one of the following ICT incidents:

(a) Enterprises have experienced ICT related incidents that resulted in unavailability of ICT services, destruction or corruption of data due to hardware or software failures

(b) Enterprises have experienced ICT related incidents that resulted in unavailability of ICT services due to attacks from outside e.g. denial of service attack

(c) Enterprises have experienced ICT related incidents that resulted in destruction or corruption of data due to infection or malicious software or unauthorized access

(d) Enterprises have experienced ICT related incidents that resulted in disclosure of confidential data due to intrusion.

Figure 1 presents the aggregate comparative analysis of the study's two independent variables of password authentication and staff training factors as adopted by enterprises.

Figure 1: Comparison between Strong Password

authentication, SP and Staff Awareness training, SA (% of enterprises that deployed each solution).

From the pie chart in Fig. 1, staff training witnessed fifty-two percent (52%) adoption than those who practiced the use of strong password authentication (48%) and other identification methods such as smart cards put together. Effective controls of these incidents formed the core elements of Information Security, which are— integrity, confidentiality and availability of data and IT systems.

4.2 *Password Authentication/User Identification*

Identification refers to the ability to identify and distinguish between individual users. User ID, an authentication procedure is considered as common practice in many business enterprises today.

Table 1 column 4 shows percentage of Enterprises that have used strong password authentication or user identification and authentication via hardware tokens, by economic activity of each sector.

4.3 *Staff Training/Security Awareness*

Enterprises adopt various approaches aimed at raising staff awareness of ICT security policy and the relevant risks in relation to their ICT-related security obligations.

From Table 4.1 column 3 displays the percentage of Enterprises which have adopted any approach to make staff aware of their obligations in relation to ICT security, by economic activity.

4.4. **Test of Hypothesis**

The hypothesis was formulated to test the validity of the study. The data used for the testing of the hypothesis was derived from data questionnaire dispersed to the respondents in sectors across all economic activities as presented in Table 4.1.

H_o: The implementation of both password authentication/user ID and staff security awareness training do not offer significant protection against ICT security-related incidents.

H_A: The implementation of both password authentication/user ID and staff security awareness training offer significant protection against ICT security-related incidents.

Table 2: Analysis of Variance (ANOVA)

Source Of Variation	Degrees Of Freedom (Df)	Sum Of Squares (SS)	Mean Square (MS)	Variance Ratio (F-Ratio)
Regression	k = 1	SSR = 553.72	MSR = 553.72	F = 1.331
Error (Residual)	n– k = 24	SSE = 9,993.3	MSE = 416.39	
Total	n – 1 = 25	SST = 10,547		

Source: https://onlinecourses.science.psu.edu/stat501/node/295

To perform the test of significance, we use F-Test statistics.

$$\text{F-computed, } F^{*} = \frac{\text{MSR}}{\text{MSE}} = \frac{553.72}{416.39} = 1.331$$

Since F-computed, F^{*} (1.331) < F-critical, F_c (3.42)

We accept the Null Hypothesis, H_0 at the significance level (5%), the hypothesis test showed that from the F – statistical test, the observed F-critical (3.42) was greater than calculated F-computed (1.331) at 0.05 level of significance.

We accept the null hypothesis, H_0, which states that implementing both password authentication/user ID and staff security awareness training does not offer significant protection from ICT security-related incidents in enterprises. The co-efficient of determination, R^2 (adj) was 5.25 percent. Therefore, we conclude that the two security approaches have no significant effect on data destruction or corruption in enterprise networks.

4.5 **Discussion of Results**

The findings revealed that the extent of the two security solutions (the password authentication/user ID and staff security awareness training together) had non-significant positive impacts in determining the availability of ICT services and protection of data in companies. This implied that their combined effort in preventing loss and data corruption was not statistically significant. Our interest is on the magnitude of the impact of the selected security methods used on the problem of unavailability of ICT services in enterprises.

The study revealed that most employees relied mainly on the use of passwords for validating their identities. However, a few others in the

corporate world employ complex passwords as their own form of top security. Moreover, some security conscious IT professionals did stepped-up by installing hardware detection tools for use with smart cards, in order to provide extra level of authentication. Even that is not adequate in withstanding any security violations in public networks or stand-alone computer systems.

P.Wood (2015) recognized passwords as the common means of authentication. Unfortunately, most users do not know how to construct a secure password, nor understand the risks involved. Also, he recognized the fact that employees often use the same password in several different situations. Thus, anyone who steals the identity of a specific user becomes the user and has access to her system and sensitive corporate data. In discussing the weakness of passwords, LastPass' 2016 report stated that several companies admitted being faced with today's reality of password proliferation across their entire organization, but identified most as weak and reused.

The study also recognized strict compliance to corporate policies for effective defence. In the workplace, a common practice is for staff from all departments to Share credentials with vendors, partners, clients, and others. However, they must ensure uniqueness and privacy of each of those passwords to curtail social engineering attacks.

Businesses must advocate for proper training of their workers to Establish and maintain security awareness. Through Security awareness programs, C. Moore (2017) noted that people become aware of the importance of protecting the internal network and data and how to handle all securely organization's progress and success.

Y. E. Yildirim, (2018) agrees that, for a comprehensive security of user-systems in view of business threats, enterprises must incorporate additional tasks in their ecosystems that include security technology controls without ignoring organizational issues that drive information security risks. With the growing cyber threats that is constantly changing IT security landscape, businesses are waking up in discovering that end-users PCs are known sources of all kinds of invasion into the network architecture, and hence the need for their maximum protection.

V. Conclusion and Recommendations

Information Technology has been a force behind the advancement of several industries, and these advancements in technology would require further increase in the security apparatus of enterprises. All hands must be on deck to embrace preventive measures within the corporate world.

On the basis of the findings of this study, the following recommendations are made to facilitate the efficient protection of user systems operating within the enterprise network environments.

- The management and policy makers should be properly guided in finding far reaching solutions to IT-related security breaches in the corporation.
- Information security administrators need to belong to some security networks groups, forum or societies for more enlightenment and notification about current trends and practices in the world of information technology.

- There is need for allocation of special funds to IT units annually or quarterly for the purchase of security facilities and periodic conduct of staff awareness training sessions.
- Other security tools - internal and external should be deployed including secure firewall services, routers, secure clients and servers systems, and third-party security applications and services.

Further research will be required to extend the theoretical foundation of this work by identifying more security-related attributes and techniques that can address completely ICT issues indicated earlier.

Acknowledgement

V. U. Achunike thanks the management of the Institut Bilingue libre Du Togo, Lome for their support. V. U. Achunike also acknowledges the contribution of the European Statistical Data team.

References

[1] C. Moore "Implementing a security awareness program – creating security conscious employees," Prince George's County Memorial Library System, UK, December 8, 2017.

[2] D. Lohrmann, "Reducing risk through next-gen cyber awareness training**"** CSO State of Michigan, Produced by The Security Confab, at La Jolla, California, pp4, April 15-17, 2012.

[3] J. Bernstein, "People have way too many passwords to remember" Intel World Password Day Survey 2016, Intel, USA.

[4] L. Zink, "How to tailor security awareness training to employees' need," Security magazine BNP Media, Skokie, Illinois, IL, US., Nov. 2017.

[5] M. Drolet, "Infosec at your service: 4 steps to launch a security awareness training program," CDG Technologies, contributor Network, Boston, 2108.

[6] N. C. Ozigbo, "The adoption of information and communication technologies in the management of Nigerian oil and gas industry," International Journal of Humanities Social Sciences and Education (IJHSSE) Volume 1, Issue 7, July 2014, pp 179-190.

[7] Ovum "Close the password security gap: convenience for employees and control for IT" report, LastPass, LogMeIn, Inc, 2017.

[8] Psychology of the Password 2016 Report, "Password exposé: 8 truths about the threats and opportunities of employee passwords, LastPass, LogMeIn, Inc, 2016.

[9] P. Wood, "How To ensure Strong Password And Better Authentication" First Base Technologies LLP, Brighton, UK, Oct. 2015.

[10] STAT 501 "Regression methods lesson 6.2 - the general linear F-Test,"

https://onlinecourses.science.psu.edu/stat501/node/295, PennState Eberly College Of Science, The Pennsylvania State University. Aug. 2018.

[11] Verizon's Data Breach Investigations Report, 2017, Verizon enterprise.

[12] White Paper "Why your business needs enterprise-strength password management" Keeper Security, Inc., Suite 500,Chicago, IL., 2017.

[13] Y. E. Yeniman, "The importance of risk management in information security," Uludag University, Computer Technologies Department, Research gate publisher, Turkey, 31 May 2018.

[14] K. Giannakour, and M. Smihily, "ICT security in enterprises" Statistics In Focus, Eurostat, National Statistical Authorities, ISSN 1977-0316, Luxembourg, Feb. 2011.

SURVEY OF INTELLECTUAL CAPITAL MODELS, STRENGTHS AND WEAKNESSES (C013)

O. E. Afolabi
Department of Computer Sciences,
University of Lagos, Nigeria
afolabiolamiposi@yahoo.com

O.B Okunoye
Department of Computer Sciences,
University of Lagos, Nigeria
bokunoye@unilag.edu.ng

Abstract— The Market Value (MV) of any organization does not only depends on the Book Value (BV), but also on the Intellectual Capital (IC) of such organization. Intellectual Capital(IC) can simply be defined as the intangible assets of an organization, i.e. any asset that is not directly recorded in financial statements of the organization. Unlike book value which is recorded in the financial statement of any organization, the intellectual capital is not usually measured. Many researchers have come up with different methods in which IC can be measure, but up till now, there is no generally acceptable or agreed method of which intellectual capital can be measure. This paper presents different methods, their strengths and weaknesses and evaluation.

Keywords: Intellectual Capital (IC), Direct Method, Return on Assets, Market Capitalization, Scored Card

1.0.

I. INTRODUCTION

Intellectual capital has been described as "the intellectual material – knowledge, information, intellectual property, experience that can be put to use to create wealth" [1]. Though organizations pay little or no attention on intellectual capital, intellectual capital has always been a major part of market value. The book value can be gotten from financial record, but intelletual capital is not always valued. One of the major challenges faced by the concept of intellectual capital is the method of measuring it.

Different researchers such as [2] and [3] have identified different methods in which IC can be measured. According to [2], methods of measuring IC can be grouped into two general methods. These two general methods are: **Component-by-Component Evaluation** and **Measuring the value of Intellectual Assets in Financial Terms**. The component-by-component evaluation method uses appropriate units of measurement for each component. The components include the value of patents, market share, and the number of work-related competencies, each with its own unique unit measure and usefulness at different level of an organization. However, all of these measures, no matter what level they are being used and their unit of measurement, they must all work together in harmony to achieve one purpose, so this method can be said to be effective. The second general method, measures the value of intellectual assets in financial terms at the organization level without referring to any component of IC.

Shareholder value is a key indicator in today's economy of how effectively managers employ intellectual and other assets. Therefore, measures expressed in financial terms that take into account the harmonious effect of intellectual assets at the organization level provide a key measure of progress and value. In addition, different measures have different relevance and usefulness at different levels in an organization.

Other researchers have also identified various methods in which IC can be measured and these methods have been grouped into four major categories which are Market Capitalization Methods (MCM), Return on Assets Methods (ROA), Direct Intellectual Capital Methods (DICM), and Scorecard Methods (SC) [3].

II. Methods of Measuring Intellectual Capital

As stated earlier, researchers have grouped different methods of which intellectual capital can be measure into four categories, each of these categories has its own strengthens and weaknesses, this section describes these methods and their individual strengthens and weaknesses.

A. Market Capitalization Methods (MCM)

According to [14], the methods under MCM determine the difference between the market capitalization of an organization and its liquid patrimony as the value of its intellectual capital or intangible asset. One major characteristic of IC methods under market capitalization is that, all the methods use capital market values to estimate

the aggregate value of IC based on the assumption that capital market provides a useful estimation of the aggregate value of IC. The following are some of the sub-methods under MCM:

i. Market – to – Book Value

This method measures the present worth of a given company, in comparison with the amount of capital invested by current and past shareholders into it. According to [1], this method is based on the assumption that "the increase in market value of an entity (the value of shares of shareholders) to its book value is represented in the intellectual capital of the entity. This means, intellectual capital is expressed as a cash residual values." This method assumes that a company's approximate worth (i.e. the summation of tangible assets and intangible assets) can be reflected by its market value. Market value is the market price per share of common stock multiplied by the number of shares outstanding.

- **Strength:** it expresses intellectual capital as a cash residual values
- **Weakness:** The only limitation of this method is it does not consider the total difference (i.e. it ignores part) between the market value and book value. Therefore, the result of the difference between book value as reflected on the company's balance sheet and market value only gives an approximate measure of the intellectual capital; which also contributes to the company's total worth and does not show on the balance sheet [2].

ii. Tobin's Q

Initially Tobin's Q was not meant for measuring the intellectual capital, it was developed to help predict the investment decisions for the organization. The **Q** signifies the ratio of market value of the organization to the replacement cost of the assets. Tobin's Q is calculated by adding accumulated depreciation to the book value of a company, and then do the necessary and appropriate adjustments for price changes in different classes of assets from the time of purchase. This method was developed by James Tobin, a Nobel prizewinning economist [2]. This shows the impact of investments in human capital and information technology. The positive value of ratio Q is the intellectual capital [3].

According to James Tobin, the combined market value of all the companies on the stock market should be about equal to their replacement costs. That is, the ratio of all the combined stock market valuations to the combined replacement costs should be around one. Mathematically, Tobin's Q is calculated as:

$$Tobin's\ Q = \frac{\text{Total Market value + Liabilities}}{\text{Replacement value + Liabilitie}} \text{..... i}$$

In a competitive market, if the value of q of certain company is greater than 1 and greater than competitors' value of q, then it means the company has something intangible that cannot be physically measure from the financial records, which give that company an upper hand to produce higher profits than other similar companies [2].

It is worth noting that, "if the proportion (i.e., the Tobin Q) is less than one, then the market asset value is less than the replacement value (Book value), it means the company may be under valuing.

On the other hand, if the Tobin Q is greater than one, then the market value is greater than the replacement cost (company may be overvaluing), and thus it is improbable that the company will buy more assets of this type; however, if the ratio Q is greater than one, the company will invest in similar assets, which are worth more than the cost of their replacement [4].

Strength: it eliminates the effect of the different consumption policies, which vary from one company to another and from one country to another, which considered more meaningful when comparing companies over a period of time [3]. More so, this method is more accurate than the market-to-book method because it uses replacement, rather than historic, costs.

Weakness: it is more tedious to find replacement costs than simply referring to a balance sheet. It cannot provide an accurate figure for individual intellectual assets and its real value lies in trend analysis.

iii. Financial Method of Intangible Assets Measuring (FIMIAM):

The monetary value of the intellectual capital of any company is calculate with this method, on the basis that the difference between the market value and book value is equal to the intellectual capital. FIMLAM method provides information on intellectual capital for companies and allows them make decisions. However, it limitation is in finding the difference between the market value and book value, which is the achieved intellectual capital and which differs from the real intellectual capital. So, the processes involved in defining the achieved intellectual capital according to this method is unclear. In particular, with regard to the identification parameters for each component of the three components of the intellectual capital, and also the difference between the real intellectual capital and the achieved intellectual capital which expressed as defunct Capital cannot be calculated [3].

Strength: It provides necessary information on intellectual capital for companies in order to make good decisions

Weakness: It only find the difference between the market value and book value, which is the achieved intellectual capital and which differs from the real intellectual capital.

iv. General Strengths and Weaknesses of MCM

Below are some strengths and limitations of MCM

Strengths:

- MC methods provide little details which enhance crude comparisons between companies within the same industry.
- Because of the accuracy in the comparison between companies of the same industry, MCM gives real valuations which may be useful in many situations.
- In the book value method affiliated to (MC) method, it is a simple method. This indicator can be easily computed for the companies listed on the stock market.
- In the Tobin's Q method affiliated to (MC) method the positive value of ratio Q refers to the intellectual capital, which is not shown by traditional accounting systems, this advantage of this method eliminate the effect of the different consumption policies.

Weaknesses:

- MC methods do not give enough detail for adequate comparison.
- They are weakest measurement methods where market varies can lead to big changes in intellectual capital and lead to highly suspicious indicators.
- In The Tobin's Q method affiliated to (MC) method, the method uses replacement cost of tangible assets, in place of their book value.
- There are many difficulties with the market-to-book ratio that are neutralized.
- Market-to-Book value &Tobin's (Q); there is no very significant practical usefulness for the company management.

B. Return on Assets Methods (ROA)

This method takes company's average profit before deducting tax, it is then divided by the average value of tangible assets; which gives the "Return on Assets (ROA)". This result is then compared with the average of the industry and the difference is multiplied by the average of tangible assets. The result of this product is equal to the annual average income of the Intangible. Division of the remuneration earned above the average cost of the company capital or interest rate, can be used to calculate an estimated value of its intangible assets or intellectual capital [3]. ROA measures IC by calculating the average earnings of a company before tax deduction divided by the average tangible assets. The result is a company's ROA that is then compared with its industry average [5]. The following are some of the sub-methods under Return on Assets Method:

i. Calculated Intangible Value (CIV)

Calculated Intangible Value (CIV) method was developed to estimate or calculate the value of the intellectual capital of a company, based on the assumption that the company's profits are higher than the industry average profit [3]. CIV determines the currency value of intangible assets. It compares the performance of a company with an average business competitor of the same tangible assets to determine the value of intangible assets [6]. Process of CIV consists of six steps:

- Calculate company's average profits before deduction of taxed for the past three years.
- Calculating the average of company's tangible assets from the balance sheet for the past three years.
- Divide company's pretax profits on the average tangible assets, to get the return on company's assets.

$$\text{ROA} = \frac{Average\ profit\ before\ deduction\ of\ tax}{\text{the average value of tangible asset}} \ldots\ldots\ldots ii$$

- At this stage, check if the company's return on tangible assets for the past three years is higher than the industry's return on the tangible assets, if it higher; follow and complete the remaining steps. If it is less or equal zero, stop. This means there is not intellectual capital for the company.
- Calculate excess return on assets by multiplying the industry average ROA by the company's average tangible assets, and then multiply the result by the tax rate to get the increase in return after tax.
- Calculating the value of intellectual capital, by dividing the increase in the ROA by the capital cost.
-

$$IC = \frac{\text{Increase in the ROA}}{\text{Average of capital cost}} \ldots\ldots\ldots iii$$

ii. Economic Value Added (EVA):

EVA be described as a method used to determine the difference between net operating profit and an appropriate burden for the opportunity cost of the total capital invested in the company. It was developed by Shorn Steward. it calculates company's financial performance based on the residual wealth calculated by deducting capital cost from its operating profit, adjusted for taxes on a cash basis.

It is the amount that increases the profit or decreases from the first rate return which is possible to get it by shareholders and lenders to invest in other paper Securities with approximating risks [3].

A company's EVA is made of three key components, which are NOPAT, the amount of capital invested and the WACC. So, EVA can be calculated with equation below:

$$EVA = (\text{RI}) + (\text{AcAdj}) \dots\dots\dots \text{iv}$$

and:

$$RI = (NOPAT) - (Cap\ Chg) \dots\dots\dots v$$
$$NOPAT = (EBEI) + (ATInt) \dots\dots\dots vi$$
$$EBEI = (CFO) + Accurals \dots\dots\dots vii$$
$$ATInt = NIEx(1 - Tax\ Rate) \dots\dots\dots viii$$

Where:

RI = Residual Income

AcAdj = Accounting Adjustments

NOPAT = Net Operating Profits After Taxes

Cap Chg = Capital Charge

EBEI = Earnings Before Extraordinary Item

ATInt = After Tax Interest

CFO = Cash Flow from Operations

NIE = Net Interest Expense

EVA = Economic Value Added,

NOPAT = Net Operating After Taxes -which can be calculated manually or found in the company's financials.

IC = Invested Capital -amount of money used for execution of a specific project

WACC = Weighted Average Cost of Capital -average rate of return a company expects to pay its investors. Usually found in the public record, but can also be calculated.

The purpose of EVA is to measure the charge (i.e. the minimum return that investors require to make their investment worthwhile) or cost, for investing capital into a certain project, and then assess whether it is generating enough cash to be considered a good investment. If the company's EVA is positive value, it means the project is generating value from the funds invested. But if it's negative, it means the company is not generating value from the funds invested into the project [7].

iii. Value Added Intellectual Capital Coefficient (VAIC)

VAIC method can be referred to as a performance measurement which is suitable to meet the requirement of modern economy, as well as capable of measuring the effectiveness of key resources in the enterprise. It concept of value added as the measure of performance, relative to intellectual capital [8].

The Austrian founder of the Intellectual Capital Research Centre, [5], developed Value Added Intellectual Capital Coefficient to measure the effectiveness of resources in an organization. Pulic also used this method to measure the efficiency of regions in Croatia. It is very important to note that, VAIC does not actually measure intellectual capital itself, but it measures it impact or extent on the management [3], [8], [9].

iv. Components of VAIC

Pulic also identified two key resources that create value-added in organizations, the resources are: **Capital Employed Efficiency (CEE) and Intellectual Capital Efficiency (ICE)**. Capital employed is further broken into two components which are **Physical Capital Efficiency (PCE) and Financial Capital Efficiency (FCE)**. Intellectual Capital on the hand is sub-divide into **Human Capital Efficiency (HCE) and Structural Capital Efficiency (SCE).** [5],[8],[3]. So, to calculate the final measure with VAIC, some other variable variables and coefficients need to be calculated. To get value for VAIC, the following steps are involved:

Step1: Calculate Value Added $VA = OP + EC + D + A$

Step2: Calculate Intellectual Capital $IC = EC + SC$

Step3: Calculate Human Capital Efficiency $HCE = \frac{VA}{HC}$

Step4: Calculate Structural Capital Efficiency $SCE = \frac{SC}{VA}$

Step5: Calculate Intellectual Capital Efficiency $ICE = \frac{HCE}{SCE}$

Step6: Calculate Capital Employed Efficiency $CEE = \frac{VA}{CE}$

Step7: Calculate Value Added Intellectual Coefficient $VAIC = ICE + CEE$

Where: OP = Operating Profit; EC = Employee Costs; D = Depreciation; A = Amortization SC = Structural Capital; HC = Human Capital; CE = Book value of net assets.

Note:

$$SC = VA - HC \dots\dots\dots ix$$

$VAIC = ICE + CEE \dots\dots\dots x$ or

$VAIC = CEE + HCE + SCE \dots\dots\dots xi$

In the field of Intellectual capital measurement, VAIC method has been proven to be one of most efficient methods. VAIC is a transparent method, simple and easy to use. VAIC is known to be an objective method, because the data (which are reliable and verifiable) used for calculations are derived directly from the financial

statements, which enables one to easily compare companies. VAIC has also be used in statistical analysis successfully. This method can also be applied in business practice and in research. Despite its advantages, VAIC also has some adversities, which include: how to calculate the value-added, as well as the components used to determine human capital. This can lead to inconsistences of the results [5].

v. General Strengths and Weaknesses of ROA

Below are some strengths and limitations of ROA

Strengths:

- VAIC is a simple and easy to use in determining the value of IC and gives an important information to managers, investors, and governments.
- VAIC can be successfully used for statistical analysis.
- Because ROA methods can do crude comparisons between companies within the same industry, they are used for real valuations which may be useful in many situations.
- ROA methods are very sensitive to interest rate assumptions.
- They are not used for non-profit organizations.
- They can be used determination of investment opportunities through Economic Feasibility Studies.
- VAIC is a simple and straight forward method for determining the value of IC and gives an important information to managers, investors, and governments.

Weaknesses:

- ROA methods are not really intellectual capital methods except VAIC, they are simple ways of explaining a financial feature and attributing changes in them to the efficiency in the deployment of intellectual capital resources.
- They do not provide enough detail for adequate comparison.
- The methods are also very sensitive to interest rate assumptions.
- These methods avoid direct comparison with market values.
- ROI method except for (VAIC) fails as a measuring system due to internal difficulties and the defined resources independence [3].

C. Scorecard Methods (SC)

In this method, the generated indicator and indexes of various components of the intangible assets or intellectual capital identified are compared in the scorecards.

i. Balanced Scorecard (BSC)

Balance Scorecard (BSC) can simply be described as an organized planning and management system used by organizations to clearly state their purpose or what they are trying to accomplish, systematically set individual daily activities, prioritize projects, products, and services and effectively monitor and measure the progress towards they are making towards achieving the stated purpose [10].

BSC can also be referred to as an organized way of measuring and monitoring the effectiveness of an organization's implementation of its process towards achieving it stated goals [11]. BSC was developed by Dr. Robert Kaplan and Dr. David Norton in the 1990s with the aim to create an integrated vision for Measuring Systems.

BSC Four Perspectives

With BSC, an organization's performance can be viewed from four perspectives:

a. **Financial/**Stewardship: views financial performance and the effective use of financial resources of an organization.
b. **Customer/Stakeholder:** views customer value, satisfaction and/or retention
c. **Internal Process:** views the efficiency and quality of organization's product or services and any other key business processes
d. **Organizational Capacity/ Learning and Growth:** views human capital, infrastructure, technology, culture and other capacities that have enhanced organization performance [3], [10].

BSCs can be used worldwide in various sectors such as government, business and industry, and nonprofit organization. It provides a comprehensive strategy for evaluating activities related to the generation of value through tangible and intangible resources [3]. However, BSC specific enough in view of their generic nature to serve as an adequately funded model [12].

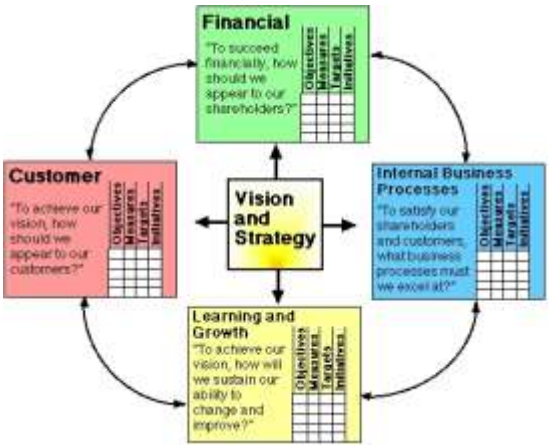

Figure 1: Balanced Scorecard by [19]

ii. Skandia Navigator

Skandia Navigator is one the best methods of measuring intellectual capital [12]. It was developed by Skandia Sweden Company in the field of financial services and insurance. The output of this method is the Intellectual Capital Report. The model was designed to give a balanced view for the intellectual capital and financial capital of the organization. The model presents a balanced and completed view of an organization's operations, by focusing on five dimensions in the organization which are: Customers, Processes, Human, Research, development & Financial. Each of these dimensions is attached with a set of indicators. The indicators can be financial on non-financial [3]. "The value of intellectual capital is determined by the Skandia Market Value Scheme, which places the market value within a hierarchical structure" [12].

iii. Intangible Asset Monitor (IAM):

Intangible Asset Monitor (IAM) is a non-financial scorecard system that is based on the knowledge of an organization to measure the intangible asset – "an additional demonstration of a company's financial success and its shareholder value" [12]. This method was developed by [11], when working as financial manager in one of the biggest companies. It measures intangible assets and presents different indicators; the choice of which depends on the company's strategy, to simply measure the intangible assets. IAM can be embedded in a management information system [13].

[6], described IAM as management tool used by organizations monitor and measure the value of their intangible assets, especially for calculating the difference between market and book value. IAM is based on the assumption that people are the true agents and the main source of profit of any business or organization.

IAM grouped the intangible assets of a company's balance sheet into three structures:

a. External structure: this shows the relationship between a company and its customers and suppliers, brand names, trademarks, and reputation.
b. Internal structure: shows a company's organizational assets, such as processes, concepts, systems, patents, etc.
c. Individual competence: this is an employee's ability to function in different situations, e.g. skills, experiences, etc.

Human efforts are converted into both tangible and intangible knowledge structures and the structures can either be external structures or internal structures, and they are all refer to assets because of their effect on the organization's revenue streams [6].

iv. General Strengths and Weaknesses of Scored Card Methods

Below are some strengths and limitations of ROA

Strengths**:**

- SC methods have the ability to create a clearer picture than both of methods (MCM) and (ROA) than financial metrics.
- They are faster and give more accurate measurement than (ROA) and (MCM) methods with respect to the resources.
- These methods are very useful to non-profit organizations.
- Give detailed report and easier to apply at any level of an organization.
- Because these methods use software solutions, it enhances the collection and processing of data.
- Enable managers to have a better understand of company's strategy and their mission.

Weaknesses:

The meaning of resource might differ to each organization and to each purpose, this makes comparisons not easy that cannot be easily connected to pending financial results always been a weakness of the intellectual capital movement.

D. Direct Intellectual Capital Methods (DICM)

This method calculates the value of intangible assets by first identify the components, and evaluate the components either individually or as an aggregated coefficient [5]. With the methods under DICM, the value of intangible assets can be measured and evaluated, when all it components are identified. This method calculates monetary value of intellectual capital by identifying its various components and attach monetary value to each component. The evaluation of the components can be done individually or as an aggregated coefficient and these also assign currency value (dollar value) or monetary value to the intangible asset [14]. The following are some of the method under DICM

i. Technology Broker method

According to [15], Technology Broker method estimates the coin value of intangible assets by first identifying each component, and immediately evaluate the components, either individually or as an aggregated coefficient. More so, [16] in his research said that Technology Broker evaluate the value of Intellectual Capital based on diagnostic analysis of a firm's response to some certain questions across the four major components of IC.

Brooking divided intellectual capital assets into four major categories which are **intellectual property assets, human-centred assets, market assets, and infrastructure assets**. She described intellectual property assets as legal rights to protect many corporate assets. This type of assets includes trade secrets, copyright, patent and many other legal rights. She saw market assets as assets obtained by a firm through beneficial relationships with its market and customers. Examples of such assets include favourable licensing, brands, reputation, and distribution channels. More so, Brooking described human centred assets as assets which incorporate the collective efforts, expertise, creative and problem solving capabilities, leadership, entrepreneurial and managerial skills possessed by employees. She argued that human assets can be increased by allowing employees to have access to mechanisms that would enable them to achieve their full potential. Finally, she described infrastructure assets as methodologies, processes, and technologies used to facilitate the operation. The assets include information systems, corporate culture, financial systems, risk management, sales management, and communication systems.

ii. Citation weighted patent

This method deals with the measurement of patent impact on an organization based on technology factors. It calculates intellectual capital's performance derived from researches on different indices. In his book [17], described this method as the factor of technology that is calculated based on patents developed by a firm. According to [16], the technology factor is calculated based on the patents developed by a firm, while the intellectual capital and its performance is measured based on the impact of research development efforts on a series of indices. Such as number of patents and cost of patents to sales turnover, that describe the firm's patents.

The author in [18], said that "Weighted patent citation can be calculated by counting the number of times each patent has been cited in the subsequent patents and using the resulting number to compute the weighted patent". According to him, the number of times a patent would be cited subsequently in the patent documents might be an indication of its technological significance or economic success. Meanwhile, research has shown the relationship between citation weighted patents and value creation. Patent citations have some important information on the market value of the firm. If an increase in quality of patents leads to one additional citation, then, the market value of the firm would increase by at least 3% on average, which is the stock market reaction to the firm's.

iii. The Value Explorer

This is an accounting methodology proposed by KMPG in order to calculate and allocate value to five different kinds of intangibles assets, which are assets and endowments, skills & implicit, the rules of collective values, technology and explicit knowledge, and major and management processes.

iv. Intellectual Asset Valuation:

This method simply calculates the value of Intellectual Property **such as** patent rights. The property rights may be a source of income.

v. Strengths and Weaknesses of DICM

Strengths:

- DICM can create a clearer picture than both (MCM) and (ROA) than financial metrics.
- Gives more detailed and accurate result.
- DICM is easy apply at any level of an organization
- Faster and more accurate than (ROA) and (MCM) methods with respect to the resource.
- They are very useful for non -profit organizations and do not need to be measured in financial terms

Weaknesses:

- DICM cannot be connected easily to financial statements results.
- The meaning of resource might differ to each organization and to each purpose, this makes comparisons difficult.

vi. Evaluation of Methods of Measuring Intellectual Capital

The Table 1 shows evaluation of the four broad methods for measuring IC

Table 1. Evaluation of Method of Measuring Intellectual Capital (Source: [3], [20], [21])

Metrics/Method	MCM	ROA	SC	DIC
Detail analysis	Provides far too little detail i.e. it does not give room for adequate comparison.	Provides far too little details i.e. it does not give room for adequate comparison.	Provides more accurate details and offers clearer picture than both of methods (MCM) & (ROA)	Provides more and accurate details and offers clearer picture than both of methods (MCM) and (ROA
Simplicity	The book value method affiliated to (MC) method, is a simple method	Simple and easy to use	Easy to use, faster and more accurate than (ROA)and (MCM)	Easy to use, faster and more accurate than (ROA)and (MCM)
Application	It has is no significant practical usefulness for the company management	Not applicable to non-profit organizations	Very useful for non-profit organizations. And it can be applied at any level of an organization and also gives managers a better understand of company's strategy and their mission.	Very useful for non-profit organizations. More so, it can be applied at any level of an organization
Comparison with market values and book value	It uses replacement cost of tangible assets instead of their book value	It avoids direct comparison with market values.	Because the meaning of resource might be different to each organization and to each purpose , so comparisons becomes difficult	Because the meaning of resource might be different to each organization and to each purpose , so comparisons becomes difficult
Calculation of IC	It is a weakest measurement for intellectual capital especially where market varies, which can lead to highly suspicious indicators. More so, in order to accurately calculate the value of intellectual capital, this method must be adjusted to substitutive cost.	Except for VAIC, ROA methods do not really calculate IC, but rather; are simple ways of explaining a financial feature and attributing changes in them to the efficiency	It measures intellectual capital resources from the bottom up.	It measures intellectual capital resources from the bottom up.
Dependency financial metrics and accounting rules	It depends on financial metrics and accounting rules		It cannot be easily connected to pending financial results	It does not depend on financial term, so there is no need to measure financial term

E. Conclusion

- Intellectual Capital is an important aspect of any organization essential for measuring the value of the organization, but calculating IC has been a great challenge as there is standard and commonly accepted method for measuring it value. From the evaluation, it can be seen that SC and DIC have a lot of similarities. Direct method calculates the monetary value of intangible assets of a given organization by considering each component or constituent elements. The Scorecard method is similar to direct method, it also identifies each element of IC and evaluate them, the only difference between SC and DIC, unlike DIC which evaluate the monetary value of each element of intellectual capital, SC does not evaluate the monetary value of the elements, instead, it uses indicate and represent the report in a graph. ROA methods are not really intellectual capital methods except VAIC, they are just simple ways of explaining a financial feature and attributing changes in them to the efficiency in the deployment of intellectual capital resources. Meanwhile, methods under market capitalization use capital market values to estimate the aggregate value of IC based on the assumption that capital market provides a useful estimation of the aggregate value of IC. It can therefore be concluded that there is not perfect method suitable every situation, each method has it own strength and weakness. More work should be done to come up with appropriate and suitable method.

References

1 Stewart, T. (1997). *Intellectual Capital: The New Wealth of Organizations,*. New York, NY ., USA.

2 Luthy, D. H. (2013). *INTELLECTUAL CAPITAL AND ITS MEASUREMENT*. Retrieved Jully 06, 2017, from http://www.apira2013.org/past/apira1998/archives/pdfs/25.pdf

3 Mohamed, I. A. (2017). Methods of Measuring Intellectual Capital and the Efficiency of Investment. *Imperial Journal of Interdisciplinary Research (IJIR), 3*(2), 1083- 1092 . Retrieved June 30, 2017

4 Berzkalnea, I., & Zelgalvea, E. (2013). Intellectual capital and company value. *Contemporary Issues in Business, Management and Education*. doi:10.1016/j.sbspro.2013.12.934

5 Svanadze, S., & Kowalewska, M. (2015). The measurement of intellectual capital by VAIC method – example of WIG20. *Online Journal of Applied Knowledge Management, 3*(2), 36-44. Retrieved July 12, 201, from http://www.iiakm.org/ojakm/articles/2015/volume3_2/OJAKM_Volume3_2pp36-44.pdf

6 Minchin, N. (2001, June). INVISIBLE VALUE: THE CASE FOR MEASURING: AND REPORTING INTELLECTUAL CAPITAL. *ISR New Economy Issues*(1). Retrieved July 9, 2017, from http://www.bengin.net/chadmin/NEBic-short_july01.pdf

7 Investopedia. (2011). *Economic Value Added - EVA*. Retrieved July 09, 2017, from investopedia.com: http://www.investopedia.com/terms/e/eva.asp

8 Fijałkowska, J. (2014). Value Added Intellectual Coefficient (VAIC™) as a Tool of Performance Measurement. *Przedsiębiorczość i Zarządanie (Entrepreneurship and Management), 15*(1), 129-140. doi:10.2478/eam-2014-0010

9 Ulum, I., Ghozali, I., & Purwanto, A. (2014, December 1). Intellectual Capital Performance of Indonesian Banking Sector: A Modified VAIC (M-VAIC) Perspective. *Asian Journal of Finance & Accounting, 6*(2), 103-123. doi:10.5296/ajfa.v6i2.5246

10 Institute, B. S. (2014). *Balanced Scorecard Basics*. Retrieved July 8, 2017, from balancedscorecard.org: http://www.balancedscorecard.org/BSC-Basics/About-the-Balanced-Scorecard

11 Kokemuller, N. (n.d.). *How Does the Balance Scorecard Work?* Retrieved July 8, 2017, from chron.com: http://smallbusiness.chron.com/balance-scorecard-work-16092.html

12 Sabine, B. G. (2013). Measuring Intellectual Capital. *Enabling Innovation: Innovative Capability – German and International Views*, 17- 26. doi:10.1007/978-3-642-33389-7_2

13 Syeiby, K.-E. (2016, january 6). *Measuring the value of intangble asset: summary of Syeiby's IAM*. Retrieved July 8, 2017, from valuebasedmanagement.net: http://www.valuebasedmanagement.net/methods_iam.html

14 Vaz, C. R., Rocha, P. R., Werutsky, V. D., Selig, P. M., & Morales, A. B. (2015). Measurement Models of Intellectal Capital for the Decision Making and Performance Variables. *Global Journal of Management and Business Research: G Interdisciplinary, 15*(1). Retrieved July 04, 2017

15 Brooking, A. (1996). *Intellectual Capital: Core Asset for the Third Millennium Enterprise*, . New York.: International Thomson Business Press.

16 Müller, C. (1997). The 3 MS of Intellectual Capital - Measuring, Monitoring, and Managing

17 Bontis, N. (1998). *Intellectual capital: an exploratory study that develops measures and models. Management Decision* (Vol. 2). doi:10.1108/00251749810204142

18 Trajtenberg, M. (1990). A penny for your quotes: Patent citations and the value of innovations. *Rand Journal of Economics, 21*(1), 172-187.

19 Kaplan, R., & Norton, D. (2016, January 6). *Summary of the BSC Method By Kaplan and Norton*. Retrieved July 8, 2017, from valuebasedmanagement.net: http://www.valuebasedmanagement.net/methods_balancedscorecard.html

20 Matos, F. (2013). A Theoretical Model for the Report of Intellectual Capital. *The Electronic Journal, 11*(4), 339-36. Retrieved from www.ejkm.com

21 George, B. C. (2010). Intellectual Capital Measuring - A Comparative Approach. *The Young Economists Journal, 8*(Special Issue), 55-60.