Development of an Improved Multi-Factor Authentication Scheme for Internet Banking

Afolabi Olaitan O. [1] and Oluwatope Ayodeji O.[2]

[1]Salem University, Lokoja, Nigeria, olaitanmails@yahoo.co.uk

[2]ObafemiAwolowo University, Ile-Ife, Nigeria, aoluwato@oauife.edu.ng

Abstract

Data compromise is a major challenge for the Internet banking system. Several schemes have been proposed to mitigate attacks against users; this includes use of passwords, which are vulnerable to keyboard sniffers, password guessing and shoulder surfing. The need to accurately and reliably authenticate users is the motivation behind this study. In this paper, a multi-factor authentication technique is formulated by integrating three entity authentication policies. The technique is characterised by the use of unique factors of authentication at different points in a transaction process. The model was transformed into an algorithm and simulated with Matlab. A set of passwords, challenge questions, token codes and iris images were obtained to serves as input data to the simulated model. Performance comparison of the proposed model with an existing model was carried out using false acceptance rate (FAR) and false rejection rate (FRR) as metrics. The simulation result for the proposed and existing scheme showed a 100% and 95% Success Rate respectively. The proposed scheme can substantially strengthen the overall security of internet-based bank transactions and effectively protect customers' sensitive information.

Keywords: *Data compromise, Internet banking, multi-factor, entity authentication, performance, information security.*

1. Introduction

Society depends heavily on computers. One benefit is computers' ability to communicate with one another creating networks. In most cases, network computing is cost-effective from the pooling of resources [1] [2].

Economic and social factors may lure network users into data compromise. A dishonest party can access and sometimes be able to control a communication. Protection against malicious activities [3] using various network security mechanisms is among the main objectives of building a dependable system.

Financial institutions use communication networks for storing, processing, and exchanging private and critical information. A basic network infrastructure normally does not provide any guarantee to a communicating party about the state of other parties on the network [4]. Therefore, a layer of protocols is employed for reliable communication and synchronisation of the states of communicating parties.

An important goal of network security is entity authentication [5], which refers to the process where one party, the verifier, clears the claimed identity of another communicating party, the claimant. Usually, the claimant presents claimed identity to a verifier with evidence to support any information.

Entity authentication is a natural requirement for Internet banking (a possibility to initiate financial transaction via Internet connection to one's bank or other financial institution) transactions. Authentication enables a manager to prevent unauthorised parties from using a private network, while allowing the actions of authorised parties. Without authentication, an adversary can pretend to be an authorised party and could play an intermediate role between honest parties.

To bind identity more closely to an entity and appropriate authorisation, a strong identity convention must be in place. This should not be based only on what a person has (smart cards) or knows (passwords) but in addition t physical characteristics or personal behavioural traits - biometrics. These are measurements of behavioural or physical attributes; how an individual smells, walks, signs their name, or even types on a keyboard, their voice, fingers, facial structure, vein patterns or patterns of an eye's iris. Form more than a decade financial institutions have seen an increase of Internet-banking abuse. Since Internet banking is widely used, criminal users have proliferated- organised criminal attempts are commonplace. Therefore, financial institutions need to implement robust controls as the transaction risk level increases.

This paper introduces a multi-factor (combination of more than one authentication factor) technique, ensuring a higher level of security to Internet banking applications. The scheme implements use of unique authentication factors at different points in a transaction process so the strength of one factor compensates for the weakness of another. This can substantially strengthen the overall performance of Internet-based services by reducing account takeovers and resulting financial loss.

The rremainder of this paper is: Section 2 presents a brief literature review of previous work in the field of entity authentication; Section 3 is a description of methodology adopted; Section 4 details experimental results; Section 5 discusses and analyses results of the experiments and general conclusions are made in Section 6.

2. Literature Review

Much research has been performed in the field of entity authentication; many models have been developed. In [6] Yoon *et al.* propose a scheme to address the problem of insecurity in remote access of Internet and wire/wireless communication environments. The scheme adopted bit-wise exclusive-OR (XOR) operation and collision-free one-way hash functions as main cryptographic operations to provide flexibility in a biometrics remote user authentication scheme via smart cards - in a quest to achieve security, reliability and efficiency. However, the scheme proved vulnerable to impersonation in the event of a smart card loss.

To address the vulnerability of session password to shoulder surfing; Sreelatha *et al.* [7] proposed a pair-based, hybrid textual authentication scheme suitable for use in Personal Digital assistants (PDA). The method generated session passwords using text and colours. Ramasamy *et al*. [8] proposed a scheme to reduce authentication attacks, using password RSA cryptography embedded in a smart card in a bid to provide authentication with reasonable computational cost. In their own scheme Chandran *et al.* [9] integrated fingerprint and iris scenario using multiple sensors for data acquisition. The integration of iris and fingerprint biometrics to overcome hurdles of uni-modal biometric system accomplished the purpose of a reliable and accurate identification/verification using biometric technologies.

To enhance security with an optimal overall time taken for the grid operation, Jaspher *et al.* [10] combined location factor: 'some place the user is'; with password and biometric data to propose a privacy preserving biometric authentication scheme for a grid environment. Liao *et al.* [11] presented their Diffie-Hellman key agreement protocol to encrypt /decrypt communicated messages with symmetric cryptosystem for prevention of system resources fraud by illegal users over insecure networks. For Patel *et al*. [12] resolving security issues evolving from entity authentication was a concern. Their solution for accurate identity authentication was based on pattern recognition of human iris; the scheme is applicable to many authentication systems, enhancing security and eliminating fraud.

An algorithm based on local binary pattern and histogram approaches for feature extraction, and a linear vector quantisation classifier for classification was developed by Suganthy *et al.* in [13]. They designed the scheme to distinguish valid from unauthorised users during an identity check. The major advantages of their system were its requirement of few components on implementation and effectiveness of integration within security systems. In their survey of different iris recognition methods to build integrated classifier on latest input device, Sheela *et al*. [14] explored discrete cosine transforms, corner detection and parametric template methods to provide a measurable physical attribute for authentication.

They recommended the application for accuracy and speed in secure communications and mobile commerce.

Rama *et al.* [15] proposed a fusion mechanism amalgamating a canny edge detection scheme and a circular Hough transform, to detect the iris boundaries digital eye images. The scheme integrates iris recognition with a smart card to develop a high security access environment for reliable human authentication in automated teller machines (ATMs).

In fingerprint-based online banking authentication scheme proposed by Singhal *et al*. [16].Statistical, spectral and structural texture analysis techniques was used in the analysis and classification of fingerprint images. This model has an advantage in a low cost fingerprint identification system operable with small computers. However, the password factor in this scheme factor was static in nature hence prone to replay attack and impersonation, since a one-time registration used over time; the fingerprint biometric authentication is prone to a higher error rate. To cover these drawbacks the writers of this paper present an integration of three authentication factors in four echelons; a combination of static passwords, challenge questions, random numbers codes and iris recognition as authentication factors in their algorithm. A major advantage is each authentication factor for each user is synchronised. This implies each authentication tool or device issued by a bank authority is tagged with a user name and password such that in the case of token device loss an impostor will not be able to access a user's account without the corresponding iris template. The schematic representation of this technique is as shown in Figure 2.1.

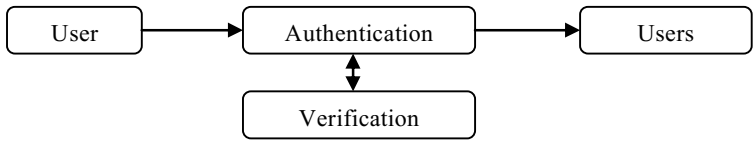

Figure 1: The proposed multifactor authentication scheme

3. Methodology

The proposed Multifactor Authentication Scheme is a solution born from an inherent lack of security of traditional authentication techniques via the Internet. The multi-factor authentication scheme allows a web page to include a validation check using objects embedded in the page. This calls on an interface to activate an Iris recognition device attached to the client's computer, which returns a coded Iris to the server where it is validated alongside with password and user ID, challenge questions and token codes.

3.1 Model Description

A description of the MAS algorithm is:

Registration Phase
A user was enrolled for an Internet bank transaction with assistance of a bank employee by capturing an eye image with an iris recognition device connected to the bank's registration computer system. The user was issued a password for initial login. Users were then required to change the password, then issued a token device. Information personal to a user was recorded and stored in the bank's database to serve as challenge questions.

First Authentication Phase
A user navigated to a page on the secured server through a Web browser and if not logged-in redirected to a log-in page. There, a form with fields prompted a user's ID and password. The user filled in user ID and password then submitted the page to the server for authentication. The web server received the log-in ID and the encrypted password and passed on the user ID and password data to a server-side authentication application. On a successful validation, the user proceeded to the second authentication phase - challenge questions.

Second Authentication Phase
A user was prompted to answer personal pre-registered questions supplied during the registration phase and submit. After a maximum of three attempts, a user was logged out. If a user was successfully authenticated the browser navigated to the third phase for token authentication.

Third Authentication Phase
This phase required the user to supply codes generated from the token issued by the authorising bank. The token was tagged with the user's identity prior to issue; a user was equally subjected to maximum of three attempts at this level.

Fourth Authentication Phase
The final phase of authentication was Iris recognition; a user focused on the Iris recognition device attached to the computer. A live eye image captured by the camera was displayed on the page of the computer. The biometric authentication application fetched the user's iris codes, obtained previously during the registration process from the database and compared it against the live iris codes. Based on success or failure result the browser redirected the user either to a page reporting the failed attempt or to a page where the user carried out the Internet transaction. In failed attempts, the user's account is locked and they were required to consults the bank for account reactivation. Figure 2 shows the structural description of the proposed multifactor model; Figure 3depicts the architectural design.

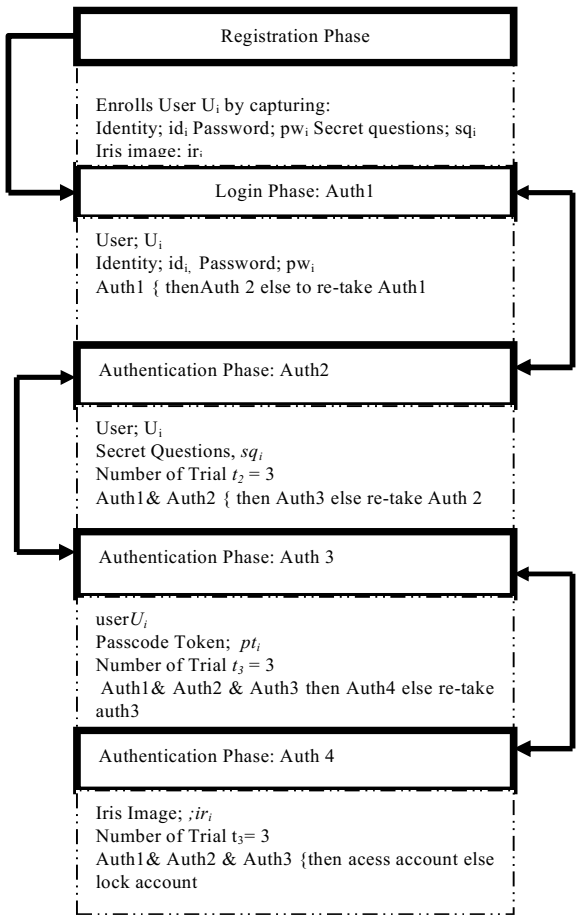

Figure 2: Structural diagram of representation proposed Multifactor Authentication Scheme

3.2 Performance Metrics

Metrics used for performance evaluation include:

False Acceptance Rate (FAR): The ratio of the number of impostor images considered as authentic by the algorithm against the total of impostor images.

$$FAR = \frac{ImpostersClaimAccepted}{TotalImpostClaim} x\ 100\% \quad \text{(1)}$$

False Rejection Rate (FRR): The ratio of the number of authentic images not considered qualified by the algorithm against total authentic images

$$FRR = \frac{TrueClaimsRejected}{TotalTrueClaims} x\ 100\% \quad \text{(2)}$$

Equal Error Rate (EER): The point at which FRR and FAR intercepts; used as the threshold point to calculate score distribution.

$$EER = \frac{FAR+FRR}{2} \quad \text{(3)}$$

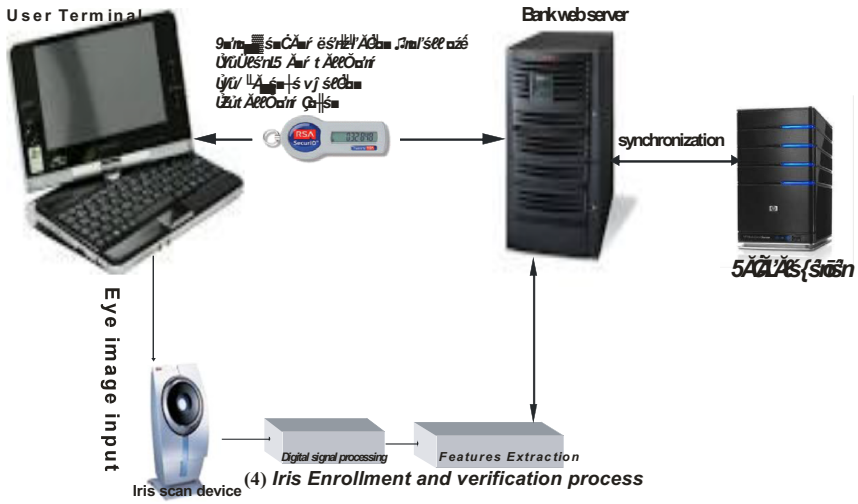

Figure 3: Architectural design of the proposed Multifactor Authentication Scheme

3.3 Data Acquisition

To implement the model, four different datasets were required for each authentication phase. This included passwords, challenge questions, token codes, and iris images. For this research passwords were generated from: http://www.freepasswordgenerator.com/, challenge questions were formulated for each user, eight digits tokens were randomly generated from: http://graphpad.com/quickcalcs/randomN1.cfm while fingerprint and eye images were downloaded from http://biometrics.idealtest.org/; CASIA; Chinese Academy of Sciences - Institute of Automation database. Fingerprint images were used to implement the existing model used for performance evaluation.

4. Experimental Results

In this section experiments were performed on the proposed and the existing schemes in which case the results were evaluated.

4.1 Proposed Scheme

Users U001 to U070 were serially enrolled for their passwords, challenge questions, token codes and a pair (left and right) of 70 iris images were enrolled for iris using their respective algorithms. Enrolment process of the iris image involves image pre-processing and feature extraction with a resulting iris codes in form of binary bits stored in the database.

To verify the proposed model for FAR, eighty (80) users were serially verified for the same datasets enrolled. In this case, users U071 to U080 were not part of the earlier enrolled users. Serial matching of each user's input passwords, challenge questions, token codes and iris images was performed with the database. To match iris templates, the Hamming Distances between input iris code and the stored iris code was computed to decide the condition for acceptance or rejection of an iris image as authentic or otherwise. [The Hamming Distance is a measure of the variation between the current iris code and the iris code stored in the database].

Under normal circumstances the algorithm was expected to correctly recognise users U001 to U070 and reject users U071 to U080, which were not enrolled users. However, there are many possible scenarios of impersonations in FAR; of which the following two are considered:

i) Keystroke loggers only.
ii) Keystroke loggers and hardware token theft.

For FRR, users U001 to U070were enrolled and verified using the same procedure in FAR. The algorithm was expected to correctly recognise all users, since only correct users were verified. FRR is said to have occurred in case of any rejection. Figure 4 shows the plotting of the resulting FRR and FAR using common threshold values: 0.00, 0.05, 0.10, 0.23, 0.37, 0.42 and 0.53in both cases.

4.2 Existing Scheme

To compare the performance of this scheme a similar experiment was performed with the Singhal *et al* scheme. The model implemented two authentication factors: password and fingerprint biometrics using the algorithm proposed. Users U001 to U070 were serially enrolled for their passwords and a pair (left and right) of 70 fingerprint images. To verify the model for FAR, eighty (80) users were serially verified for the same datasets enrolled. In this case, users U071 to U080 were not part of the earlier enrolled users. Serial matching of each user's input passwords and fingerprint was performed with the database.

Similarly, users U001 to U070 were enrolled and verified for FRR using the same procedure in FAR. The algorithm was expected to correctly recognise all users, since correct users only were verified in this case. FRR is said to have occurred in case of any rejection. Figure 5 shows the plotting of the resulting FRR and FAR.

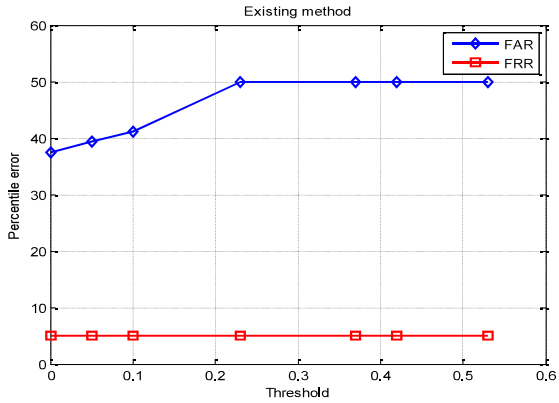

Figure 3: Plot of FAR and FRR of Singhal et al (existing) scheme

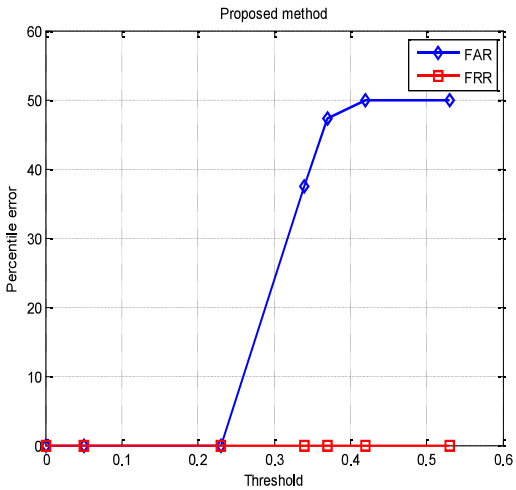

Figure 4: Plot of FAR and FRR of proposed scheme(FAR scenario (i))

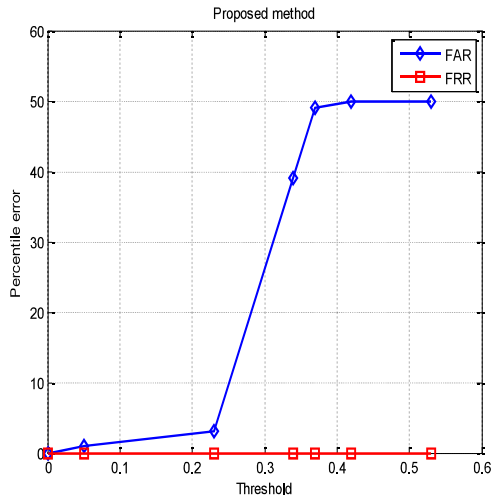

Figure 5: Plot of FAR and FRR of proposed scheme (FAR scenario (ii))

5. Discussion

Figure 3 shows the graphical plotting of FAR and FRR of the Singhal *et al*. scheme. In this scenario, the writers assumed all users' impersonation of password factor for FAR succeeded; the only input data prone to impersonation was the password factor. The system stood a risk of higher vulnerability to impersonation attack compared to the proposed scheme. This degraded the performance of the overall system resulting in 50% of FAR and 5% of FRR. This result implied the system accepted 50% only of all genuine users; 5% of true users were falsely rejected. In other words, the system recorded a 50% and 95% success rate for FAR FRR respectively.

Figure 4 shows results of FAR and FRR of the proposed scheme under scenario (i). This scenario assumes users' computers were compromised for the first two factors: passwords and challenge questions; being the only two inputs capable of being impersonated by key loggers. By analogy, imposters were not in possession of the other two factors: hardware token device and the live eye image of the correct users. In this case, the performance of the system was increased which implied a lower FAR. This was because imposters, which might have tricked the biometric authentication phase, it being the final phase, were rejected at the time the token codes were checked. The experiment showed 0% error rate below 0.23threshold, percentile error, however increased above 0.23.If one considers a threshold of 0.23, a FAR

of 0% and 0% FRR is achieved. This implied the system in general accepted 100% of all genuine users; 0% true users were falsely rejected - the system recorded a 100% success rate in each case.

Figure 5 shows the plotting of FAR and FRR of the proposed scheme under scenario (ii). There it was assumed potential impostors were in possession of the correct first three factors: password, challenge questions, and hardware token device with the exception of the live eye image of the original user of the account. Under this condition, the performance of the system was degraded as all impostors succeeded in gaining access to the final authentication phase - iris biometric authentication. This scenario also implied only fingerprint and iris biometrics was accessed in the proposed and existing schemes respectively. Although the result showed a better performance with only 1% and 3% FAR at 0.05 and 0.23 threshold respectively, as opposed 39.39% and 50% FAR in Singhal *et al* scheme. Scenario (ii) however defeated the purpose of our research, and as such, the result was not considered for performance evaluation.

6. Conclusions

This paper describes an alternate scheme to identify individuals for Internet bank transactions using multiple authentication factors.Comparing the simulation results of the proposed scheme with Singhal *et al.* scheme, this implementation served its purpose with a better performance in users' authentication.To this end, the approach presented in this paper provided better insight for entity authentication in Internet banking. Future work may see threat-alerting capabilities considered

References and Bibliography

[1] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, United State of America, January 2011.

[2] L. Zhu, Q Li.and L.He, "Study on Cloud Computing Resource Scheduling Strategy Based on the Ant Colony Optimization Algorithm", IJCSI, International Journal of Computer Science Issues,Vol. 9, Issue 5, No 2, pp 54-58, September 2012.

[3] K. Alsubhi, Y. Alhazmi, N. Bouabdallah, "Security Configuration Management in Intrusion", International Journal of Security and Networks, Vol. No.1, pp 30-39, 2012.

[4] P. Darandale, S. Deshmukh, S. Jadhav, and S. Gore, "A reliable and flow control communication for dynamic network coverage and data security having energy audit functionality in Mobile sensor network", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 10,pp 581-585, October 2012.

[5] M. Aiash, G. Mapp and A. Lasebae. "A Survey on Authentication and Key Agreement Protocols In Heterogeneous Networks", International Journal of Network Security & Its Applications (IJNSA).Vol.4, No.4, pp 199-214, July 2012.

[6] J. E. Yoonand K. Y.Yoo."A Robust and Flexible Biometrics Remote User Authentication Scheme", International Journal of Innovative Computing, Vol. 8 No. 5, pp 3173-3188, May 2012.

[7] M. Sreelatha, M. Shashi, M. Anirudh, M. S. Ahamer and V. M Kumar, " Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No.3, pp 111-119, May 2011.

[8] R. Ramasamy, and P.A Muniyandi, "An Efficient Password Authentication Scheme for Smart Card",International Journal of Network Security, 14(3):180-186, June, 2012.

[9] G. C. Chandran and R. S. Rajesh, "Performance Analysis of Multimodal System Authentication", International Journal of Computer Science and Network Security, Vol. 9No.3, pp 290-296, March 2009.

[10] G. Jaspher, K. Willsie and E. Kirubakaran, "Biometric Authentication and Authorization System for Grid Security", International Journal of Hybrid Information Technology Vol. 4 No.4, pp 43-58, October 2011.

[11] I. Liao, C. C. Lee and S. M. Hwang, "A Password Authentication Scheme Over Insecure Networks", Journal of Computer and System Sciences, Vol.72 Nol. 2006, pp 727–740, October 2005.

[12] D. C. Patel, S. Trivedi and S. Patel, "Biometrics in Iris Technology: A Survey", International Journal of Scientific and Research Publications, Vol.2 No.1, pp 1-5, January 2012.

[13] M. Suganthy, P. Ramamoorthy, R. Krishnamoorthy, "Effective Iris Recognition for Security Enhancement", International Journal of Engineering Research and Applications (IJERA), Vol. 2 No.2, pp 1016-1019, April 2012.

[14] S. V. Sheelaand P.A Vijaya, "Iris Recognition Methods – Survey", International Journal of Computer Applications, Vol. 3 No.5 pp19-25, June 2012.

[15] R. Rama and V. A. William, "Design of Iris Recognition based Authentication System in ATM", "*International Conference on Computing and Control Engineering*", *ICCCE-2012*, 12 & 13 April, 2012.

[16] A. Singhaland V. Mittal, "A Brief Review: Fingerprint Authentication System", International Journal of Applied Engineering Research, Vol. 7 No.11, ISSN: 0973-4567, 2012.

Authors

Principal Author: Afolabi Olaitan O. holds a B.Tech degree in Computer Engineering from the Ladoke Akintola University of Technology, Ogbomoso, Nigeria and is working on her Masters degree in Computer Science at Obafemi Awolowo University Ile-Ife, Nigeria. She teaches at the College of Information and Communication Technology, Salem University, Lokoja, Nigeria.

Co-author: Oluwatope Ayodeji O. has a Ph.D in Computer Science. He teaches and conducts research in the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife. Nigeria. He is the supervisor of this study. He has published several articles and received research grants; including TETFund Research Grant from the Nigerian Government. He is a member of the Nigerian Young Academy.

Presenter: This paper is presented by Afolabi Olaitan O.