# MULTI-LEVEL ACCESS CONTROL SYSTEM FOR INTERNET FINANCIAL TRANSACTIONS

**Afolabi Olaitan O.**
Salem University, Lokoja
**NIGERIA**

**Oluwatope Ayodeji O.**
Obafemi Awolowo University, Ile-Ife
**NIGERIA**

**Oluwagbemi Folakemi E.**
Salem University, Lokoja
**NIGERIA**

## ABSTRACT

This study developed an improved multi-level access control system for internet financial transactions. It formulated, simulated and evaluated the performance of the model. This was with a view of preventing internet financial transaction fraud, which mitigates against users. Three factors of entity authentication policies in four levels were integrated. 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 serve 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 result showed that 50% of FAR and 5% of FRR was recorded resulting in 50 % and 95 % Total Success Rate (TSR) respectively in the existing scheme. In the proposed scheme, FAR of 3 % and 0 % FRR were achieved, this implied 97 % and 100 % TSR respectively. The research implementation served its purpose when compared with the existing scheme by showing a better performance in users' authentication. This proposed system can be effective in protecting sensitive customers' information by significantly reducing the rate of internet financial transaction frauds.

**Keywords:** Access Control, Authentication, Internet, Security.

## INTRODUCTION

The present society depends heavily on computers. One of the benefits of these computers is their ability to communicate with each other and engage in network computing. In most cases, network computing is cost-effective, due to pooling of network resources, and it provides redundancy to develop dependable services (Mell & Grance, 2009), (Zhu et. al., 2012). One of the benefactors of network computing is financial institutions. Financial institutions use communication networks for storing, processing, and exchanging private and critical information. However, the basic network infrastructure normally does not provide any guarantee to a communicating party about the state of other parties on the network (Darandale et. al., 2012). Therefore, a layer of protocols is often used for reliable communication and synchronization of the states of communicating parties.

An important goal of network security is entity authentication (Aiash et. al., 2012), which refers to the process where one party, the verifier, verifies the claimed identity of another communicating party, the claimant (Chavan, 2013). Authentication enables a manager to prevent unauthorized parties from using a private network and allows accountability on the actions of authorized parties. Without any authentication, an adversary can pretend to be an authorized party and may play an intermediate role between honest parties. To bind identity more closely to an entity and appropriate authorization, a combination of different authentication factors can be used. Which includes passwords, challenge question, token codes and biometrics features such as; measurements of behavioral 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 in the iris. Since internet financial transactions is used widely, financial institutions have witnessed an increase in the abuse. Therefore, there is a need to implement more robust controls as the risk level of the transaction increases.

This paper, introduces a multi-level (combination of more than one authentication factor in four levels) technique which will provide a higher level of security to internet financial applications. This authentication scheme is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control (FFIE, 2005). This can substantially strengthen the overall security of internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses.

## LITERATURE REVIEW

Over years numerous researches had been carried out in the field of entity authentication with many different models being developed. Chandran and Rajesh (2009) integrated fingerprint and iris using multiple sensors for data acquisition. The independence of the traits ensures the improvement in performance multimodal biometric system. To address the vulnerability of session password to shoulder surfing; Sreelatha et. al, (2011) proposed a pair-based and hybrid textual authentication scheme. The method generates session passwords using text and colours. This scheme is identified as suitable for use in Personal Digital Assistants (PDA). According to Ramasamy and Muniyandi; the focus of their scheme is to reduce authentication attacks as well as the server over head of maintaining large user data for authentication. The technique adopts password RSA cryptography embedded in a smart card in a bid to provide authentication with reasonable computational cost.

To mitigates illegitimates access into email account Ghogare et. al. (2012) also proposed location based authentication scheme using location, biometrics and cryptographic techniques. It captures geographical location of a user entity which is latitude and longitude with a Global Positioning System (GPS) device for authentication. It ensures authentication of legitimate users with location credentials into email account. Singhal and Mittal (2012) is the core literature used in evaluating our proposed scheme. Statistical, spectral and structural texture analysis techniques was used in the analysis and classification of fingerprint images.

## METHODOLOGY

The proposed scheme is designed to suit internet financial transactions system for the purpose of accuracy in authentication of entities. The model allows a web page to include a validation check using objects embedded in the web page. This calls on an interface to an iris recognition device attached to the client computer, which returns a coded iris to the server where it is validated along with password and user ID, challenge questions and token codes. The scheme consists of five phases namely: the registration phase, the first authentication phase, the second authentication phase, the third authentication phase and the fourth authentication phase.

The registration phase enrolled users for internet financial transaction by capturing his/her eye image with an iris recognition device connected to the bank's registration computer system. The user was also issued a password to be used for initial login. Users were required to change the password before further transactions were carried out. At this point; the user was issued a token device, information personal to a user were also recorded and stored in the banks database to serve as challenge questions. The first and second authentication phases prompts users for his/her password and pre-registered challenge question respectively, the process carries out a matching with the earlier stored record. On a successful validation, the user proceeded to the third authentication phase. The third authentication phase requires that a user supply codes generated from the token issued by the authorizing financial institution, this token was tagged with the user's identity prior to issuance; a user was equally subjected to maximum of three attempts at this level. Upon a successful validation, the user proceeds to the fourth authentication phase.

The fourth phase of authentication is the user's iris subject recognition. A live iris subject was compared with the subject obtained previously during the registration process from the database. Iris recognition process involves image acquisition, segmentation, normalization, feature extraction and image matching. Segmentation is the technique used to isolate and exclude the non-iris features as well as locating the circular iris region. The normalization process produced iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. In the process of feature extraction, the significant feature of the iris was encoded in binary bits so that comparisons between templates can be made. Image matching process involves comparison of the stored iris code record with an image just scanned. Based on success or failure result, a user was either given an access to carry out his/her internet bank transaction or logged out while the account was locked and required to consults the financial institution's authority for a reactivation of his/her account.

## Performance Metrics

Performance parameters are metrics that allow the model to be evaluated for accuracy. To evaluate the performance of the model, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) and Total Success Rate (TSR) are the metrics used in the evaluation of the model. False Acceptance Rate (FAR) is the ratio of the number of impostor images considered as authentic by the algorithm to the total number of impostor images. False Rejection Rate (FRR) is the ratio of the number of authentic images not considered qualified by the algorithm to the total number of authentic images. Equal error rate (EER) is **t**he point at which FRR and FAR intercepts. This is the used as the threshold point used to calculate score distribution. Total Success Rate (TSR**)** is the success of the experimentation with either FAR or FRR. Equations (1), (2), (3) and (4) represents the mathematical notations for FAR, FRR, EER and TSR respectively.

$$FAR = \frac{Ica}{Tic} x\ 100 \qquad (1)$$

$$FRR = \frac{Tcr}{Ttc}\ x\ 100 \qquad (2)$$

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

$$TSR_1 = 100\% - \%FAR \qquad (4)$$

$$TSR_2 = 100\% - \%FRR \qquad (5)$$

Where:
$Ic_a$ = Impostors Claim Accepted, $Ti_c$= Total Impostors Claim, $Tc_r$= True Claims Rejected, $Tt_c$= Total True Claims, $TSR_1$ = Success of the experimentation with FAR, $TSR_2$ = Success of the experimentation with FRR

## Data Acquisition Method

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.

## Model Simulation

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 the simulated model. The resulting iris codes in form of binary bits were stored in the database. To verify the proposed model for FAR, eighty (80) users were serially verified for the same datasets enrolled. In which case, users U071 to U080 were not part of the earlier enrolled users. Serial matching of each users' 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. Under a normal circumstance; the algorithm is expected to correctly recognize users U001 to U070 and reject users U071 to U080, which were not part of the enrolled users in the database. To experiment for FRR, users U001 to U070 were enrolled and verified using the same procedure in FAR. The simulated model is expected to correctly recognize all users since only correct users are verified in this case. FRR is said to have occurred in case of any rejection.

To evaluate the performance of the proposed scheme, similar experiment was performed with Singhal and Mittal (2012) scheme. 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 users' 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 is expected to correctly recognize all users since only correct users are verified in this case. In case of any rejection; FRR is said to have occurred.

## RESULTS

Figure 1. and Figure 2. represents the graphical plot of the resulting FRR and FAR in the proposed and existing schemes respectively, using threshold values: 0.00, 0.05, 0.10, 0.23, 0.37, 0.42 and 0.53 in both cases. Figure 3. represents the graphical comparison of the Total Success Rate recorded when the model was experimented for FAR in the existing and the proposed schemes. While Figure 4 represents the graphical comparison of the Total Success Rate recorded when the model was experimented for FRR in the existing and the proposed.

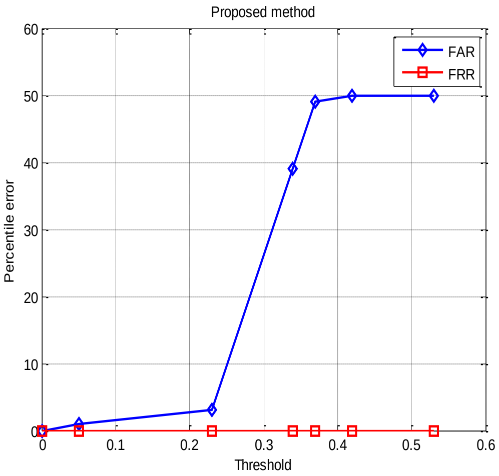

Figure 1. Graphical Plot of FAR and FRR of Proposed Scheme

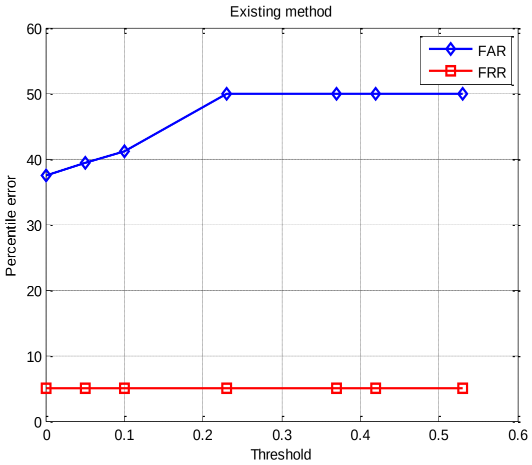

Figure 2. Graphical Plot of FAR and FRR of the Existing Scheme

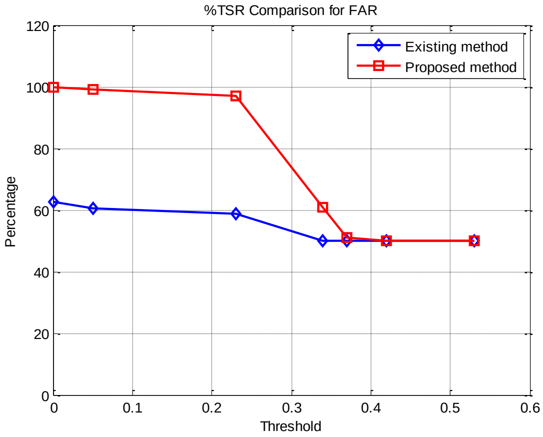

Figure 3. Graphical Plot of Percentage FAR Total Success Rate Comparison in the Proposed and the Existing Scheme

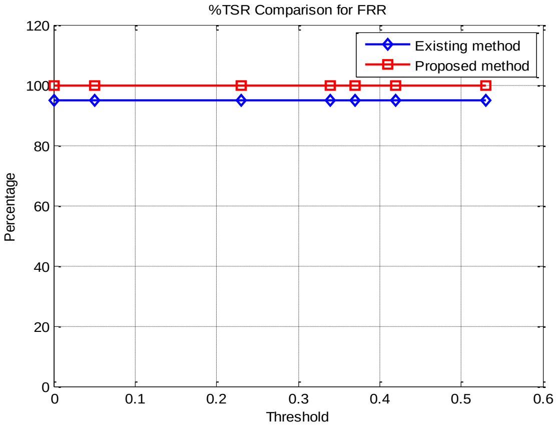

Figure 4. Graphical Plot of Percentage FRR Total Success Rate Comparison in the Proposed and the Existing Schemes.

## DISCUSSION

In the existing scheme (Singhal and Mittal, 2012) the system recorded a 50% and 95% Total Success Rate when it was experimented for accuracy for FAR and FRR respectively at a threshold of 0.23. While a 97% and 100% Total Success Rate was achieved in the proposed scheme experimented for accuracy FAR and FRR respectively.

## CONCLUSION

It can be concluded that there is not any single strategy that covers all the different dangers threatening the internet banking platforms. On the contrary, focusing on a multi-factor protection approach is the best alternative for massive authentication processes of applications that are highly exposed on the internet. This research through the results obtained established the fact that the rate of internet banking fraud is much lower when compared with Singhal and Mittal (2012) scheme. To this end, the approach presented in this thesis has provided better insight for entity authentication in internet banking.

## REFERENCES

Aiash, M., Mapp, G. & Lasebae, A. (2012). A Survey on Authentication and Key Agreement Protocols In Heterogeneous Networks. International Journal of Network Security & Its Applications. 4(4): 199-214.

Alsubhi, K., Alhazmi Y., & Bouabdallah, N. (2012). Security Configuration Management in Intrusion. Int. Journal of Security and Networks, 7(1) :30-39.

Chandran, G. C. J. & Rajesh, R.S. (2009). Performance Analysis of Multimodal Biometric System Authentication, International Journal of Computer Science and Network Security, 9(3): 290-296.

Chavan, J. (2013). Internet Banking- Benefits and Challenges in an Emerging Economy. International Journal of Research in Business Management (IJRBM), 1(1):19-26.

Darandale, P., Deshmukh, S., Jadhav, S. & Gore, S. (2012). A Reliable and Flow Control Communication Protocol for Dynamic Network Coverage and Data Security Having Energy Audit Functionality in Mobile Sensor Network. International Journal of Emerging Technology and Advanced Engineering, 2(10): 581-585.

FFIE. (2005). Supplement to Authentication in an Internet Banking Environment. Federal Financial Institutions Examination Council. Retrieved on 29th March, 2015 from: http:// www.federalreserve.gov/bankinforeg/srletters/sr1109a1.pdf.

Mell, P., & Grance, T. (2009). The NIST Definition of Cloud Computing National. Institute of Standards and Technology, United State of America.

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

Singhal, A. & Mittal V. (2012). A Brief Review: Fingerprint Authentication System. International Journal of Applied Engineering Research, 7(11): 1-4.

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, S. & Manoj, K. V (2011). Authentication Schemes for Session Passwords using Color and Images. International Journal of Network Security & Its Applications (IJNSA), 3(3): 111-119.

Zhu, L., Li, Q., & He L. (2012). Study on Cloud Computing Resource Scheduling Strategy Based on the Ant Colony Optimization Algorithm. International Journal of Computer Science Issues, 9(5): 54-58.