EasyChair Preprint

№ 4066

An Enhanced Multimodal eBanking Security Model

Moses Agana and Samuel Eneji

August 23, 2020

An Enhanced Multimodal eBanking Security Model

Abstract: This study is designed to provide an enhanced multimodal eBanking security using Bank Verification Number (BVN) Personal Identification Number (PIN) and biometrics as mandatory authentication requirements to forestall the vulnerabilities in existing eBanking security systems. The design divides the authentication requirements into two datasets, stored separately and accessed independently by two servers. The system collects a user's biometric and the non-biometric data in a separate database objects. Each user record in one database has a link to call the record in the other database. Divide-and-Conquer algorithm is employed with QuickSort method to sort desired records independently. During transaction, the two servers sort and retrieve the user's record for matching and authentication before granting access. The test results show that the model would provide an enhanced security in eBanking transactions over existing systems. The implementation of the system would significantly curb frauds associated with eBanking and related services.

Keywords: Multimodal, eBanking, Authentication, Biometric, Fraud, Security.

1. Introduction

Electronic banking (eBanking), otherwise known as Internet banking is simply an online banking system propagated via the Internet using communication gadgets such as the computer, mobile phones, Automated Teller Machine (ATM), etc. Internet banking improves greatly on banking services to customers and makes transactions more convenient without requiring the user to necessarily visit the banking hall, and it is devoid of time barriers [1]

Internet or electronic banking is simply an online banking system propagated via the Internet, using communication gadgets such as the computer, mobile phones, Automated Teller Machine (ATM), etc. Internet banking improves greatly on banking services to customers and makes transactions more convenient without necessarily visiting the banking hall and without time barriers [2].

Internet banking improves greatly on banking services to customers and makes transactions more convenient without necessitating users to visit the banking hall and without time barriers [3]. With internet banking, one can buy and sell without physical cash, make deposits, transfer, pay bills, etc. with ease [4]. Electronic banking is driving the world toward cashless banking. It connects the users to their banks universally without barriers of time and location provided they have access to the Internet [5].

1.1 Security Threats in eBanking

The electronic banking system with its great benefits to the users and the banking system, has heralded great security threats to banks and their customers due to the insecure nature of the cyberspace through which the services are mediated. Electronic banking makes use of access codes such as Personal Identification Number (PIN) and passwords before access is granted to the user. The rationale for using such codes is based on the assumption that the blogger is the genuine bank customer [3]. This is not always true, fraudsters use various avenues to divulge or steel customers' secret access codes which they personalize, and use

the opportunity to impersonate and rob their victims of their funds from the bank without being detected or caught [6].

Many banking customers dread electronic banking for fear of being defrauded. Some internet thieves (cyber criminals) send scams at random to phone numbers requesting personal for electronic bank access codes in the guise that they are bank staff who render customer services. Bank customers who do not seek verification from their banks will easily fall prey.

Insecure network protocols that provide end-to-end connections via which eBanking transactions are mediated provide avenues for cyber criminals to exploit and defraud bank customers anonymously [7]. Some of the threats to Internet banking include, but are not restricted to session hijacking, identity theft (such as password and PIN cracking), phishing scam, (luring users to divulge sensitive information about their accounts to fraudsters who masquerade as genuine bank staff or agents), use of Trojans, Denial of Service (DoS) attacks, server bugs, super user exploits (a situation where fraudsters or attackers gain control of a system as if they were an administrator), etc. [8], [9], [10], [11].

1.2 Electronic Banking Security Models

As a compendium to combat the menace of Internet banking security threats, various models have been developed over time. A retinue of such security models for Internet banking as summarised in Table 1 have their strengths and weaknesses [12], [13], [14].

Table 1: eBanking security models with their strengths and weaknesses.

eBanking Security Models	**Weaknesses**
Digital Certificates: Uses Public Key Infrastructure (PKI) and a Certificate Authority (CA) to authenticate both the users and the banking system itself.	Both A1 and A3 certificates can be exported and remotely used by more than one user at the same time, enabling criminals to use stolen certificates
One-Time Password (OTP) Token: Often used as a second authentication factor, and may be requested in specific or random situations. The passwords change dynamically, thus rendering captured authentication data useless for future attacks.	The password leaked to a third party if the owner is lured and can be used for unauthorized transactions.
Browser Protection: used in securing the system at the Internet browser level.	Counterfeit online banking system web pages can be used prevent the protection from properly loading.
Device Registering: used in restricting access to the banking system to previously known and registered devices.	Spoofing of characteristics thought to be unique to the user's device may be reproduced by hackers for fraudulent transactions.
CAPTCHA (Automated Public Turing test to tell Computers and Humans Apart): used to render automated attacks against authenticated sessions ineffective.	OCR software can be used to extract the desired information.
Positive Identification: requires the user i to input some secret information only known to him for self identification.	Secret information may leak in the Internet or via social engineering techniques.
Transaction Monitoring: uses artificial intelligence transaction history analysis and related methods to identify fraud patterns in previously processed transactions.	Some malwares can create behavior profiles to impersonate the user profile.

2. Objectives

The objectives of this study are to:

1. Design an eBanking security model using Bank Verification Number (BVN) and biometrics (fingerprints, voice and/or facial recognition) as a mandatory requirements in each login for user authentication.
2. Use the model to prevent electronic banking fraud by granting access to electronic banking services only to those authenticated using the login requirements in (1) above.
3. Implement the model using the Divide-and-Conquer algorithm with the QuickSort method on two separate servers to sort and retrieve the user's records for matching and authentication before granting access.

3. Methodology

Biometrics authentication on the Bank Verification Number (BVN) database was employed in the model. This is to ensure that at any point of transaction; the customer is authenticated using the actual biometrics. The system is an integration of the BVN module, the authentication module, and the transaction module.

The BVN database is the backend of the system that stores non-biometric data entities of a bank customer, used for real time authentication. The bank customer's BVN and the biometrics captured at the point of registration/account opening are authenticated with the information contained in the BVN database against the customer.

The authentication module provides the user interface and verifies login credentials against what is stored in the database. If there is a match, the system will capture the customer's biometrics (fingerprint and voice/facial image) as applicable for further authentication with the records in the BVN database. If the authentication is successful, the customer is granted access to the electronic banking platform for transactions. If an authentication attempt fails in three successive times, the user is branded a fraud suspect, triggering the blocking of the suspect's accounts, and a comprehensive report is generated for management action. The system will equally check for any account in the BVN database that may be associated to the captured biometrics with wrong BVN and block the accounts as well.

The transactions module allows a customer who logs in successfully to do electronic banking transactions.

3.1 Mathematical Specifications of the System

The database specification of the system is expressed mathematically as:

$f_n = \frac{1}{2}\, n(f_x.f_y)$ (1)

where:

f_n = function for sorted customer's record

n = Divide-and-Conquer algorithm factor

f_x = function for a customer's biometrics record sorted from BVN database

f_y = function for customer's other records without biometrics sorted from BVN database

The function is to enhance quick sort of customer's records from the BVN database, and the presentation of the sorted record on the customer's page for authentication access.

The logic representation of the system is expressed as:

$$(c.f_n) = \begin{cases} y_1 = f_c \text{ if } (f_b \in f_{d)} \text{----------} T \\ y_2 = f_c \text{ if } ((f_{b\,.f_{b2}}) \in f_{d)} \text{--------} T \\ y_3 = Grant\ Access \end{cases} \quad (2)$$

$$(c.f_n) = \begin{cases} y_1 = f_c \text{ if } ((f_b + f_{b2}) \in f_d) - - - - - \text{T} \\ y_2 = f_c \text{ if } ((f_{b\,.f_{b2}}) \notin f_d) - - - - - - \text{T} \\ y_3 = Suspect\ User, Deny\ Access \end{cases} \quad (3)$$

Where;

c = Customer

f_n = Customer's sort function

f_c = function for expected sort outcome

f_b = function for customer's BVN in the BVN database

f_{b2} = function for customer's biometrics input in the cause of operation

f_d = function for BVN database

$\in$ = Is an element of

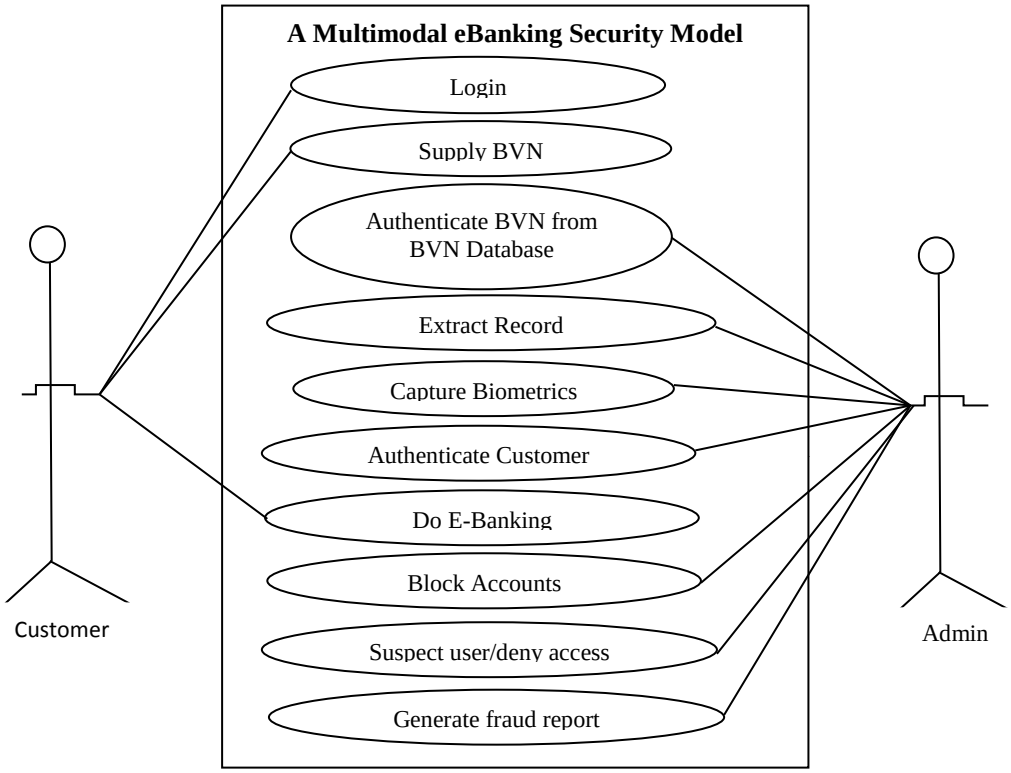
$\notin$ = Is not an element of

The function in equation (2) collects the customer's BVN and current biometrics which are authenticated using the BVN database. On successful authentication, access is granted to the customer for e-banking operations.

The function in equation (3) considers a situation where the customer's BVN matches records in the BVN database, but the biometric authentication fails as well as a situation where both BVN and biometrics do not match any record on the BVN database. In either cases, the customer is branded a suspect, he is denied access to e-banking services and a comprehensive report is generated for management to take appropriate action while the suspected accounts linked to such BVN are blocked to forestall fraud.

3.2 System Design Specifications

A system use case and a quick-sort model have been adopted to simplify the system design. Figure 1 shows the use case model of the system, with the bank customer and the banking administrative control system as the actors.



The following are the activities carried out by the system.

i. The system collects a customer's BVN and verifies from the BVN database if such BVN exists. If it does, the corresponding data in the databases are extracted to the customer's page.
ii. The system captures the current biometrics (fingerprint, voice/facial image) of the customer and authenticates the customer's biometrics with the biometrics saved in the BVN database.
iii. On successful authentication, the customer is granted. If authentication fails, the customer is labelled a suspect, he is denied access, the accounts associated to either the BVN, or the biometrics observed are blocked, and a report is generated about him that is forwarded to management for interpretation and necessary action.

Figure 2 depicts the BVN database design for quick-sort and access.

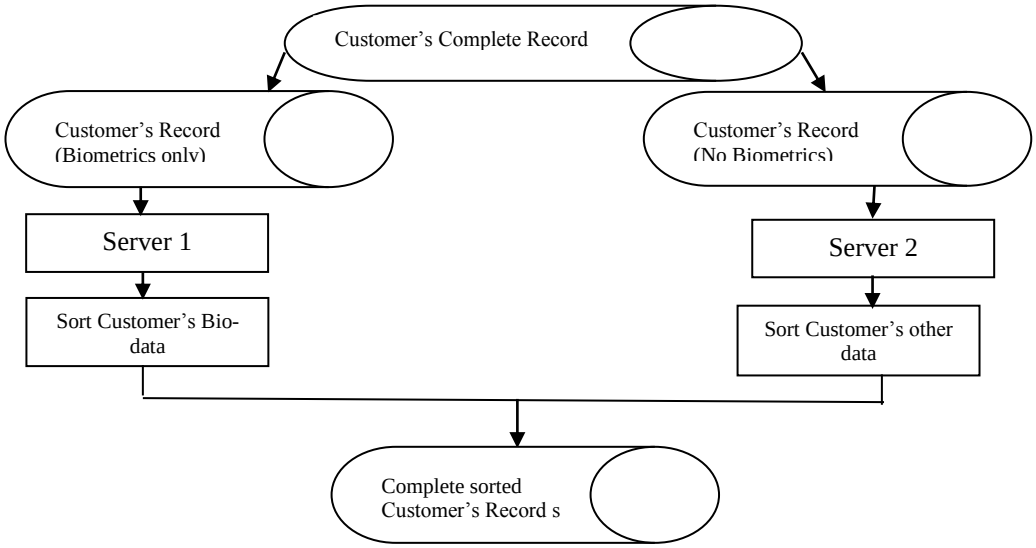


Figure 2: BVN Database Design for Quick Sort and Access

Figure 2 describes the following activities;

1. The customer's record during BVN registration is divided into two (his biometrics, and other records without biometrics).
2. The two records are saved in separate databases with a dynamic link to each other.
3. During login session, both records are sorted independently. The complete sorted record is presented on a customer's page for authentication and e-banking.

4. Results

The system was tested using some hypothetical banking transaction data.The program results after the system testing on a local host are displayed and explained in this section. Figure 3 shows the welcome screen where the bank administrator logs in. The interface shows two controls which allow the administrator to provide his username, password and biometrics to be able to gain access to the eBanking platform.

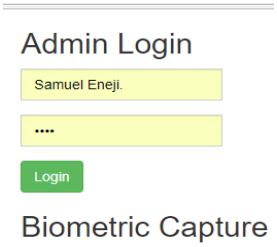


Figure 3: Admin Login

A successful login and authentication show the admin dashboard as illustrated in figure 4

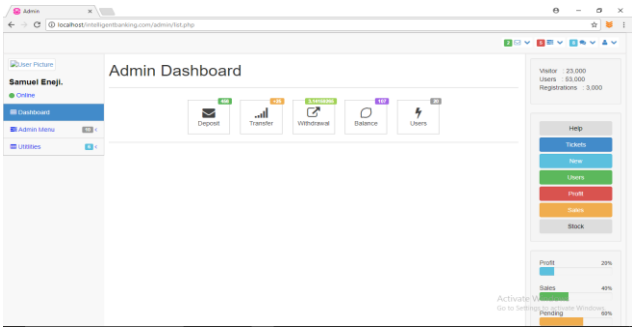


Figure 4: Admin Dashboard

A failure in login and authentication generates a report of a fraud instance as shown in Figure 5.

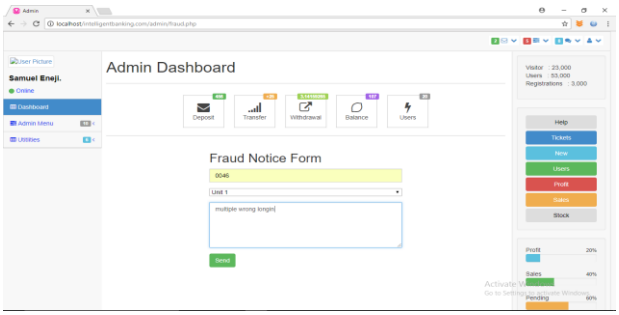


Figure 5: Fraud Notification Window

A successful authentication leads the user to the Internet banking platfoorm as illustrated in Figure 6.

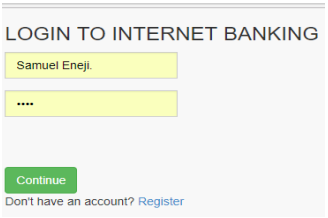


Figure 6: Customer's E-Banking Platform Testing

The customer can create a new Internet banking account as a fresher, or login with his identity (account number) and biometrics for authentication and clearance to access his or her account. An instance of a customer's biometric authentication dashboard is illustrated in figure 7.

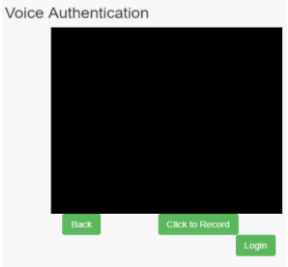


Figure 7: Biometric Authentication (Voice)

On successful authentication, the customer is logged in to the customer dashboard for further transacrions such as withdrawals, account balance checking, etc. as shown in Figure 8.

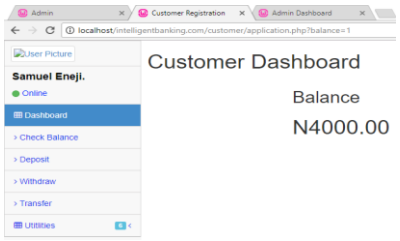


Figure 8: Customer's Dashboard (Checking Balance)

Even while in session, if a customer wants to perform another transaction, he must be re-authenticated to avoid session hijack. A failure in such re-authentication can make the customer's transaction attempt to be unsuccessful even if he is the administrator as illustrated in Figure 9.

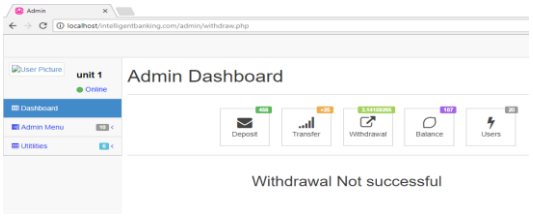


Figure 9: Unsuccessful Transaction Dashboard

An unsuccessful transaction can lead to the generation of a fraud analysis report as shown in Figure 10.

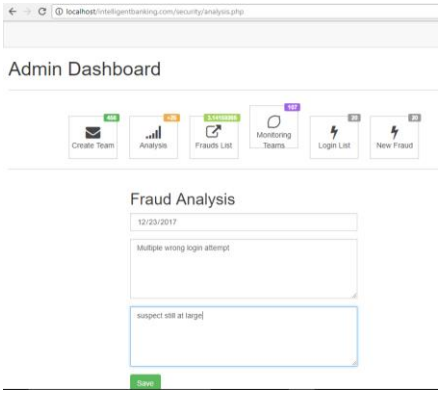


Figure 10: Fraud Analysis Dashboard

A suspect is reported with adequate geographical cordinates with the map location for tracing and apprehension as shown in Figure 11.

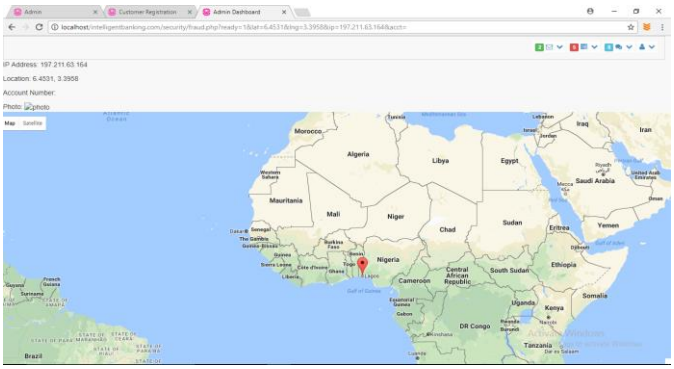


Figure 11: Geo-Location of a Suspected Fraudster.

The test result is summarized in tabe 18 below;

5. Conclusions

This study has proposed a security model that is homogeneously integrated with the electronic banking application to aid fraud mitigation by adopting a strategy to uniquely identify any user of the electronic banking application such that, the real owner of any bank account is the one given access to his account no matter what fraudsters may do. The model has a smart application of biometrics with other security parameters like the BVN and password, making it a multimodal eBanking security system capable of denying access to unauthorized persons, blocking accounts where fraud is suspected and reporting the suspect for further actions.

The model is recommended for implementation in electronic banking transactions, and further work can be extended on the model to incorporate electronic banking crime investigation and prosecution.

References

[1] Oluduro, O.F. (201). History and Evolution of Banking in Nigeria. ACADEM ARENA, 9-14. Retrieved from https://biblio.ugent.be/publication/5991963 on 15-12-2019

[2] Ogunleye, G. O., Fashoto, S. G., Andile, M. and Ogunde, A. O. (2017). Development of an Online Bank Verification Number System Using Linear Congruential Algorithm. *Information Technology Journal, 16: 62-70*

[3] Onu, F.U., Umeakuka, C. V. and Eneji, S. E. (2017). Computer Based Forecasting in Managing Risks Associated with Electronic Banking in Nigeria. Journal of Innovative Research and Advanced Studies (IJIRAS), 4(3), 390-396.

[4] Adewale, A. A., Ibunni, A. S., Badejo, J. and Odu, T. (2014). Biometric Enabled E-Banking in Nigeria: Management and Customers' Perspectives. Journal of Information and Knowledge Management, 4(11), 23-28.

[5] Amtul, F. (2011). E-Banking Security Issues – Is There A Solution in Biometrics? Journal of Internet Banking and Commerce, 16(2), 1-9.

[6] Aleksandar, L. (2015). Benefits and Security Threats in Electronic Banking. International Journal of Management Studies and Research (IJMSR), 3(6), 44-47.

[7] Bilal, A.S. and Rajimohan, P. (2015). Internet Banking, Security Models and Weaknesses. International Journal of Research in Management and Business Studies (IJRMBS), 2(4), 17-22.

[8] Adesuyi, F., Adepoju, S. and David, R. (2013). A Survey of ATM Security Implementation within the Nigerian Banking Environment. Journal of Internet Banking and Commerce, 18(1), 1-16.

[9] Beranek, L and Jiri, K. (2013).The Use of Contextual Information to Detection of Fraud on Online Auctions. Journal of Internet Banking and Commerce, 18(3), 1-17.

[10] Sarma, G. and Pranav, K. (2010). Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. International Journal of Pure and Applied Sciences and Technology, 1(2), 67-78.

[11] Peotta, H.B. and David, D. (2011). A formal Classification of Internet Banking Attacks and Vulnerabilities. International Journal of Computer Science & Information Technology, 3(1), 186-197

[12] Sarma, G. and Pranav, K. (2010). Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. International Journal of Pure and Applied Sciences and Technology, 1(2), 67-78.

[13] Sharaaf, N. A., Haamid, M.N., Samarawickrama, S.S., Gunawardhane, C.N., Kuragala, K.R.S.C.B and Dhishan, D. (2016). Improved E-Banking System With Advanced Encryption Standards And Security Models. International Journal of Scientific and Technology Research, 5(10), 22-27.

[14] Akinola, K.E, Ehiwe, D.D. and Somefun, O.M. (2016). Secured Models for Online Bank Vulnerabilities in Nigeria. IOSR Journal of Mobile Computing & Application, 3(5), 25-31.