Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute InformingScience.org

IJIKM.org

Volume 13, 2018

MULTILEVEL AUTHENTICATION SYSTEM FOR STEMMING CRIME IN ONLINE BANKING

Boniface Kayode Alese *	The Federal University of Technology, Akure, Nigeria	bkalese@futa.edu.ng
Aderonke F. Thompson	The Federal University of Technology, Akure, Nigeria	afthompson@futa.edu.ng
Olufunso D. Alowolodu	The Federal University of Technology, Akure, Nigeria	odalowolodu@futa.edu.ng
Blessing Oladele	The Federal University of Technology, Akure, Nigeria	blessemol@gmail.com

*Corresponding author

ABSTRACT

Aim/Purpose	The wide use of online banking and technological advancement has attracted the interest of malicious and criminal users with a more sophisticated form of attacks.
Background	Therefore, banks need to adapt their security systems to effectively stem threats posed by imposters and hackers and to also provide higher security standards that assure customers of a secured environment to perform their financial transactions.
Methodology	The use of authentication techniques that include the mutual secure socket layer authentication embedded with some specific features.
Contribution	An approach was made through this paper towards providing a more reliable and complete solution for implementing multi-level user authentication in a banking environment.
Findings	The use of soft token as the final stage of authentication provides ease of management with no additional hardware requirement.
Recommendations for Practitioners	This work is an approach made towards providing a more reliable and complete solution for implementing multi-level user authentication in a banking environment to stem cybercrime.
Recommendation for Researchers	With this approach, a reliable system of authentication is being suggested to stem the growing rate of hacking activities in the information technology sector.

Accepted by Editor June Lu | Received: November 27, 2017 | Revised: February 24, March 29, April 2, April 26, 2018 | Accepted: May 23, 2018.

Cite as: Alese, B. K., Thompson, A. F., Alowolodu, O. D., & Oladele, B. (2018). Multilevel authentication system for stemming crime in online banking. *Interdisciplinary Journal of Information, Knowledge, and Management*, *13*, 79-94. https://doi.org/10.28945/4063

(CC BY-NC 4.0) This article is licensed to you under a Creative Commons Attribution-NonCommercial 4.0 International License. When you copy and redistribute this paper in full or in part, you need to provide proper attribution to it to ensure that others can later locate this work (and to ensure that others do not accuse you of plagiarism). You may (and we encourage you to) adapt, remix, transform, and build upon the material for any non-commercial purposes. This license does not permit you to use this material for commercial purposes.

Impact on Society	This work if adopted will give the entire populace confidence in carrying out online banking without fear of any compromise.
Future Research	This work can be adopted to model a real-life scenario.
Keywords	multilevel-security, authentication, soft-token, cybercrime

INTRODUCTION

The unending nature of technological developments has greatly increased consumers access to internet services, which is more evident in the area of online banking. As commercialization of the Internet evolved in the early 1990s, traditional "bricks and mortar" (physical presence) banks began to investigate ways of delivering limited online services to reduce operating costs (Karim, Karim, & Rezaul, 2009). The success of these early efforts led many banks to expand their internet presence with improved websites that featured the ability to open new accounts, download forms, and process loan applications. This is very convenient for consumers and the ready access to the Internet in all advanced countries, coupled with the cost savings from closing bank branches, drove the deployment and adoption of these services (Gunajitand & Pranav, 2010).

However, with cybercrime, online banking is faced with a lot of security challenges. Online banking can be carried out from locations where there is a computer with Internet access, at any point in time. In spite of the great benefits of online banking, the number of malicious applications and security problems of online banking transactions has increased dramatically in recent years. This represents a challenge, not only to the customers who use such facilities but also to the institutions offering them (Dixit, 2016). The safe and secure environment of computer technology is the most important concern of all financial service organizations. Sunday and Emmanuel (2013) carried out a study that showed that about one fifth of some sampled customers have little trust in their Nigeria banks while a quarter are at the average level of trust (neither high nor low). The study shows further that one of the most likely reasons for this variation is network reliability in the banking industry. Most of the sampled customers responded that the banking sector operates with an unreliable network. Another likely reason for the variation in the level of trust, as discovered from the study, is cash deduction from account without any cash withdrawal while using ATM. This is a common observation among customers of various banks in Nigeria. It is therefore not a surprise that most sampled customers concluded that Nigeria banking system is not stable enough for e-banking and insecurity in the financial institutions is a major obstacle to electronic banking. Obviously, the banking industries in Nigeria have more responsibilities on their shoulders as far as information technology security and e-banking are concerned in the sector. Emeka and McChester (2015) also noted that the main problem with Internet banking has been that of securing the system from unauthorized access. The study further revealed that there have been concerns about customers' knowledge of the system's operation and use. Most customers are still oblivious of the security challenges associated with this service; as a result, the vulnerability of these customers to Internet banking attacks continues to grow. There have been cases of incomplete sign out from such systems by ignorant users, often leading to attacks resulting in heavy fund transfer from customer's account to an attacker's choice account. Therefore, security of information relating to online financial transactions is required to carry out a secure transaction. With regard to this issue, a multilevel authentication system is proposed to ensure the secure access and communication when performing financial transactions, making full use of sophisticated platforms provided by the increasing advancements in technology.

To recommend this multilevel authentication system, literature on the subject matter and very closely related past works are reviewed, methodology involved in the system design, comparison with other systems, with the existing models in the Nigerian banks are presented, followed by possible system implementation plan and potential contributions to online banking.

LITERATURE REVIEW

The subject of cybercrime has been a matter of discussion for close to three decades but, for the purpose of this paper, our review on the subject matter shall be limited to about a decade. Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails, including theft of government or corporate secrets through criminal trespass into remote systems around the globe (National Crime Prevention Council, 2012). In essence, cybercrime is a crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbolic or any other way, and transferred through local and global networks (Azeez & Osunade, 2009). Online Banking Fraud is the act of committing fraud or theft using online technology to illegally remove money from, or transfer it to, a different bank account. Alese, Iwasokun, Haruna, Thompson, and Otasowie (2014) divide cybercrime into four different categories: cyber-trespass, cyber-deceptions, and thefts, cyber-pornography, and cyber-violence. Online banking fraud is best fitted in the cyber-deceptions category. It is defined as "stealing (money, property), such as credit card fraud, intellectual property violations (that is 'Piracy')". Anderson et al. (2012) differentiate online banking fraud from card fraud while both target financial systems and banks. The authors argue that in online banking fraud only customers and banks suffer while this is different in the case of card fraud where merchants also suffer from the fraudulent activity. However, multi-factor authentication is expected to sufficiently overcome the challenges posed by Anderson et al.'s (2012) proposition.

The unique aspect about information security in the banking industry is that the security posture of a bank does not depend solely on the safeguards and practices implemented by the bank, it is equally dependent on the awareness of the users (Data Security Council of India, 2011). The biggest threat to online banking is still malicious code executed carelessly on the end-user's computer. Banks should also publish on website, security tips along with their security policy for online banking, so users should always use those tips before going for any transaction. In order to ensure that bank security measures are not undermined by manipulation, it is essential that customers take steps to protect their devices ensuring the security paradigm employed.

According to RSA Whitepaper (2009), Multi-channel Approach (MCA) of authentication provides protection against most real-time attacks including Man-In-The-Middle attacks, Real-time Transport Protocol (RTP) attacks and malwares. Some of these attacks have the ability to capture and manipulate data that is being exchanged between users (customers) and the online services (online banking application) in real time, and this could be considered as a global threat with the aim of financial gain. It is worthy to note that various authors have proposed different security mechanisms to avert the activities of cybercrime in the banking industry; however, there has always been counter efforts from the hackers and crackers quarters. Stallings (2010, 452-469) explained Kerberos as a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove the identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Naik and Koul's (2013) authentication schemes suffer from many weaknesses. Textual passwords are widely used; however, users tend to choose meaningful words from dictionaries. This makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords face lack of space. Smart cards or tokens can be lost or are prone to theft. Many biometric authentications have been proposed but users tend to resist using them because of their intrusiveness on their privacy. Kim, Kim, and Kim (2007) proposed that security is the most important thing in the pervasive environments. The personal information is identified by the malicious user. Some of the drawbacks are involved in the UPnP architecture. They are user authentication, and service access control. These are all not suitable in the pervasive environments. A study done by Moore and Clayton (2007) indicates that some banks are targeted much more frequently than others. Hastings and Dodson (2004) defined authentication as the process of confirming someone's identity in terms of claimants, relying parties, and verifiers. A

claimant is the individual claiming to be the rightful user to use services and resources. A relying party is the provider of the services and resources needed by the users. A verifier is another individual or an automated system which verifies the delivery medium that exchanges data between the user and the service provider. Therefore, for an attacker to gain full access to a user's account, all channels involved must have been compromised. Sabzevar and Stavrou (2008) presented some authentication techniques using a graphical password, where the second authentication stage involves decoding of password using the user's device. The password, however, is represented by an image, and the user is expected to decode it by locating the suitable clicks and their order on the image which are given only through the user's device. De Cristofaro, Du, Freudiger, and Norcie (2014) categorized authentication factors into three: (i) knowledge factors, the most used authentication technique such as passwords, PIN, secret questions, where only the user knows the answer, (ii) possession factors, hardware authentication technique such as tokens, (iii) inherence factors, authentication techniques based on the biometric attributes of the user, such as fingerprint, retina and voice.

Therefore, as Alese et al.(2014) categorized online banking fraud under cyber-deceptions, and Naik and Koul (2013) noted that singular use of authentication schemes suffer from many weaknesses, inline with Kim et al.'s (2007) proposal about the importance of security in the pervasive environment, it is evident, according to RSA Whitepaper (2009), that the use of multiple factors and multiple channels of authentication provides a better security against most real-time attacks and crimes in online banking.

AUTHENTICATION

There are a number of approaches to stem online banking fraud such as using Hidden Markov Model (HMM) decision support system and many other ones (Kovach & Ruggiero, 2011; Mhamane & Lobo, 2012; Ogunleye, Adewale, & Alese 2012). An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. Multifactor authentication (MFA, also referred to as multi-level authentication) is a system whereby two or more different factors are used together for authentication (Central Bank of Nigeria, 2003).

Mutual authentication

Mutual authentication is a process of customer identity authentication, and the target website is authenticated to the customer. Most financial institutions do not adopt mutual authentication when retrieving sensitive information from their customers. One reason phishing attacks are successful is that unsuspecting customers cannot determine if they are being directed to spoof websites during the processing stage of an attack. The spoof sites are designed in a way that users cannot doubt their authenticity. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a website vary. The use of digital certificates coupled with encrypted communications (e.g., Secure Socket Layer (SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks (Federal Financial Institutions Examination Council [FFIEC], 2009).

One of the most popular and older remote user authentication schemes was suggested by Lamport (1981) in which the server stores the hashed value of a user's password which can be compromised, stolen, or modified by an adversary, then the system could be partially or completely compromised. Hao, Zhong, and Yu (2011), proposed a Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing which generates a ticket for a user which was user specific. The additional security measure is given to protect the ticket from modification (Jaidhar, 2013). The identified flaw in Hao et al. (2011), is the fact that the scheme was non-resistant to DoS (Denial of Service) attack during the registration phase and change password phase. The author has improved on this scheme by

applying mutual authentication. This proposed scheme inherited the security measure of previous scheme and is resistant to DoS Attack. The scheme is using a smartcard, which needs an extra device to read/write it and increases the cost of implementation.

In online banking, security of information is required to carry out secure transactions. Information relating to online financial transactions includes individual authentication parameters and some other account related information. Various techniques are used in authentication which include username-passwords, textual passwords, graphical passwords, biometric face recognition, public key transfer and symmetric key based authentication, 3D password, and so on. Each of these techniques has its own advantages and disadvantages (Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005).

Jaidhar (2013) authentication schemes suffer from many weaknesses. Textual passwords are widely used; however, users tend to choose meaningful words from dictionaries. This makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords face lack of space. Smart cards or tokens can be lost or are prone to theft. Many biometric authentications have been proposed, but users tend to resist using them because of their intrusiveness on their privacy. The three dimensional (3-D) password is a multifactor authentication scheme; it combines most of the existing authentication schemes such as textual passwords, graphical passwords, and biometrics into a single virtual three-dimensional environment. The combination of all the actions and inputs towards the virtual three-dimensional environment constructs the user's 3D password. A simple approach for a secure authentication is to use one or more of the above-mentioned authentication techniques in combination for multi-level authentication so that the probability of breaking such a password is reduced to a large extent. Hence, multi-level authentication technique can be used for ensuring a more stringent authentication.

Related works

A few studies proposed security schemes that are characterized by the multi-factor authentication. These are not field-specifics; however, they could be employed as tradeoffs with respect to storage and speed as desired in the sought field or application. These studies are particularly reviewed as follows.

Closely related to this research work is a study carried out by Weir, Douglas, Richardson, & Jack (2010), where the usability of passwords and two other methods of two-factor authentication: codes generated by tokens and PINs received through text message were analyzed. A lab study was carried out where 141 users were requested to give report on the usability of the three methods of authentication using 30 proposed questions. It was concluded by the authors that familiarity with a technology (rather than perceived usability) affected the users' willingness to adopt a given authentication technology. It was further shown that users preferred the one-factor method of authentication (on which the average user had the most experience) as the most secure and convenient option.

Inglesant and Sasse (2010) carried out a study and analyzed "password diaries", that is they requested users to record the times they did password authentication, and realized that frequent changes in password is burdensome, and users do not see the need to change their passwords except they are forced to do so, which is difficult to create a secure and memorable password, adhering to the policy governing the creation of password. The authors therefore concluded that the context of use of a password has an important role to play on the ability of the users to become used to complex passwords and its usability.

Gunson, Marshall, Morton, & Jack (2011) studied the usability of single and two-factor authentication in automated telephone banking. A survey involving 62 users was presented in which participants were requested to rate their experiences using a set of 22 usability-related questions, and it was concluded, according to their analysis, that two-factor authentication was perceived to be more secured, but less usable, than simple passwords and PINs. In the same year, the Post-Quantum Cryptography based security framework proposed by Gabriel, Alese, and Adetunmbi (2011) gave a tech-

nique of combining cryptography and steganography as a tool for enhancing the security of communications and computations in the cloud. This framework is an improvement on the integer factorization and discrete logarithm by enhancing quantum computer bits.

Bonneau, Herley, van Oorschot, and Stajano (2012), without carrying out any user study, evaluated authentication models which includes plain-passwords, open ID, security tokens, and phone-based tokens. They employed a set of 25 subjective factors: 8 measured usability, 6 measured ability to deploy, and 11 measured security. It was concluded that none of the existing authentication schemes performs the best in all metrics, and the models that could be categorized as two-factor authentication performed better than passwords in security but worse in usability.

Alese et al. (2014) proposed a software piracy prevention technique in which client/user purchases a software product but must connect to the remote server of the software developer before installation. The user is provided with an activation code that is activated through mobile agent. The validity of the activation is checked, the software user identity information is compared with stored information in the database of the developer to ascertain authenticity and to prevent privacy.

Abhaysingh, Mangesh, and Pranali (2015) proposed a system in which behavior biometric can provide a better alternative for traditional password methods and also for physiological biometrics, due to the fact that they are very economical and easy to integrate with existing system. Various approaches have been made towards enhancing and improving the performance of keystroke dynamics system. The aim was to deal with all the possible uncertainties which can lead to the degradation of the overall system accuracy and performance. The entire authentication system is divided into several modules, each of which is responsible for improving the overall system performance. Providing keystroke-based verification in addition with the password, helps to reduce the False Acceptance Rate (FAR). FAR is the probability that the system incorrectly authorizes a non-authorized person, due to incorrectly matching the biometric input with a template. The FAR is normally expressed as a percentage, following the FAR definition this is the percentage of invalid inputs which are incorrectly accepted. The security question and answer make the system more flexible to access in case of unmatched keystroke behavior. Adaptive learning module takes care of the changing nature of human and reflects the most recent behavior during matching. This helps to reduce the False Rejection Rate (FRR). FRR is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template. The FRR is normally expressed as a percentage, following the FRR definition this is the percentage of valid inputs which are incorrectly rejected. If the user is unable to generate the matching keystroke template due to some psychological or physical problems, alternate authentication can be done using one-time passwords generated from emails or cell phones. The user's session can be later monitored to maintain the authenticity during the entire session.

Yugha, Uma, Swarnalatha, and Poovizhi (2015) proposed a multi-level authentication system for providing security. The system uses image-based passwords and integrates image registration and authentication. Currently, multilevel authentication is inevitable in mobile phones, systems, and online applications. The proposed system is an image-based 3-level authentication system. The first level is the registration process and the second level is image-based authentication, while the third level is the alias email verification. The users are directed to pass the image selection, only if they choose the correct type. Hence, it cannot be guessed, and this strengthens the security (Yugha et al., 2015).

A study done by Nivethithai and Parijathan (2016) shows the novel possibility introduced by biometrics to define a protocol for continuous authentication which enhances the security of user session. The proposed protocol works with features, templates, or raw data. The prototype only performs some checks on face recognition, where only one face is considered for identity verification, and the others deleted. The client device uses part of its sensors extensively through time and transmits data on the Internet. This introduces the problem of battery consumption, which could not be quantified. Also, the frequency of the acquisition of biometric data is fundamental for the protocol usage; if

biometric data are acquired too sparingly, the protocol would be useless. This mostly depends on the profile of the client and consequently on the usage of the device (Nivethithai & Parijathan, 2016).

Integrating the contributions from the previous studies, a multi-level authentication system is proposed as an attempt to solve the identified security issue in the online banking systems in Nigeria.

SYSTEM DESIGN

THE PROPOSED SYSTEM

The architecture of the proposed multi-level authentication system is presented in Figure 1. The architecture uniquely combines different authentication techniques used by other banks. It provides a robust platform for authentication with the deployment of operator challenge which is not in any other existing systemin the financial institutions. The system requires each user to register their accounts online, which is connected to their bank account numbers generated by the bank. However, the online authentication system consists of mutual authentication, password authentication, operator challenge, and soft token authentication, which enables secure communication between the user and the online bank server. When this level of authentication is completed, the user is posed with a basic operator challenge based on the user's specifications during registration. Also, successful completion of the operator challenge authentication level requests the user to enter a code generated (based on Diffie Hellman's algorithm) from the user's soft token, before full access to the system is granted.

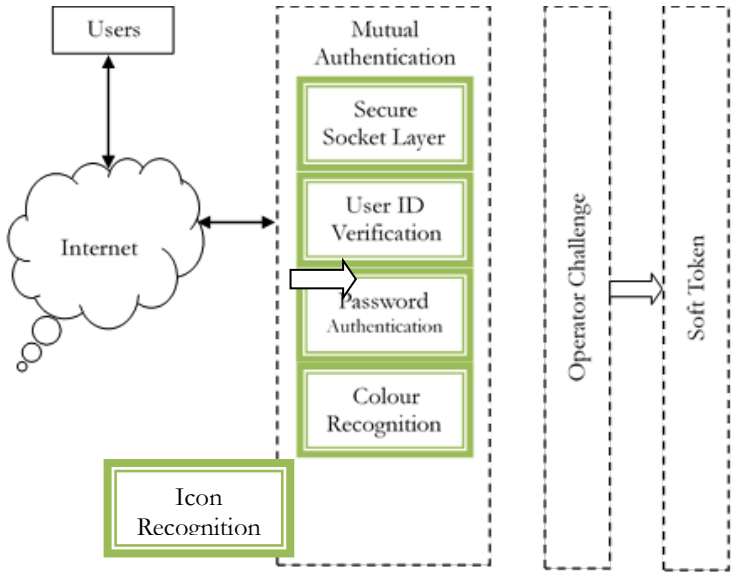

Figure 1: The Secure Bank System Architecture

Mutual authentication

Mutual authentication is a process of customer identity authentication, and the target website is authenticated to the customer. At this level, the client and the server authenticate each other by verifying the provided digital certificate so that both parties are assured of each other's' identity. The processes contained in the mutual authentication level are secure socket layer authentication, user ID verification, colour recognition and icon recognition.

Secure socket layer

The process of authenticating and establishing an encrypted channel using secure socket layer based on mutual authentication involves the following steps:

(i). A client requests access to a protected resource.

(ii). The server presents its certificate to the client.

(iii). The client verifies the server's certificate.

(iv). If successful, the client sends its certificate to the server.

(v). The server verifies the client's credentials.

(vi). If successful, the server grants access to the protected resource requested by the client.

The client and server use 12-handshake messages to establish an encrypted channel before message exchanging as shown in Figure 2

Figure 2: The 12 handshake messages

User ID verification

The user ID verification stage requests the client to input the user ID obtained at the point of registration, and this is compared with user IDs stored in the server's database. If there is a match, the server returns a successful message; else, the server returns an error message indicating that the user ID does not exist.

Icon recognition

After successful user ID verification, the unique icon specified by the user at the point of registration is displayed to the user to ascertain the validity of the intended website. This icon serves as the user's unique icon which is used to visually authenticate the webpage whenever the user is connected.

Password authentication

Client authentication needs security for remote login while the client program tries to communicate with the server program over insecure networks such as the Internet. The user identity and the secret password are used for authentication and access control. To combat the possibility of password compromise during transmission, the password authentication approach employs the use of public key encryption, private key encryption, and hash function.

The password authentication protocol steps are:

Step 1. Client → Server: id, {rc, pw}Ks

Step 2. Server → Client: rc, rs, H(rs)

Step 3. Client → Server: id, H(rc, rs)

Step 4. Server → Client: Access Granted/Denied

Where id is the client's username, pw is client's password, rc is random number (client), rs is random number (server), Ks is public key, H is hash function

The server stores H (pw) instead of pw, to protect the password. During the password authentication, a client selects a random number rc and encrypts rc and pw with server's public key Ks and sends the same with client's id to the server as stated in step 1. The server decrypts (rc, pw)Ks using its own private key and retrieves rc and pw, then compares hashed result of extracted pw with H(pw), which is stored in the server's database. If the result is matched, then the server selects a random number rs, compute rc⊕ rs and sends back the computed rc⊕rs and H(rs) to the client. After receiving rc⊕rs, H (rs) from the server, the client XORs rc with rc⊕ rs and retrieves rs. The client compares if the hashed value of retrieved rs and received H(rs), depending on this condition client computes the authentication token H(rc, rs) and sends back id, H(rc, rs) to the server. Therefore, the server computes H(rc , rs) using its own copies of rs and rc and compares with received H(rc, rs). If it is matched, then the server sends a message 'Access granted' otherwise send an error message: 'Access Denied' to the client.

Soft token authentication

The soft token is stored on a general-purpose computer such as a desktop, laptop, or mobile device; and requires activation through a second factor of authentication (PIN – Personal Identification Number) which is stored on the remote server. If there are attempts made to guess the PIN, it will be detected and logged on the server, which will disable the token.

Using the Diffie-Hellman key exchange method, the token client generates its key pair and exchange public keys with the server. The method allows two parties (token client and server), which have no prior knowledge of each other to jointly establish a shared secret key over a communication channel. The protocol uses a multiplicative group of integers modulo p (unique to both users – token client and server), where p is prime, and g is primitive root mod p.

The steps involved are as follow:

Token client and Server has a unique large prime p and a nonzero integer g modulo p. They can make both the values of p and g known. The chosen value of nonzero integer g is such that its order in F*p is a large prime.

Token client picks a secret integer a, which is kept secret, while at the same time server picks an integer b, that is also kept secret. Server and Token client use their secret integers to compute equations 1 and 2

$$A \equiv g^a (\text{mod } p) \qquad 1$$

$$B \equiv g^b (\text{mod } p) \qquad 2$$

They next step is to exchange these computed values; a Token client sends A to Server and Server sends B to Token.

Finally, Server and Token again use their secret integers to compute equations 3 and 4.

$$A' \equiv B^a (\text{mod } p) \qquad 3$$

$$B' \equiv A^b (\text{mod } p)$$

The values computed, A' and B' respectively, according to exponential law, are the same, since

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' (\text{mod } p) \qquad 4$$

This common value is the exchanged key which is used to establish a secure communication between the client and the bank server.

User registration

This is the stage where the user creates an online account with the bank (Figure 3). The creation of the online account has some processes that include the following.

The new user initiates the online account registration by validating the user account number with the bank.

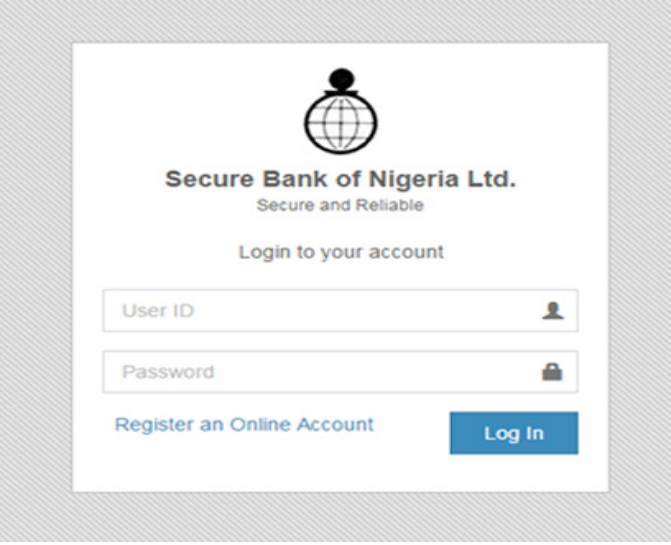

Figure 3: Registration of an online Account

New User Registration Form

After the process of user account number validation is successful, the user then fills an online registration form (Figure 4). The form required fields include the date of birth, gender, secret question, secret answer, unique color, unique icon, operator selection, password to the online account, and soft token password.

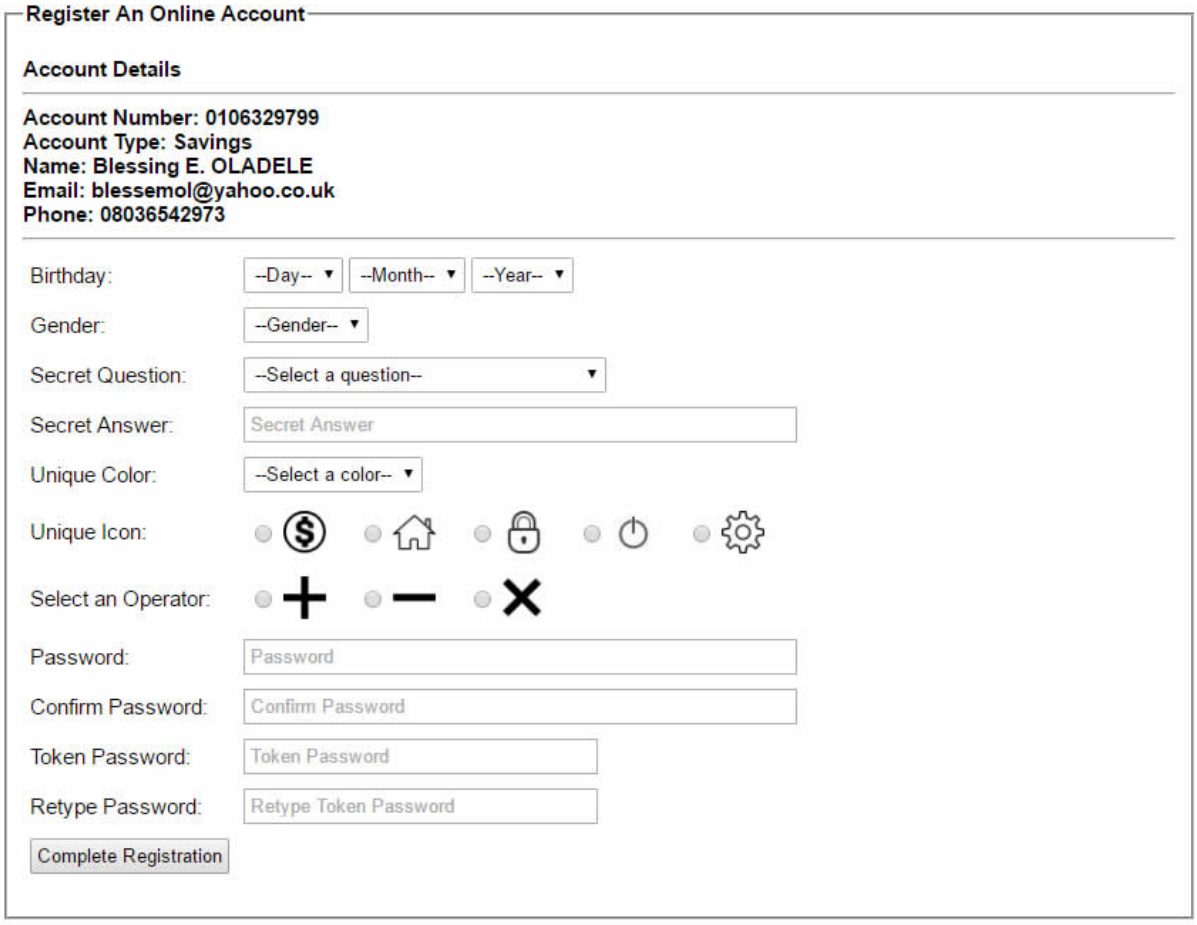

Figure 4: New User Registration Form

DISCUSSION

This section will compare the proposed multi-level authentication system with those proposed in previous studies, compare our proposed system with those already in use in the online banking services in Nigeria, and then elaborate on some potential contributions.

COMPARISON WITH RELATED WORKS

Table 1 shows the comparison of the proposed system to those in other related works. The table identifies the variability in the authentication systems proposed by different authors and the uniqueness of the multi-level authentication system proposed in this work. The proposed system uses public key encryption that projects a higher level of security than any other system which uses storage of hashed user's password, use of textual password, sending passwords through user's mobile phone and email, and plain storage of passwords on the server that could be easily compromised. The proposed system also incorporates colour recognition, icon recognition, operator challenge, which are

not employed in any of the other systems, except the one in the study by Abhaysingh and his colleagues (2015). Their system relied on proposed security question and answer in authentication which could be easily guessed by the user's close associate. Our proposed system is free of that type of potential weakness.

Table 1: Comparison with Existing Works

	Lamport (1981)	Naik & Koul (2013)	Kim et al. (2007)	Yugha et al, (2015)	Abhaysingh et al. (2015)	Proposed System
Password	Stores only the hashed value of the user's password on the server	Use of textual passwords	Passwords generated are sent through user's mobile phone	Passwords are sent to the user's email which can be compromised	Users' passwords are plainly stored on the server	Uses public key encryption and hash function to store the password specified by the user
Colour Recognition	Does not implement colour recognition in the authentication process	Does not implement colour recognition in the authentication process	Does not implement colour recognition in the authentication process	Does not implement colour recognition in the authentication process	Does not implement colour recognition in the authentication process	Uses colour recognition as part of the authentication process
Icon Recognition	Does not implement icon recognition in the authentication process	Does not implement icon recognition in the authentication process	Does not implement icon recognition in the authentication process	Does not implement icon recognition in the authentication process	Does not implement icon recognition in the authentication process	Uses icon recognition as part of the authentication process
Operator Challenge	Does not implement operator challenge in the authentication process	Does not implement operator challenge in the authentication process	Does not implement operator challenge in the authentication process	Does not implement operator challenge in the authentication process	Uses security question and answer in authentication which can be guessed by an attacker	Uses operator challenge in the authentication process, which is difficult to guess by an attacker as it involves basic calculation

Comparison with Existing Models in Nigerian Banks

Table 2 shows the comparison of the authentication systems in Nigeria online banking services. The table identifies the variability in the authentication systems provided by the banking institutions and the uniqueness of the multilevel authentication system. The proposed system combines different factors to complete the authentication process. The factors include mutual authentication, password

authentication, operator challenge, icon recognition, colour recognition and soft token authentication. However, none of the top ten most commonly used banks as indicated by Adeniyi (2017), combines all the factors of authentication as indicated by the proposed system.

Table 2 Authentication Systems in Online Banking Providers in Nigeria

Banks	**Mutual Authentication**	**Username and password**	**Operator Challenge**	**Icon Recognition**	**Colour Recognition**	**Soft Token**
Proposed System	Yes	Yes	Yes	Yes	Yes	Yes
Zenith Bank	Yes	Yes	No	No	No	No
First bank of Nigeria	Yes	Yes	No	Yes	No	Yes
Guaranty Trust Bank	Yes	Yes	No	No	No	No
Access Bank	Yes	Yes	No	Yes	No	No
Diamond Bank	Yes	Yes	No	No	No	Yes
Ecobank Nigeria	Yes	Yes	No	No	No	No
Union Bank of Nigeria	Yes	Yes	No	No	No	Yes
Fidelity Bank Nigeria	Yes	Yes	No	No	No	No
Sterling Bank Plc	Yes	Yes	No	No	No	Yes
First City Monument Bank	Yes	Yes	No	No	No	Yes

Potential contributions

This proposed mulita-level authentication system is divided into several levels, each is responsible for improving the overall system security. Providing mutual authentication by employing colour recognition, icon recognition, user ID verification, in addition to the secured socket layer, helps to stem crime in an online banking environment. These procedures will help the populace- literate and non-literate in information technology. The operator challenge makes the system more secured from attackers as it requires the user to perform a simple but effective calculation on what the user knows (a mathematical operator). Encrypted and hashed password authentication level takes care of network eavesdroppers who may be listening on the user's internet connection to retrieve passwords (Wall, 2001), as the passwords employ public key encryption and hash function to secure the password. The use of the soft token as the final stage of authentication provides ease of management with no additional hardware requirement. Therefore, our proposed system is an approach made towards providing a more reliable and complete solution to implementing multi-level user authentication in a banking environment to stem cyber-crime. Consequently, the research provides a model and software that can stem cyber-crime in online banking system more effectively. It should prove to be a practical security solution to be adopted by the online banking providers in Nigeria. Moreover, it should also add value to the literature of information security.

CONCLUSION

This study proposes an approach towards providing a more reliable and complete solution for implementing multi-level user authentication in a banking environment to stem cyber-crime. The proposed architecture can be easily tested and implemented by any online banking service provider in Nigeria in their existing security architecture, with introduction of little modification to avoid high level attacks as the security architecture should be classified documentation which third parties should not be privy to at any level. The order of authentication levels can be re-arranged, the scope of variables, operators and channels used can be widened for each level of authentication.

REFERENCES

Abhaysingh, S., Mangesh, B., & Pranali, K. (2015), Multi-level user authentication via keystroke dynamics. *International Journal of Computer Science and Mobile Computing.4*(10), 239-245.

Adeniyi A. (2017). List of best top 10 banks in Nigeria and net worth. Retrieved from https://www.reviewcious.com/list-of-banks-in-nigeria

Alese, B. K., Iwasokun, G., Haruna, D., Thompson, A., & Otasowie, I. (2014) Game-based analysis of the network attack-defense interaction. *Proceedings of the World Congress on Engineering* (I) 2014.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). *Measuring the cost of cybercrime*. Workshop on the Economics of Information Security. Retrieved from https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Azeez, N. A., & Osunade, O. (2009). Towards ameliorating cybercrime and cybersecurity, *International Journal of Computer Science and Information Security, 3*(1).

Bonneau, J., Herley, C., van Oorschot, P. C., & F. Stajano, F. (2012) *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes*. In IEEE Symposium on Security and Privacy, 2012. https://doi.org/10.1109/SP.2012.44

Central Bank of Nigeria (2003). *Guidelines on electronic banking in Nigeria.*

Data Security Council of India. (2011). *State of data security and privacy in Indian banking industry*. DSCI-KPMG Survey-2010.

De Cristofaro, E., Du, H., Freudiger, J. & Norcie, G. (2014). *A comparative usability study of two-factor authentication.* 8th NDSS Workshop on Usable Security (USEC 2014) https://doi.org/10.14722/usec.2014.23025

Dixit, N. (2016). Acceptance of E-banking among adult customers: An empirical investigation in India. *Journal of Internet Banking and Commerce; 15*(2).

Emeka, N., & McChester, O. (2015). Security issues analysis on online banking implementations in Nigeria. *International Journal of Computer Science and Telecommunications, 6*(1).

Federal Financial Institutions Examination Council (FFIEC). (2001). *Authentication in an electronic banking environment.*

Gabriel, A., Alese, B. K., & Adetunmbi, A. O. (2011). Design and implementation of internet protocol security filtering rules in a network environment. *International Journal Computer Science and Information Security, 9* 7).

Gunajit, S., & Pranav, K. S. (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.

Gunson, N., Marshall, D., Morton, M., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security, 30*(4). https://doi.org/10.1016/j.cose.2010.12.001

Hao, Z., Zhong, S., & Yu, N. (2011). A time-bound ticket-based mutual authentication scheme for cloud computing. *International Journal of Computers, Communications, and Control; 6*. https://doi.org/10.15837/ijccc.2011.2.2170

Hastings, N. E., & Dodson, D. F. (2204). *Quantifying assurance of knowledge-based authentication*. The 3rd European Conference on Information Warfare and Security, 2004.

Inglesant, P. G., & Sasse, A. M. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of SIGCHI Conference on Human Factors in Computing Systems* (CHI 2010), 383–392. ACM.

Jaidhar, C. (2013). Enhanced mutual authentication scheme for cloud architecture. In *Proceedings of 3rd IEEE International Advance Computing Conference (IACC)*. https://doi.org/10.1109/IAdCC.2013.6514197

Karim, Z., Karim, M., & Rezaul, A. H. (2009). Towards secure information systems in online banking. *International Conference on Internet Technology and Secured Transactions*. https://doi.org/10.1109/ICITST.2009.5402619

Kim, J., Kim, Z., & Kim, K. (2007). A lightweight privacy preserving authentication and access control scheme for ubiquitous computing environment. *Proceedings of the 10th International Conference on Information Security and Cryptology*, Berlin, Heidelberg: Springer-Verlag; 37–48. https://doi.org/10.1007/978-3-540-76788-6_4

Kovach, S., & Ruggiero, W. (2011). Online banking fraud detection based on local and global behavior. In *ICDS 2011: The Fifth International Conferance on Digital Society,* 166–171.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), 770-772. https://doi.org/10.1145/358790.358797

Mhamane, S., & Lobo, L. M. R. J. (2012). *Fraud detection in online banking using HMM*. 2012 International Conference on Information and Network Technology (ICINT 2012), pp. 200 -204.

Moore, T., & Clayton, R. (2009). The economics of online crime. *Journal of Economics Perspectives; 23*(3), 3-20. https://doi.org/10.1257/jep.23.3.3

Naik, T., & Koul, S. (2013). Multi-dimensional and multi-level authentication techniques. *International Journal of Computer Applications*, *75*(12), 17-22. https://doi.org/10.5120/13163-0845

National Crime Prevention Council. (2012). *Annual report 2012*. Retrieved from http://www.ncpc.org.sg

Nivethithai, S., & Parijatham, R. (2016). Security of web-service using biometric authentication. *International Journal of Computer Science and Engineering* (SSRG-IJCSE).

Ogunleye G. O., Adewale O. S., & Alese B. K**.** (2012). An exploratory study on electronic retail payment systems: User acceptability and payment problems in Nigeria. *Proceedings of the 24th National Conference of the Nigeria Computer Society (NCS), Volume 23*.

RSA Whitepaper. (2009). *Making sense of man-in-the-browser attacks*. Available at http://viewer.media.bitpipe.com/1039183786_34/1295277188_16/MITB_WP_0510-RSA.pdf

Sabzevar, A. P., & Stavrou, A. (2008). Universal multi-factor authentication using graphical passwords. In the *Proceedings of the 2nd IEEE/ACM Workshop on Security and Privacy in Telecommunications and Information Systems* (SePTIS). December 2008, Bali, Indonesia. https://doi.org/10.1109/SITIS.2008.92

Stallings, W. (2010). *Cryptography and network security* (5th ed.). Prentice Hall.

Sunday, T., & Emmanuel, F. (2013). IT security and e-banking in Nigeria. *Greener Journal of Internet, Information and Communication Systems*, *1*(3), 61-65.

Wall, D. (2001). Cybercrimes and the Internet. In *Proceedings of 3rd IEEE International Security Computing Conference (ISCC)*. https://doi.org/10.4324/9780203164501_chapter_1

Weir C. S., Douglas, G., Richardson, T., & Jack, M. (2010). Usable security: User preferences for authentication methods in ebanking and the effects of experience. *Interacting with Computers, 22*(3). https://doi.org/10.1016/j.intcom.2009.10.001

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Basic results. In *Proceedings Human-Comput. Interaction Int*.

Yugha, R., Uma, S., Swarnalatha, S., & Poovizhi, M (2015). Multilevel authentication system for providing security. IPASJ *International Journal of Computer Science, 3*(3).

BIOGRAPHIES

Boniface Kayode Alese is a Professor of Cyber-Security and Cryptography at the Federal University of Technology, Akure, Nigeria.

Aderonke F. Thompson (Ph.D) is a Senior Lecturer in the Department of Computer Science, The Federal University of Technology, Akure, Nigeria. Her Area of interests are: Cybersecurity, Algorithms, Simulation and Modeling.

Olufunso D. Alowolodu is a Lecturer I in the Department of Computer Science, Federal University of Technology, Akure. She had her Ph.D in 2016 in Computer Science. Her area of specialization includes Cyber-Security, Cloud Computing, and Cryptography.

Blessing Oladele is a Principal Software Engineer at Federal University, Lokoja, Nigeria. He holds a Master degree in Computer Science.