IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 3, March 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

Four-Phased Security Model For Webbased Banking System

Samuel O. Okide (Phd.)
Department of Computer Science, Nnamdi Azikiwe Unversity, Awka, Nigeria.
E-mail: samuelokide@yahoo.com

Nnenna S. Nnam
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.
E-mail: staceyous@yahoo.com

ABSTRACT - Security has been a major factor militating against the increased adoption of web-based banking in Nigeria due to lack of trust and confidence in the web-based banking system as a result of fraudulent activities experienced by users of the system. In this study, the researcher implemented a four-phase security model for web-based banking system using username and password at the first phase, Software token at the second phase, fingerprint verification at the third phase and secret question and answer at the fourth phase, as authentication mechanisms. This study aims at increasing security and trust over the existing model which has only two-level authentication and to model an innovative approach to effective security in web-based banking system to reduce fraud and thus, remedy the deficiency and weakness of the existing system. In order to achieve the aim and objective of the study, an Object Oriented Analysis and Design Methodology (OOADM) was adopted. The implementation of the new system was done using PHP programming language and Mysql database as repository. The result of this study is a four-phase authentication security model that will promote trust and good relationship between online banks and their customers. The model ensures that only qualified people can access Internet banking accounts and that the information viewed remains private and cannot be modified by third parties. Hence, solving the repudiation problem faced with the present system.

Index Term- Authentication, Web-based banking, challenge-response authentication, Fingerprint, Software token code.

1. INTRODUCTION

The new millennium brought with it new possibilities in terms of information access and availability simultaneously, introducing new challenges in protecting sensitive information from some eyes while making it available to others. Today's business environment is extremely dynamic and experience rapid changes as a result of technological improvement. Banks have traditionally been in the forefront of harnessing technology to improve their products and services. The Banking industry of the 21st century operates in a complex and competitive environment characterized by these changing conditions and highly unpredictable economic climate. Information and Communication Technology (ICT) is at the center of this global change curve of Electronic Banking System in Nigeria today [1]

The application of information and communication technology concepts, techniques, policies and implementation strategies to banking services has become a subject of fundamental importance and concerns to all banks and indeed a prerequisite for local and global competitiveness banking. The advancement in Technology has played an important role in improving service delivery standards in the Banking industry. In its simplest form, Credit Cards and deposit machines now allow consumers carry out banking transactions beyond banking hours.

With online banking, individuals can check their account balances and make payments without having to go to the bank hall. This is gradually creating a cashless society where consumers no longer have to pay for all their purchases with hard cash. For example: bank customers can pay for airline tickets and subscribe to initial public offerings by transferring the money directly from their accounts, or pay for various goods and services by electronic transfers of credit to the sellers account. As most people now own mobile phones, banks have also introduced mobile banking to cater for customers who are always on the move. Mobile banking allows individuals to check their account balances and make fund transfers using their mobile phones.

The delivery channels today in Nigeria electronic Banking are quite numerous; Automated Teller

Machine (ATM), Point of Sales (POS), Telephone Banking, Smart Cards, Internet Banking etc.

Making payment via Internet introduces new challenges for security and trustworthiness. Trust and security are key enablers of the Information Society; specifically, they are the first and foremost requirements needed to be addressed by web-based banking systems. For customers to use web-based banking services comfortably, they must have confidence that their online services are trustworthy and secure. Similarly, for banks to provide web-based banking services they need confidence in the security of online transactions.

Internet security is well known and many security models and protocols have been developed for it. Secure Sockets Layer/Transport Layer Security (SSL/TLS) is recognized as the de facto web-based banking standard to offer trust and security for transactions [2]. It is claimed by Certification Authority(s) that the use of SSL Certificate on company's Web server can securely collect customer's sensitive information online, win customer's trust, and increase business by giving customers confidence that their credentials and transactions are safe [3]. However, nowadays, trust and security has been diminished by the increasing number of local attacks (malicious software on client side such as, Trojan-horse), remote attacks (phishing, pharming), which are used to steal customer's credentials or SSL user session. An attacker can combine local and remote attacks; this can result in more serious damage [4].

In traditional banking, trust and security results from: firstly, customer and bank to authenticate each other; secondly, they conducting transactions in a secure environment; and finally, signing and keeping copies of the transaction sheets by either party. This research/project work uses the same approach to restore trust in a digital environment by authenticating bank and customer using physical credentials to access web-based banking accounts, a three-level security model is used to provide a secure environment. Digital signatures are also used to imitate traditional paper-based signature into the digital realm by adding a digital "fingerprint" as a signature to an electronic transaction document, and either side keeps a copy of the signed document [5].

II. RELATED WORK

A critical task to help businesses and financial institutions including banks is to take steps to prevent fraud and to deal with it efficiently and effectively, when it does happen [6]. Anderson [6] has identified and explained the different types of fraud, which are as many and varied as the financial institution's products and technologies.

Yu & Mukwende [7], in their paper "Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services", proposed a new model for processing Internet banking transactions that increases trust and security over the existing model, by allowing customers and banks to authenticate each other, and sign processed transactions online. According to them the system enhances security through use of a three-tier, trusted, layered, and secure channel. The model ensures that only qualified people can access Internet banking accounts, that the information viewed remains private and cannot be modified by third parties, and that any transactions made are traceable and verifiable. This model provides trustworthy security for Internet banking, by reinforcing SSL tunnel with two tunnels given one at the IP layer, and another at the Application layer, of TCP/IP networks.

Ugoh, Onyeizu, Ugwunna & Uwa [8], in their work "Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools", proposed a model for Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools. The researchers in this work responded to this challenge by developing a two-tier authentication system that is to be attached to the main banking software. This system uses magnetic featured staff identity card for identification and fingerprint biometric for authentication.

Priya, Tamilselvi & Rameshkumar [9] in the research paper, "A Novel algorithm for Secure Internet Banking with finger print recognition" proposed a solution to security in internet banking a solution through novel algorithm with finger print recognition. This involves a combination of username and password at first level and fingerprint recognition at the second level. In their proposed Internet Banking system, the user should first enter User ID and password which will be verified in the bank website for authorization. If the user ID and password matches the user can login to internet banking system. Otherwise, "Invalid user" is reported to the user. At the same time user scans his fingerprint through scanner and checked with finger print feature extraction and matching process.

The Fingerprint image should match with banking database fingerprint. If matches found, user can access to internet banking system. The details of the transactions are finally stored in the Database. If the finger print does not match, the user will get a report as "Invalid user".

Saurav , Sutapa & Md. [10] Proposed a model to mitigate fraud in internet banking in their work, "Proposed Novel Conceptual 3-Tier Security Model for Internet Banking System". According to the researchers the work helps to make a latest idea about online banking transactions as well as increases trust and security over the existing theory, by challenge-response

mutual authentication process and a transaction sign process. This model describes that only selected persons can access online bank accounts, and also it is trying to advance the strength of the authentication, and maintain the confidentiality, integrity and non-repudiation.

Kamble, N. D. & Dharani, J. [11] in "Implementation of Security System Using 3-Level Authentication" proposed the used of 3-level authentication for online banking system. According to them, the work is a unique and an esoteric study of using pattern as password and implementation of an extremely secured system, employing 3 levels of security- (Text Password, Pattern-Lock, and One-Time automated generated password). They concluded by saying that, the three level security approach applied on the above system, makes it highly secure along with being more user friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and brute-force attack at the client side. 3-Level Security system is definitely a time consuming approach, as the user has to traverse through the three levels of security, and will need to refer to his mobile number for the one-time automated generated password. Therefore, this system cannot be a suitable solution for general security purposes, where time complexity will be an issue. But will definitely be a boon in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure. In near future not only we will add more features but also make our system customizable.

Sharifah et al. [12] in Technical Issues and Challenges of Biometric Applications as Access Control Tools of Information Security highlighted some technical issues and challenges faced by biometric technologies within the physical and logical access control applications of information security. Their prime aim was to assist in information security policy and decision making, particularly in providing insights for information security trade-off and risk management analyses. The paper presents a holistic view on current technical issues and challenges of biometric systems as physical and logical access control tools in information security. The effects of biometric menagerie, robustness of the system to actual operating environment and assurance of interoperability were identified as the issues that can be used as guidelines by the industries with regard to information security policy and decision making.

III. PROBLEM STATEMENT

The security of information may be one of the biggest concerns to the Internet users. More so, the electronic banking system users today face the security risks with unauthorized access into their banking accounts. As a result of this, increased adoption of this very important technology has not been as expected. The SSL/TLS protocol being used as the de-facto Internet security standard; provides authentication, confidentiality, integrity and nonrepudiation of messages transmitted over Internet between the web browser and the web server only. However, this protocol operates below the Application layer in TCP/IP networks and does not provide way to ensure whether a user is, in fact, who he or she claims to be by asking for direct or indirect proof of the knowledge about some sort of secrecy or credential.

IV. PROPOSED METHOD

The methodology employed in the course of this research work is object oriented Methodology. An object-oriented methodology is a strategy for designing and developing programs using object technology (classes, encapsulation, inheritance, and polymorphism). Object-Oriented Analysis and Design Methodology (OOADM) methodology prototyping involving the use of unified modeling language (UML). These methodologies facilitated the use of competent high level programming tool such as PHP programming language during the development of the software (Four-phase security model for web-based banking system) after detailed system analysis and design. The security model for web-based banking system consist of several separately designed modules and sub-systems that will be integrated to form the expected software artifact which will be used in money transfer, deposit and withdrawal as well as authentication of user's access.

Object-oriented databases make the promise of reduced maintenance, code reusability, real world modeling, and improved reliability and flexibility. However, in the real world some users find that the object-oriented benefits more comparing what they originally believed. Code reusability is a subjective thing, and depends heavily on how the system is defined. The object-oriented approach does give the ability to reduce some of the major expenses associated with systems, such as maintenance and development of programming code.

V. SYSTEM DEVELOPMENT

The four-phase security model for web-based banking system was implemented using PHP Programming language. The PHP Programming Language was used for the implementation because the programming language has the advantage of easy development, flexibility and it has the ability of providing the developer with possible hints and it produces a graphical user interface.

Moreover, PHP is very user friendly and enables the design of an interface that can be modified programmatically. It consists of all necessary tools required to build main stream server Applications. The features of PHP are as follows:-

i. GUI Interface
ii. Modularization
iii. Object Oriented
iv. Debugging
v. My-Sql Data access feature

The system is an enhancement to an already existing technology. The system comprises of additional mechanism that combines to provide the needed strong security for web-based banking system. The authentication mechanisms utilized are Username and password at the first level, Software token code at the second level, fingerprint verification at the third level and Security question and answers at the fourth level. These authentication mechanisms combine to provide a stronger security for the web-based banking system. Users on the system are grouped into two, the Admin and Customer. The High level Model is as depicted in the fig. 1 below.

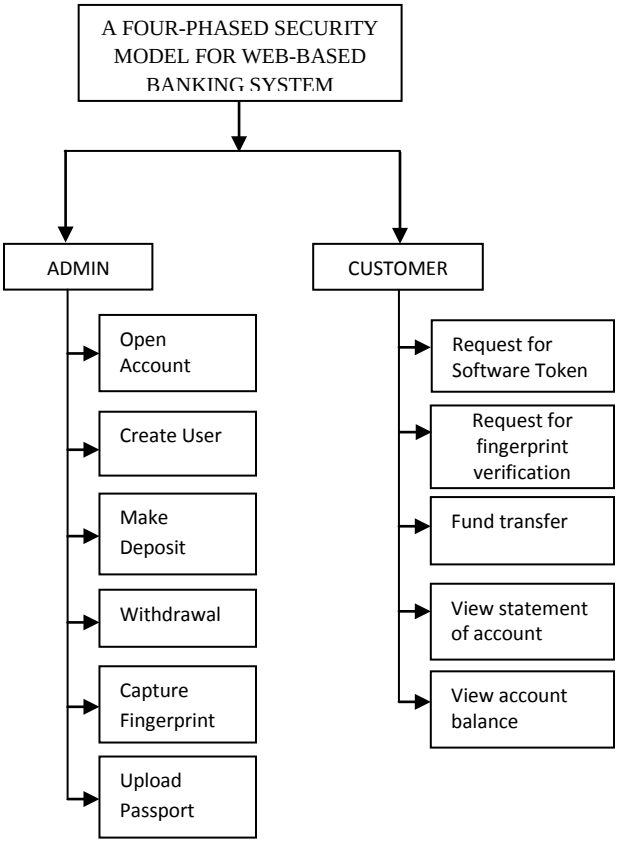

Fig. 1: High level Model of the System model

A. Justification for the four-phase security model

1. Finger print authentication provides very strong security which cannot be compromised.
2. Bank customers will develop more trust in online banking and hence more patronage of the system.
3. The issue of repudiation will be handled and confidence restored for web based banking.
4. The added secret questions and answer authentication for online transactions frustrates the fraudster's attempts to impersonate the real owner of the account.
5. Implementing account freezing by locking the account after 3 wrong attempts will check password guessing.
6. The fraud detection system ensures that all data (credit card numbers, for example) are encrypted and that only authorized users have access to data in its entirety.

B. UML Use-case Diagram of the proposed System

The use case model captures the requirements of a system. Use cases are a means of communicating with users and other stakeholders what the system is intended to do. A Use-case diagram shows the interaction between the system and entities external to the system. These external entities are referred to as actors. Actors represent roles which may include human users, external hardware or other systems. An actor is usually drawn as a named stick figure.

The model designed in this research work is divided into several modules that needs access restrictions. Different use cases were described in the way they were applicable in the software designed. Use cases are as listed below:
1. Bank staff Use Case
2. Bank customers Use Case
The researcher identified total of two roles that functions as access levels in our diagrams. A use case is a function to be performed by the system from the user's perspective. The fig. 2 is the use case diagram of the system.

Use case diagram, the large rectangle is the system boundary. Everything inside the rectangle is part of the system under development. Outside the rectangle are the actors that act upon the system.
Actors are entities outside the system that provide the stimuli for the system. Typically, they are human users, or other systems. Inside the boundary rectangle are the use cases. These are the ovals with names inside. The lines connect the actors to the use cases that they stimulate.

An <<includes>> relationship indicates that the second use case is always invoked by the first use case.
An <<extends>> relationship indicates that the second use case may optionally invoke the first use case.

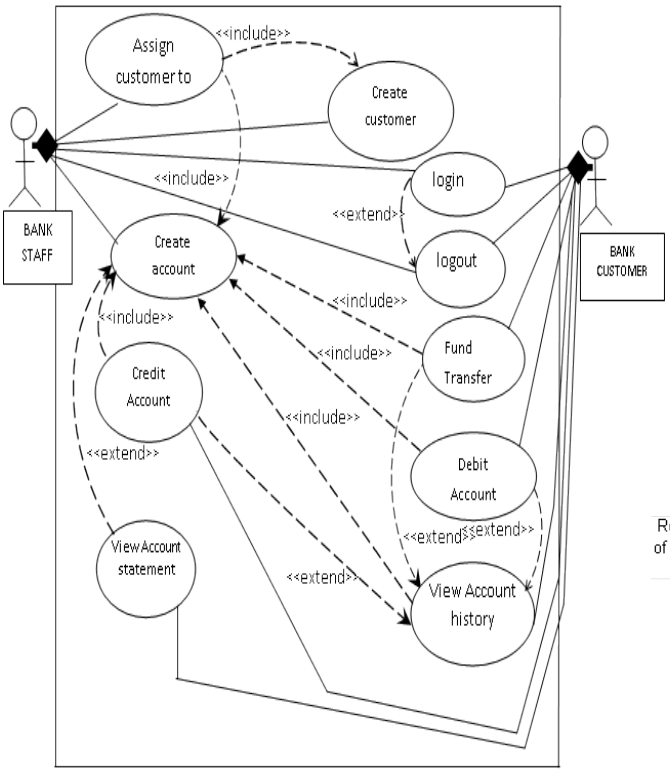

Fig. 2: Use-case diagram of the proposed system

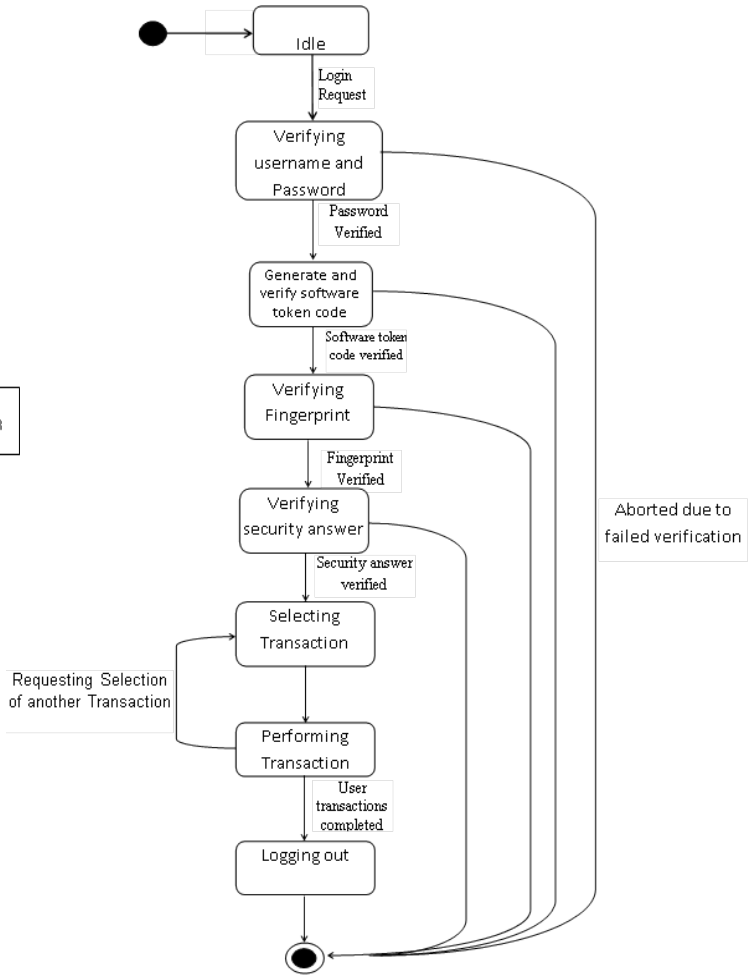

Fig 3: State Chart Diagram of the proposed system

B. UML modeling of the proposed System

Software modeling addresses the software design including interfaces, interactions with other software, and all the software methods. Software models are ways of expressing a software design. Usually some sort of abstract language or pictures are used to express the software design. For this research work being object-oriented software, the object modeling language UML is used to develop and express the software design.

State Chart Diagram of the proposed system

A state diagram, also called a state machine diagram or state chart diagram, is an illustration of the states an object can attain as well as the transitions between those states in the Unified Modeling Language (UML). In this context, a state defines a stage in the evolution or behavior of an object, which is a specific entity in a program or the unit of code representing that entity.

Activity Diagram

Activity diagram basically represents the flow from one activity to another activity in a software design. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent. Activity diagrams deals with all type of flow control by using different elements like fork, join etc. The basic purposes of activity diagrams are to captures the dynamic behaviour of the system. The Activity diagram of the proposed system is therefore used to describe the flow of activities in the new system.

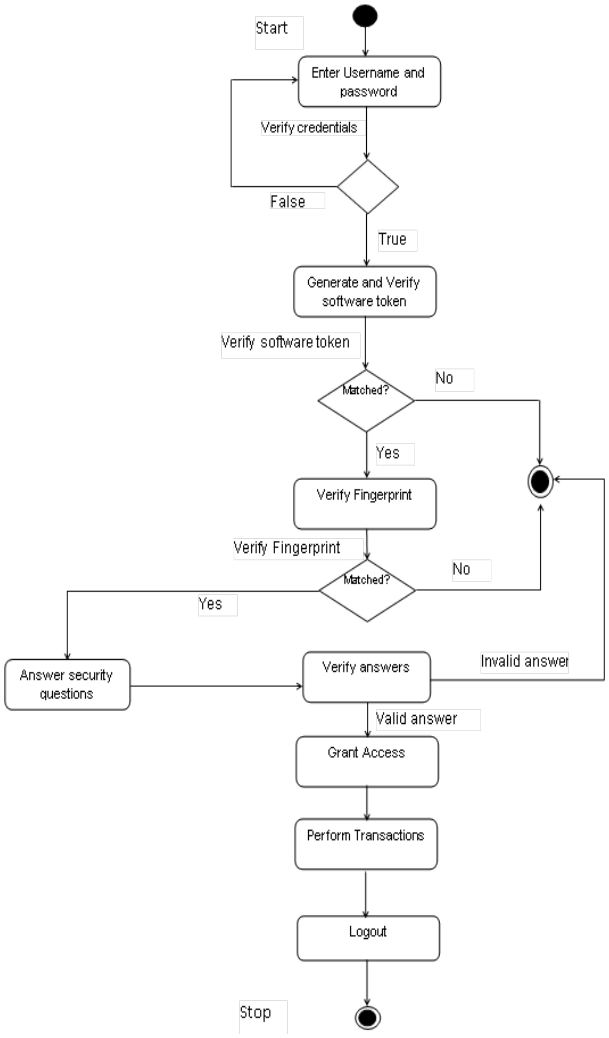

Fig. 4.5: Activity Diagram of the proposed system

C. Mathematical Specifications

In the web based security system for banking industries, the application verifies customers account balance before every transaction is completed. The system compares account balance with the transaction amount in cases of withdrawal or cash transfer. Below are some of the mathematical specifications.

Withdrawal Transaction

If the account balance is less than withdrawal amount then
Deny access to the transaction
Else
Account balance = account balance – transaction amount
End if

Deposit Transaction

Account balance = account balance + transaction amount

VI. RESULTS

The result of the system model is a web-based banking system with an enhanced security. The system tests revealed that the users cannot gain access unless fully authenticated. Fraudsters are stopped after three failed attempts. The table 1 shows the test result.

Module	Expected Test Result	Actual Test Result
Home Page	Expected to see the page containing links to other modules	The home page displayed platform and contains all the links to the various modules in the web based security system
Log In Form	Expected to see the Log In command button so that one can log in.	When clicked on log in, a form appeared where you can enter your username and password for admin or account number and account pin for customers.
New Account opening form	When clicked on the system, it is expected to display the form for entering new account opening details	When clicked on the button, the system displays the customer account opening form.
Deposit/ withdrawal form	It is expected to allow users to deposit or withdraw money	The form allowed the user to enter the account no, transaction amount, date, and post it to the customer's account
Money transfer form	It is expected to allow legitimate customer transfer money to another account	The customer was able to transfer money from his/her account to another account. The authentication phases were effective as expected.
Account Statement	In this module, it is expected to be used to view customers account statement	When you go to this module, the customers statement was displayed

Table 1: Test Result for System Model

IV CONCLUSIONS

In this research work, the primary objective is to develop a Four-phase security model for web-based banking system. Looking at the challenges encountered in web-based banking system like fraudulent money transfers by web hackers, identity theft, cloning of customers account credit card details, as well as channel-breaking attacks in online banking transactions etc, it is perceived that a stronger security using a four-phase security model that will promote trust and good relationship between online banks and their customers is a step in the right direction. The fight against document fraud and identity theft requires the implementation of new technological solutions. Biometrics has quickly established itself as the most pertinent technology for identifying individuals in a fast and reliable way through the use of unique biological characteristics. The model developed apart from using the e-token and account secret pin as a security check during online transaction, it equally authenticate the bvuser by his/her biometric data. This makes the model highly secured and removes identify theft completely as no two persons have the same fingerprint.

REFERENCES

[1] Gbolahan, D. (2005). Banking Sector Consolidation – Integration of IT applications is key, Fin. Standard., 6: 11-24.
[2] Hiltgen, A.; Zurich, T., & Thomas, W., (2006) "Secure Web-based Banking Authentication", IEEE 2006.
[3] Thawte, (2009) "The value of Authentication", http://www.thawte.com, 18 July 2009.
[4] Wueest, C. (2006) "Threats to Online Baning," Symantec Security Response, Dublin, 2006.
[5] Danhash, O., Phu Dung Le & Bala, S., (2007) "Security Analysis for Web-based Banking Banking Models", (IEEE 2007).
[6] Anderson, R. (2007). The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation. New York: Oxford University Press.
[7] Yu L. & Mukwende P. (2009). Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services. Proceedings of the Second Symposium International Computer Science and Computational Technology, Huangshan, P. R. China, 26-28, Dec. 2009, pp. 114-119
[8] Ugoh D., Onyeizu M. N., Ugwunna C. & Uwa C. O. (2015). Reducing Internal Banking Fraud using Smart Cards and Biometrics as Access Control Tools**.** International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 6, June 2015
[9] Priya R., Tamilselvi V. & Rameshkumar G.P. (2014). A Novel algorithm for Secure Internet Banking with finger print recognition. International Conference on Embedded Systems - (ICES 2014)
[10] Saurav M., Sutapa M. & Md. H.(2011). Proposed Novel Conceptual 3-Tier Security Model for Internet Banking System. 3rd International Conference on Machine Learning and Computing (ICMLC 2011)
[11] Kamble, N. D. & Dharani, J. (2014). Implementation of Security System Using 3-Level Authentication. International Journal of Engineering Development and Research. Vol. 2, Issue 2, ISSN: 2321-9939.
[12] Sharifah, M., Borhanuddin, M. & Adnan, W. (2012). Technical Issues and Challenges of Biometric Applications as Access Control Tools of Information Security. International Journal of Innovative Computing, Information and Control (ICIC), Malaysia. 8, 11, 7983-7999.

Authors' Profiles

Samuel O. Okide: is a Senior lecturer in the Department of Computer Science, Nnamdi Azikiwe University Awka. He has Ph.D in Computer Forensics / Software Development. He is a Fellow of Nigeria Computer Society (FNCS) and member of Computer professional Registration of Council of Nigeria (MCPN) . Member of Nigerian Institute of Management (MNIM).

Nnenna S. Nnam: Has a Msc PGD. (Computer Science) Nnamdi Azikiwe University Awka Nigeria. She also obtained a Bsc. (Physics/Electronics) from University of Port- Harcourt, Choba, Nigeria. She is a member of Nigeria Computer Society (NCS) and Computer professionals Registration Council of Nigeria (CPN). She works as a System Analyst with research interest is in Information Technology Network Security.