International Journal of Science Academic Research
Vol. 05, Issue 08, pp.8007-8014, August, 2024
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

DEVELOPMENT OF AN ENHANCED INTERNET BANKING NETWORK SECURITY MODEL

***Dr. Anyaragbu, Hope Uzoamaka and Anigbogu, S.O.**

Department of computer Science, NnamdiAzikiwe University Awka, Nigeria

Received 14th June 2024; **Accepted** 18th July 2024; **Published online** 20th August 2024

Abstract

The continuous growth in Internet banking has increased the importance of security in delivering Internet banking services to customers. This is because the Internet banking systems are opened up to the environment which makes it vulnerable to attack. However, the existing models are focused more on fraud identification and less on fraud prevention. In order to increase confidence and trust of customers, online banking systems require efficient network security models capable of mitigating frauds by identifying users and authorizing transactions using an enhanced model which combines different authentication mechanisms that can enforce stronger authentication and authorization for Internet banking transactions, hence this study. The aim of this work was to develop an enhanced Internet network security model for Internet banking. The objectives were to develop a system that could; ensure that the information viewed by users remain private; provide effective detective and preventive payment mechanism for legitimate users; develop a security platform where customers and banks authenticate each other; sign processed transactions online; create database history for each user and have capacity to adapt itself with future technologies. This work was done using a combination of Neural networks and Fuzzy System model of web servers for more effective decision making. The model systematically combined authentication mechanisms of Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi Factor Authentication (ZTMA) to enhance security properties of all transaction payments in the Internet banking systems. The system was implemented using Java server Pages (JSP) from a suite of Java programming language and MySQL open data base connectivity. The result of this work provided a model that enhanced security that crossed two attack boundaries - offline and online channel breaking; provided greater interoperability among banks irrespective of location; provided non repudiation of services between banks and their customers; guaranteed safety of customers' transactions through their PCs and electronic gadgets; ensured that signed transactions were traceable and verifiable and ensured proper authentication and authorization of all transactions and levels of access associated with Internet-based customer products and services; thereby increasing trust, confidence, integrity and availability to its users. The enhanced Internet banking model developed in this work ensured that bank's customers receive more efficient and secured transactions by successfully crossing the two attack boundaries – offline and online channel breaking and guaranteed that banks and their customers authenticate each other

Keywords: Presented here are definitions of essential concepts that are used throughout this work-Network, Network Security, Computer security, Information security, Identification, Authentication, Stakeholders, Internet, Threats, Vulnerability, Attacks, World Wide Web (WWW), TCP/IP, Workgroup, Workstation, Uniform Resource Locator (URL), Biometrics, Domain Name Service, Nonrepudiation, Nonrepudiable Transactions, Repudiation, Password, Payment System, System Integrity, Risk, Virus, Vulnerability,Authentication , Social engineering, Access Control (Authorization), Availability, Confidentiality, Integrity.

INTRODUCTION

Internet banking, also known as online banking, has experienced significant growth and adoption in Nigeria over the past few decades. Adoption of online banking is increasing day by day because through it, the banks can save crucial time and accelerate operations to the convenience of both customers and service providers. The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. The most recent deliverance channel to be introduced is electronic or online banking (Daniel, 1999). Electronic commerce draws on technologies such as "mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems" (Power, 2013). Electronic or online banking is the latest delivery channel to be presented by the retail banks and there is large customer acceptance rate.

Corresponding Author:** ***Dr. Anyaragbu, Hope Uzoamaka,
Department of computer Science, NnamdiAzikiwe University Awka, Nigeria.

Overall, internet banking has become an integral part of the Nigerian banking sector, driving financial inclusion, improving efficiency, and enhancing customer experience. To this end, efforts are being made to address cybersecurity challenges and ensure the continued growth and stability of online banking services in Nigeria. Despite these efforts, Internet banking have continued to evoke a range of fears and concerns for people, many of which revolve around issues of security, privacy, and usability.

Fears associated with internet banking as updaded in October 14th, 2023

1. **Security Breaches**: One of the biggest fears is the possibility of security breaches, such as hacking or identity theft, which could lead to financial loss or unauthorized access to sensitive information.
2. **Fraudulent Activities**: Users worry about falling victim to various forms of online fraud, including phishing scams, where attackers pose as legitimate institutions to trick users into disclosing personal information.
3. **Technical Issues**: Concerns about technical glitches, system failures, or cyberattacks that could disrupt online banking services and transactions also contribute to people's fears.

4. **Privacy Concerns**: Many individuals are uneasy about the privacy implications of sharing personal and financial data online, worrying that their information could be intercepted or misused.
5. **Complexity and User Experience**: Some users find internet banking platforms difficult to navigate or understand, leading to fears of making mistakes or inadvertently compromising their accounts.
6. **Dependency on Technology**: There's a fear of becoming overly reliant on technology for financial transactions, with worries about what might happen if systems fail or if access to online banking is unavailable.
7. **Lack of Human Interaction**: For some, the absence of face-to-face interaction with bank representatives can be disconcerting, as they may prefer the reassurance of speaking with someone directly when managing their finances.
8. **Regulatory Compliance**: Concerns about whether online banking services comply with relevant regulations and standards, especially regarding data protection and consumer rights.

Despite these concerns, internet banking continues to evolve, with financial institutions implementing robust security measures and improving user experiences to address these fears and build trust among their customers.

Statement of Problem

Considering these concerns, in internet banking, the current deliverance channel should be analyzed with a view of identifying vulnerability thereof and proffer an enhanced model for online access to their systems. As transactions processed through online banking systems are on the increase. Technologies are also continuously changing. The number of malware and exploits focused on online banking systems vulnerabilities has been steadily growing during past years. The developed new model is expected to introduce more sophistication in authentication and authorization to tackle the problems of existing models and ensure sound interoperability, scalability and reliability, enhance security of financial information over the net and application distribution among the banks for online internet banking transactions.

Aim and objectives of the study

The aim and objectives of this research is to develop an enhanced network security model that should be able to;

i. Facilitate interoperability of transaction for its users in different locations among the twenty two commercial banks in Nigeria.
ii. Ensure that the information viewed by the users remain private and can't be modified by third parties.
iii. Provide effective detective and preventive payment mechanism for legitimate users by alerting the users of the model of unauthorized access to their accounts via sms and email.
iv. Allow customers and banks to authenticate each other, and sign processed transactions online.
v. Create database history for each user by keeping details of user's transaction for audit trail.
vi. Have capacity to adapt itself with future technologies and handle exponential growth of customer base.

LITERATURE REVIW

Overview of its history in Nigeria as updated in January, 2022

1. **Early Adoption (1990s):** Internet banking began in Nigeria in the late 1990s with the emergence of a few pioneering banks that introduced basic online banking services. However, adoption was slow initially due to factors such as low internet penetration, limited technological infrastructure, and concerns about security.
2. **Regulatory Framework (Early 2000s):** The Central Bank of Nigeria (CBN) played a crucial role by issuing regulations and guidelines to govern online banking operations. These regulations were aimed at ensuring the security and stability of the banking sector while promoting innovation and customer convenience.
3. **Expansion and Innovation (Mid-2000s):** Throughout the mid-2000s, more banks in Nigeria started offering internet banking services as internet penetration increased and technology improved. Banks began to invest in robust online banking platforms, offering a range of services such as fund transfers, bill payments, account management, and mobile banking.
4. **Mobile Banking Revolution (2010s):** The proliferation of mobile phones, particularly smartphones, led to a significant shift towards mobile banking in Nigeria. Banks introduced mobile banking apps and USSD (Unstructured Supplementary Service Data) codes, allowing customers to access banking services directly from their mobile devices.
5. **Partnerships and Collaboration (2010s):** Nigerian banks started forming partnerships with fintech companies to enhance their internet banking offerings.
6. **Security Concerns and Regulations (Ongoing):** Despite the growth of internet banking, security remains a significant concern. Cybersecurity threats such as phishing, identity theft, and online fraud have prompted regulators and banks to continually enhance security measures and compliance standards.
7. **Current Landscape:** As at the last update in January 2022, internet banking in Nigeria continues to evolve rapidly. Most banks offer comprehensive online banking services, and the adoption rate among consumers is steadily increasing.

The number of attacks on our networks and the level of sophistication of those attacks are growing steadily, and threaten to overwhelm existing tools for guaranteeing network security. Network and computer security is critical to the financial health of every organization. Network attacks are often caused by direct or indirect interaction of humans. There are many situations in which employees themselves pose the biggest threat to enterprises. Many times, employees will unintentionally install piracy software that is infected with viruses, worms or trojans. Other times, users may forget to secure their workstations, leaving them open as an easy target to potential attackers. And yet others may give sensitive information to outsiders, or even play a role in an important part of an attack (Popescu, 2013*)*. Equally, Shoshani writing on USA Department of Energy report stated the need for new types of scientific approaches to internet network security. "This is because of increasingly sophisticated adversaries with significant resources, including organized crime which rapidly develop exploits to take advantage of these vulnerabilities. Concurrently, automated attack tools have expanded the

volume of malicious activities by lowering the level of expertise required to launch an attack. Typically, as new vulnerabilities emerge, new products, policies, and initiatives are introduced to reactively counter these exploits. The result of this reactive approach has ultimately been an ineffective posture characterized by a cycle of patching vulnerabilities, more often than not discovered by exploits of those vulnerabilities. The inevitable outcome is that some vulnerabilities will be exploited before they are patched." (Shoshani *et al.,* 2011). In spite of security models being implemented by banks, banking trojans had continued to successfully operate via pharming and phising, directing security to reactive fraud identification rather than prevention (Laerte *et al.,* 2011). It is expected that any Internet banking system must solve the issues of authentication, confidentiality, integrity, and no repudiation; to ensure that only qualified people accessed Internet banking accounts.

Some of the major problems of existing models used in online banking Nigeria are:

a) **Operability:** The desire for interoperability is largely dependent on the individual banks.
b) **Security of financial transactions:** transactions being executed from some remote location and transmission of financial information over the air need to be private and secured.
c) **Scalability and reliability**: Need for the model framework to support scale-up of the internet banking infrastructure to handle exponential growth of the customer base.
d) **Application distribution:** Due to the nature of the connectivity between bank and its customers, it is difficult for customers to regularly connect to the bank web site or visit the bank for regular upgrade of their internet banking application.

In Nigeria, Online banking usage has been on the increase, growing from paltry 0.06% in 1995 to 32.9% in 2012 (Maku, 2013). The Nigerian minister for information – Mr Labaran Maku also in his analysis stated that usage increases from 200,000 users in the year 2000 to more than 48 million users by the end of 2012. This growth is interesting and the increase in popularity has not gone unnoticed by the criminal element. Apexis (2015) opined that as the Bank security networking system requires sharing of resources and rapid response, there is need to strengthen the real-time monitoring and management of the health of the network system by considering the following points:

1) The system should have unified authentication management mode user privileges.
2) The system should adopt a multi-level user rights management mechanism to prevent unauthorized operation of the user.
3) Server equipment should be able to restrict or control access to some IP client.
4) Operating functions of the system should log important events recorded in the log list, filing and scheduled backups in case of hardware failure that causes data loss.
5) The bank security networking systems should use variety of methods to ensure network security.

Also, report from Juniper, based on data from a 2021 research, has it that the global cost of online payment fraud is expected to reach $206 billion by 2025. Bad actors will use every fraud technique in their arsenal to hack into accounts and steal hard-earned funds. Therefore, customers must understand online banking threats and utilize best practices to protect themselves.

Risk of Online Banking

Following the steps above will help ensure your online banking information is protected, but unfortunately there is no guarantee. Notable data breaches at banks and established financial institutions have happened as recently as November 2021, when the stock trading platform Robinhood disclosed a data breach that gave hackers access to the personal information of around 7 million customers. As updated on August 13, 2023, another risk of online banking is having a device you use for online banking lost or stolen. Even if you have multifactor authentication and a strong password set up for your online bank account, someone may be able to access your email to either change your password or bypass your bank's security measures. If a device you use for online banking is ever lost or stolen, call your bank to have your accounts temporarily frozen so no one can access your funds. Updating in October 14, 2023, it is stated that digital banking, online or by mobile app,is convenient, inexpensive and typically offers better interest rates on savings than traditional banks. Although money in an online bank is insured by the National Deposit Insurance Corporation (NDIC) and protected as well as in a conventional brick and mortar bank (N250, 000 per depositor, per bank), online banking security remains a concern for many people.

Summary

Hence understanding why users overlook security mechanisms will not only help in the formulation and enforcement of security policies, but also contribute to the design of usable security technologies. To this end, a model that will improve on the existing authentication and authorization mechanisms, enhance interoperability, manage continued change in the systems technology, without impacting on users experience and at the same time provide secured transactions of the users among the banks in the country becomes necessary.

SYSTEM ANALYSIS AND METHODOLOGY

This section presented analysis of the current adopted models and proposed model and thereafter the methodology and a combined authentication mechanisms that combined smart card technology, biometric details and password to enhance the model security for the users.

Analysis of currently adopted security models

The models currently adopted in online banking systems are based on parallel solutions of identification, authentication and authorization mechanisms that are reactive at protecting the banking application and the user's data. Figure 1 below showed some of the security models currently adopted in internet banking by banks in Nigeria. In the existing models, most of the attacks directed at online banking systems is targeted at the user (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authentication data.

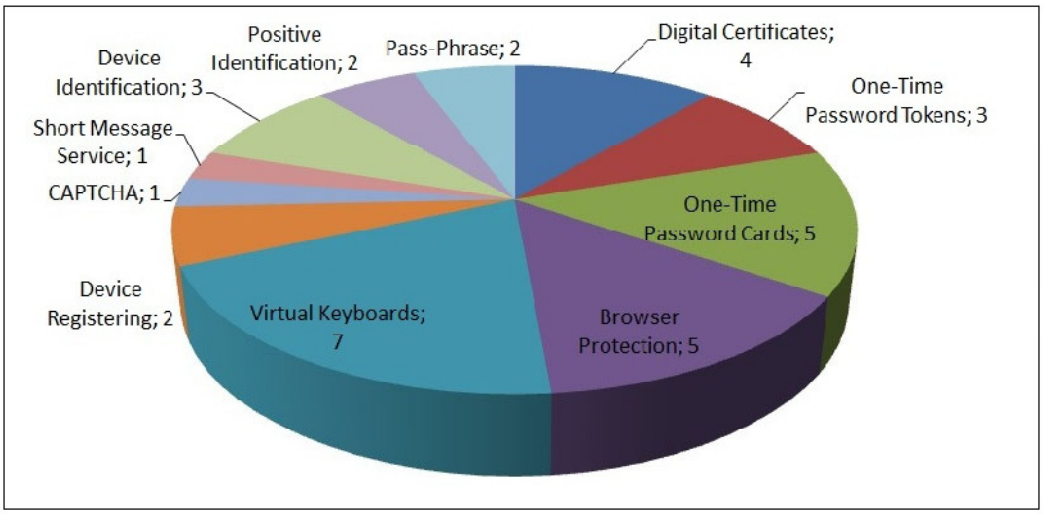

Figure 1. Current Internet Banking Security Models (adopted from International Journal of Computer Science & Information Technology (IJCSIT), 2011)

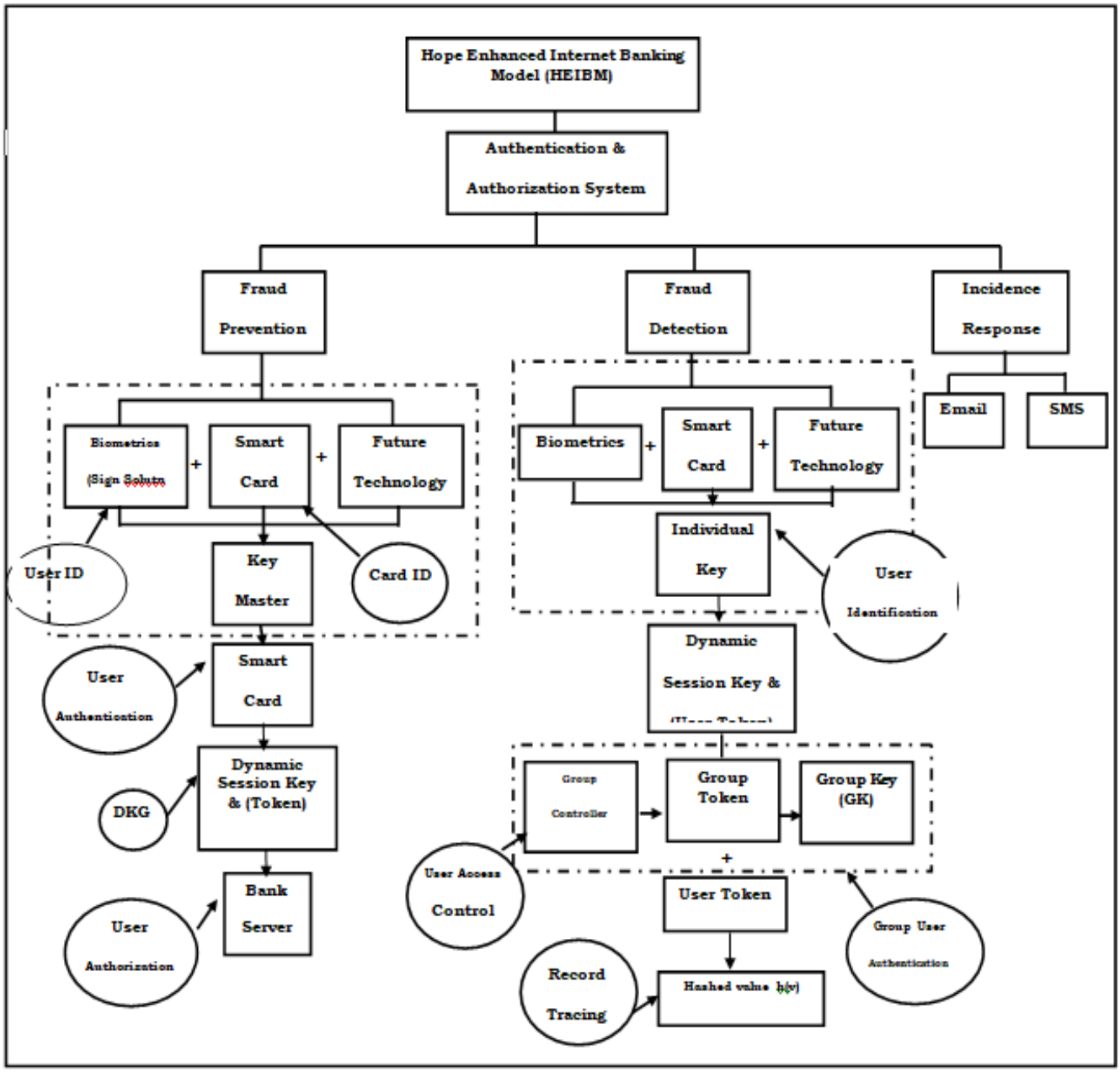

Figure 2. Illustration of the concept of Hope Enhanced Internet Banking Model (HEIBM)

Analysis of the proposed system

The model considered the main target of attack on internet banking system which is the user and their account. The proposed design divided the solution of developing enhanced internet banking model into three main areas: prevention, detection and incident response. This is to ensure that security is reactive to both fraud identification and prevention. The steps in which the proposed model tackles detection and prevention problem are as shown in (Figure 2). This model is updated with more sophisticated future technologies as they emerge to ensure continuity and relevance. HEIBM provides a good platform for more sophisticated internet banking cashless policy implementation in Nigeria, prevent and detect fraudulent payments thereby ensuring that customer's confidence and trust are protected.

Software methodology: neural networks and fuzzy system (Neuro-fuzzy model)

Hope Enhanced Internet Banking Model (HEIBM) is an intelligent system. Web technology requires the application of more complex systems for maintaining high quality of internet services. Subsequently, the methodology used for developing HEIBM is a combination of Neural networks and Fuzzy system model of web servers for effective decision making process. Neuro –Fuzzy model targets non-stationary processes by developing novel on-line learning methods and uses computationally efficient algorithms for real-time applications. Fuzzy systems have the ability to formalize in a computationally efficient manner the approximate reasoning typical of humans while Neural Networks present a convenient framework for synthesis and analysis of complex non-linear systems.

The advantages of using such a neuro-fuzzy system are:

1. It is able to process uncertain information;
2. Automatic extraction of the rule-base;
3. It is able to learn from examples;
4. It has a reduced input data space because of its locally recurrent structure.
5. The obtained experimental results by using the suggested neuro-fuzzy system reveal its good performances of approximation and generalisation.

Neuro-fuzzy systems model combine their advantages to establish machine learning methods. Web switch is responsible for controlling request flow. The switch uses request distribution algorithm for serving HTTP request. The switch transfers a request obtained from a client to the model server and a response from the server to the client (Two way architecture). The server is the key of the web switch. The model provides decision in real time. The model server consists of eight modules, namely:

1. Internet Banking Registration
2. User Login
3. Transaction
4. Hacking Simulation
5. Report
6. About us
7. Help
8. Exit

The model used combination of these authentication mechanisms - Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi-factor Authentication (ZTMA) to enhance the existing security models

System design

The emphasis of the design is on transactional aspect of internet banking which is where the bulk of the risk applies.The model used combined Authentication mechanisms of - Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi-factor Authentication (ZTMA) to identify and authenticate the users of the model and thus deliver enhanced security to internet banking transactions.

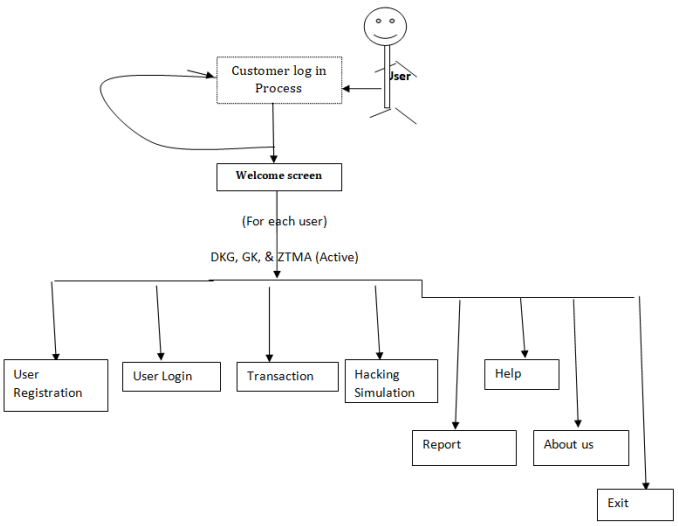

Fig. 3. System level activity diagram of the Model

Systems Flowchart

The application system is as shown in figure 4. The user starts the application, then selects activity required from the main menu. As any menu is selected, the operation is performed.

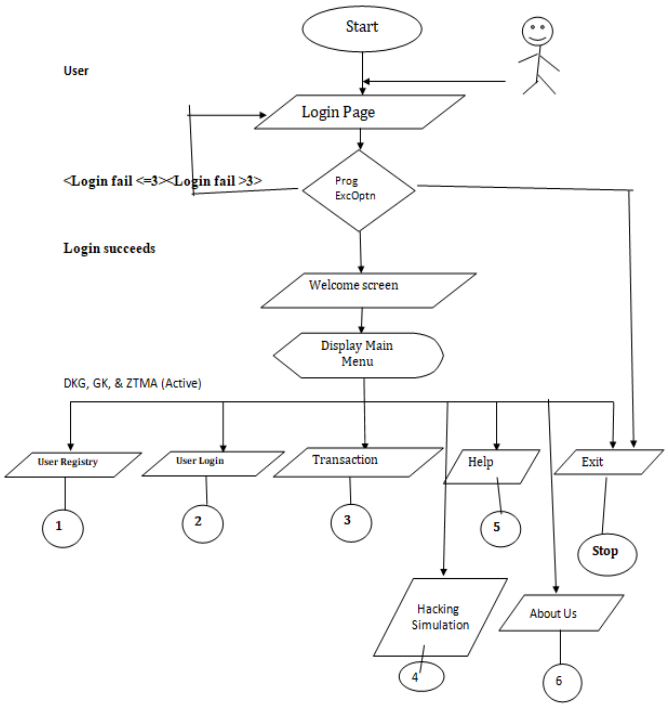

Figure 4.

Implementation and documentation

The enhanced design is implemented by dividing the solution of providing better security of transactions to users into three main areas: prevention, detection and incident response.

Prevention:

a. User Unique ID
b. User Authentication
c. Dynamic Key Generation
d. Smart card Transaction Security
e. Biometric requirements
f. Signature solutions

Detection:

a. User Identification
b. Users Access Control
c. Group Users Authentication
d. Record Tracing

Incidence Response:

a. Sms and E-Mail Alerts
b. Login reports

The architectures specified how the artifacts of the system together delivered the desired security functionality.

System's Documentation

The application used JSP for its development and presentation. JSP is a presentation layer technology that sits on top of a Java servlets model and makes working with HTML easier. JSP allows the mix of static HTML content with the server-side scripting to produce dynamic output. Figure 5. shows the dynamics of Java Server Pages (JSP) model architecture.

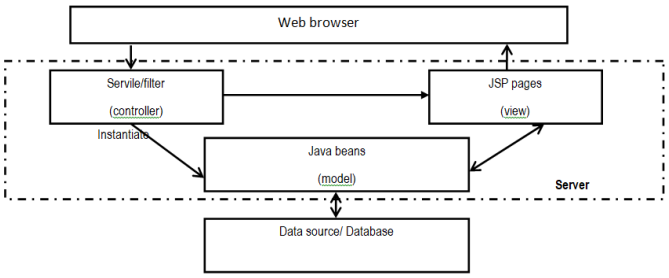

Figure 5. Diagram of JSP model architecture (adopted from Libertyenie, 2013)

System Requirements

Hardware Considerations: The under listed hardware were used to run and implement the model.

1. Customers' PC Network of computers and other network enabled devices. User may make more memory space available by removing temporary files on computer. The computer must have a minimum of 1.5 GBs of hard disk space available.
2. Wireless Access Points and Routers
3. CD-RW/DVD drive, External Hard disk (optional: for back up if necessary).
4. Screen Resolution 256 Color @1024*768(minimum)
5. The CD-ROM requires a minimum of 512MB -1GB of RAM
6. Internet connection
7. Embedded real-time systems for mass storage, automotive, industrial and networking applications
8. Secure applications including smart cards and SIMMs

Software Considerations: Software architecture includes computational components and their interrelationships, constraints on their relationships, and at the same time focus on different connections between components. The software is expected to develop rationales which demonstrate that the components, connections, and constraints will define a system that satisfies the given requirements. These components include:

1. Web Application server/Browser (Mozilla Firefox or Internet Chrome 6.0 SP2)
2. Microsoft windows server 2003 or 2007, Windows XP(with SP2) or Windows 2000 Professional (with SP 4).
3. OR one of the following distributions Red Hat Fedora Core 3, Red Hat Enterprise Linux 3.
4. Client Operating system with good Memory Management Unit (CD with minimum of 500 MHz Pentium 111 processor), in addition to minimum RAM required by the users' operating system to run the Java server pages.
5. Any Java SDK 1.0 and above that will require 1GHz Intel Pentium 4 processor or equivalent

Required Third Party Software:

1. Internet Browser (chrome 5.5 SP2 or 6.0 SP2
2. Adobe Acrobat Reader 6.0 or 7.0 or higher required. If the user does not have Adobe Acrobat Reader installed on the computer, check on the latest version of Acrobat Reader at http://www.adobe.com/products/arobat/readstep.html.
3. Xamp or Wamp server Mysql Database, Msql lite, Sql workbench etc
4. Visual Studiobor later version

System Maintenance

Security is never an absolute quantity. Effective security is Security-in-Depth. It is a moving target – as software and hardware development continue, and as new products emerge (with new bugs), hackers will seek those vulnerabilities, and discover new and innovative ways of exploiting them. It is an arms race, and the banks need to be prepared to win it. Maintenance therefore will involve continuous vulnerability and penetration assessment for removal of faults after the model has been completed, tested and implemented.

Test Plan

The security assessment was implemented to evaluate the security level of the Internet banking model designed, using authentication mechanism, taking into account all entities involved in the process, and then propose necessary countermeasures for risk reduction

The combination of the mechanisms of DKG, GK and ZTMA in Hope Enhanced model ensured resistance to all the attacks – (UT/U1) user surveillance, (UT/U2) hidden codes, worms, (UT/U3) smart card analyzers, (UT/U4) social engineering,

(CC) Man-in-the-middle (MIM) attacks or malformed IBS web sites (IBS) and thus provide more effective security controls to the system as shown in the figure below

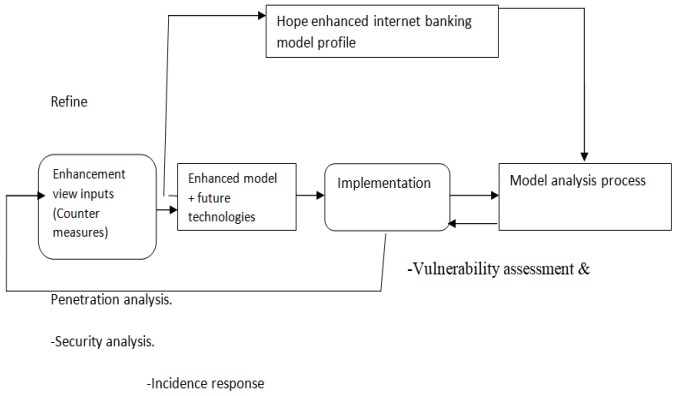

Figure 6. System Framework testing

The security provided by the model therefore:

1. Crossed the two attacks boundaries and provided greater interoperability among banks irrespective of location.
2. Provided non repudiation of services as the bank and their customers received signed transactions that either cannot later refute, given that each party receives evidenceof transaction processed.
3. Guaranteed safety of customers' transactions through their PCs and electronic gadgets through out of box authentications.
4. Signed transactions were traceable and verifiable. Hence trust level was increased proportionally to the increased level of security.
5. The combined different authentication mechanisms ensured that only qualified people accessed their bank accounts.

Summary and Conclusion

Banks are interested in increasing the use of Internet banking, because of the lower cost of transactions. Security has always been a central issue in banking. At the same time it is also commonly accepted by technologists that it is impossible to ensure perfect security. They argued that PCs and mobile phones were designed for communication rather than secure Internet commercial transactions (Adamson, 2003). This is even more true as criminal attacks on Internet banking have become more sophisticated (Adamson, 2003; McCullagh and Caelli, 2005). The Bank addressed the dilemmas of cheaper Internet transactions and imperfect security by concentrating on enhancing the security of existing models. This is sequel to the fact that:

1. Security is a process.
2. Effective security is Security-in-Depth.
3. Regular audit is needed to determine the importance of assets in their network and allocate resources accordingly to enhance their security.

Table 1. Applicability of Attacks in different Authentication Mechanisms

Attack/Authentication Method	Static Password	Soft-token Certificate	Hard-token Certificate	One-time Password/Time Based	Challenge Response	Biometrics	Knowledge-based	HEIBM
UT/U1a: User surveillance	A	X	X	A	X	X	X	X
UT/U1b: Token/notes theft	A	X	A	A	X	X	X	X
UT/U2a: Hidden code	A	A	A	A	X	X	A	X
UT/U2b: Worms	A	A	A	A	X	X	A	X
UT/U2c: E-mails with malicious code	A	A	A	A	X	X	A	X
UT/U3a: Smartcard analyzers	X	X	A	A	X	X	X	X
UT/U3b: Smartcard reader manipulator	X	X	A	X	X	X	X	X
UT/U3c:Brute-force attacks	X	X	A	A	X	X	X	X
UT/U4a: Social engineering	A	X	X	X	X	X	A	X
UT/U4b:Web page obfuscation	A	X	X	X	X	X	A	X
CC1: Pharming	A	X	X	A	A	A	A	X
CC2: Sniffing	A	X	X	A	A	A	A	X
CC3:Active man-in-the-middle attacks	A	X	X	A	A	A	A	X
CC4: Session hijacking	A	X	X	A	A	A	A	X
IBS1: Brute-force attacks	A	X	X	A	X	X	A	X
IBS2: Security Policy Violation	A	A	A	A	A	A	A	X
IBS3: Web Site Manipulation	A	X	X	A	X	X	A	X

Legend
A: Applicable
X: Not Applicable

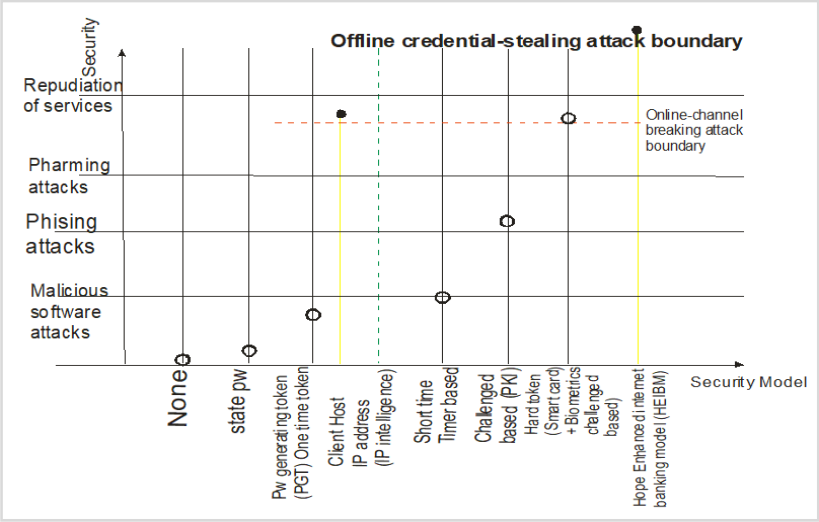

Figure 7. Effectiveness of security of HEIBM compared to that of existing models

Conclusion

A company's business is its lifeblood, and there is a need to match internet banking business opportunities with security. The magic of security is to design the banks' network securely while empowering their business without hindering it. Application of the enhanced model will help the bank in securing their network from those who would rob them of their company's most valuable asset - money. Micheal Adu, (2015) opined that "Security can be defined as the degree of resistance to, or protection from harm. It applies to any vulnerable and valuable assets, such as persons, dwellings, communities, nations or organizations" .Network security comprise of three legs (security trinity) - prevention, detection, and response (Figure 7). The security trinity – Prevention, Detection and Response are the foundation of proactive security policies for any organization.

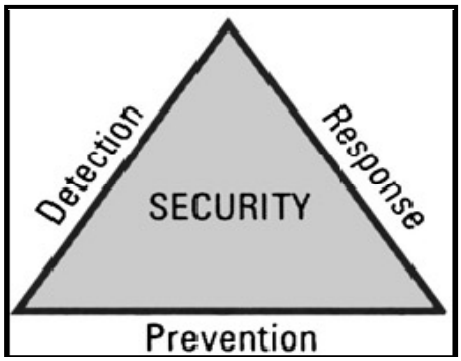

Figure 8. The security trinity (Adopted from MichealAdu, 2015)

Hope enhanced internet banking model, considered these processes, hence, it is proactive rather than defensive. The security measures provided by the model ensured that clients account information was not compromised by fraudulent users. As a result of enhancement in security, users' trust and perception of Internet banking improved. Users therefore received more efficient and secured transactions than existing models provided.

REFERENCES

Adamsom, G. (2003), "The mixed experience of achieving business benefit from the internet – A multi-Disciplinary study". Business information technology, RMIT University, Melbourne.

Adu M. (2015), "Cyber Security in Nigeria: A Collaboration between Communities and Professionals", www.Reseachgate.com 2021

Apexis G. (2015). "Analysis of the importance of the banking network monitoring*", International Computer Information & Management journal.*

Daniel and Storey (1998), "Online Retail Banking-Digital Distribution in Banking", London.

https://www.tri3.1.com – Cybersecurity Solution Set, Junifer Report 2021

LaertePeotta, Marcelo Holtz, (2011). *International journal of computer science and information technology (IJCSIT),* Vol 3, No 1, pp 16.

MakuLabaran, (2013), Electronic Banking: The Risks. A Paper Presented at chartered institute of Bankers Research Lunchon Lagos.

Powell, P. and KleinJ (1996), "Risk management for information systems development." *Journal of Information Technology,* vol11: p.309-319.

PopescuMaholtra, (2013), Determinants of Internet Banking Adoption by Banks in India, *Emerald Internet Research* Vol.17, No 3.

Lichtenstein S. (1996),"Factors in the selection of a risk assessment method." *Journal of Information Management and Computer Security*, 4(4): 20-25.

Shoshani J and Ross Anderson (2011), Security Engineering: A Guide to Building Dependable Distributed Systems, pp 185-187

www.https://dojah. Online banking security, November 2021

www.usnews.com "How to keep your information safe when online banking", Aug 13th, 2023

www.https://time.com – Time magazine" How to protect online Banking Information, October14, 2023.

****