CHAPTER ONE

INTRODUCTION

1.1 Background of the study

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.

Growth and turn-around in Nigeria's banking sector has been amazing and exceptional due to online technology exploited by the banking sector. The financial institutions are using the technology to improve services to their customers and their customers have also accepted the technology. The continued progressive competitive atmosphere in the banking sector has resulted in developing and operating substitute deliverance channels. The most recent deliverance channel to be introduced is electronic or online banking (Daniel, 1999). Electronic or online banking is the latest delivery channel to be presented by the retail banks and there is large customer acceptance rate.

Bank branches alone are no longer enough to offer services to meet the needs of today's high demanding and challenging customers (Bradley, et al., 2003). So online banking does play a very effective role. This technology is very useful in connecting different branches of the same bank or different banks with each other. The central bank of Nigeria (CBN) in its recent circular titled Industry policy on retail cash collection and lodgment dated March 16th, 2012 made some changes in the modalities for operations of its policy on Cashless Economy by indicating that no customer can withdraw or deposit more than N500,000.00 cash at a time per day from his/her account for individuals and N1m for corporate. This cash light policy is expected to extensively use this online real time technology effectively.

This means that the banks will be linked with network of computers which is administered by service provider and use this new communication media to offer its customer value added services and convenience. The electronic banking system will address several emerging trends: customers' demand for anytime, anywhere service, product time-to-market

imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels and a trusted code at both endpoints.

To buttress the need for internet network security, Yang opined “Imagine yourself in this situation. You are at home alone one evening and you have your computer connected to your banking account. You are checking out your banking account to see how much money you have. Like many people, you still have a lot of money at home because you don’t fully trust the banking system. Suddenly, you hear a noise outside and jump right out of your chair. You rush over to the window to see who is outside and realize that it is a burglar. You have a lot of money placed under your mattress and you fear that the burglar will take it. Since this is an age of advance technology, you have a mechanical device that lets you transfer paper money into electronic money which can then be sent to your bank via the Internet. This machine destroys the money and keeps track of the amount destroyed. You realized that you can save your money from the burglar and rush to get it immediately. You place all your money in the machine and it quickly converts the paper money into electronic money. By the touch of a button, you transfer your money to your banking account where it is safe. Now your money is safe. Now all you have to worry about is yourself”. (Yang, 1996)

In today’s highly technological world, the machine that destroys paper money and converts it into electronic money is far from reality. But the part on the person interacting with his or her banking account late at night is becoming more of a reality. The information superhighway has found its way into many homes, schools, businesses, and institutions. Many people are cruising the Internet each day to obtain information on the weather, latest sport scores, local news, and many other exciting information.
This new electronic media of interaction has grown to be known as the electronic commerce. According to Wikipedia, the free encyclopedia “Electronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information.”

Consequently, electronic commerce is comprised of interconnected communications networks; advanced computer hardware and software tools and services; established business transaction, data exchange, and interoperability standards; accepted security and privacy

provisions; and suitable managerial and cultural practices. This infrastructure will facilitate diverse and distributed companies nationwide to rapidly, flexibly, and securely exchange information to drive their business processes. 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).

The e-commerce system allows consumers to access their banking accounts, review most recent transactions, and request a current statement, transfer funds, view current bank rates and product information and record checks. This provides the major motive of internet banking as "Urgent decisions across the branches of the bank can be taken in minutes through access to remote databases or through Electronic Data interchange. Delicate information can be stored in remote centers and accessed by authorized users of internal coalition and exogenous entities with whom the organization have business dealings. Thus business transactions and decisions are given real time touch and emerging opportunities can be capitalized in without possible loss of golden opportunities" (Osuagwu, 2005). Another major motivation for internet banking provided by e-commerce is that it is a tool for competitive advantage" Hence, organizations must emphasize functional internet platform that possesses the attribute of resolvability, interoperability, connectivity and compatibility with the banks short and long term goals. Based on these, there is need for network security model that will provide these attributes and build confidence in the users.

Types of Internet Banking

Internet banking controller handbook 1999 identified three basic types of Internet banking employed by bank as:

i. **Informational** – This contains the marketing information about the bank*'*s products and services on a stand-alone server.

ii. **Communicative** –This allows some interaction between the ban*k'*s systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications, or static file updates (name and address changes).

iii. **Transactional** -This level of Internet banking allows customers to execute transactions. Customers operate on their accounts for transfer of funds, payment of different bills, subscribe to other products of the bank and to transact purchase and sale of securities, etc.

This is the highest risk area and must be highly secured as a path actually exists between the server and the bank ’s internal network.

Benefits of Internet Banking

Osmond Vitez in his contribution to eHow journal, 2009, enumerated the under listed benefits:

1. **Convenience -** Bank websites allow customers to conduct banking transactions 24/7 with just a computer and an Internet connection.
2. **Multiple Uses -** Internet banking allows customers to link their bank account to outside accounts, like mortgages, retirement savings, or money markets. This allows customers to quickly transfer money among their accounts.
3. **Real-Time Transactions -** Most customers use debit cards linked to their bank account for making many different daily purchases. These transactions are then uploaded to the customer's bank account instantly, tracking transactions in a real-time format.
4. **Daily Reconciliation -** Customers can use Internet banking to track their cash daily and reconcile their account to prevent theft or bank errors. This shortens the down time of finding an error and waiting to correct it until receiving their paper bank statement.
5. **Security -** Internet banking provides several types of security for customer account. Banks review transactions for validity, prevent access to the account after login failure, and cut debit card access if questionable transactions appear on a customer's account.

Business Directions of a Bank

A bank is “ the connection between customers that have capital deficits and customers with capital surpluses” (Wikipedia, the free encyclopedia) This definition refers to the core activity of commercial banks, namely the simultaneous acceptance of deposits and offering of loans, which distinguishes them from other financial intermediaries. However, banks typically conduct a broader range of activities, which can be subsumed under the following three functions:

1. First, banks provide the public with liquidity (money) and payment services through their deposit-taking business.
2. Second, banks transform assets in terms of denomination, quality and maturity, as well as manage the associated risks.
3. Third, banks process information and monitor borrowers using specialized technologies. In so doing, they often establish long-term relationships with their clients, which may

further mitigate the negative impacts of adverse selection and moral hazard on the resource allocation process.

A Bank's vision statement as stated by the managing director of unity bank Plc in her annual address to the stakeholders' 2012, is as follows:

"To be a unique preferred bank dedicated to its customers, financially strong, consistent, committed to staff and their development and delivering sustained superior performance to its shareholders".

The vision statement determines the business direction of the bank. Business directions of any bank therefore can be identified as stated.

I. The bank aims to run on performance through improved technology, rather than size which has been the case in the previous years.
II. The bank intends to build on its strengths, rather than entering new business areas.
III. The bank aims to shift from a bulk approach to a competitive consumer products business that uses sophisticated marketing apparatus.
IV. Evolve a robust secured network system that will provide efficient internet banking service.
V. Aim to use technology as much as possible to service and acquire/retain customers.
VI. Achieve the priorities of the bank by executing the business plan, focusing on productivity, build formidable management team, and reduce volatility of earnings.

Banks apply Information Security Control Model (Figure 1.1) to ensure strict adherence to the business directions. The model shows the hierarchical nature of information assets, their policies and standards, the functional responsibilities and tasks associated with the various levels. Subsequently, it manages the access level of the bank staff as they work to achieve the overall goal of the bank.

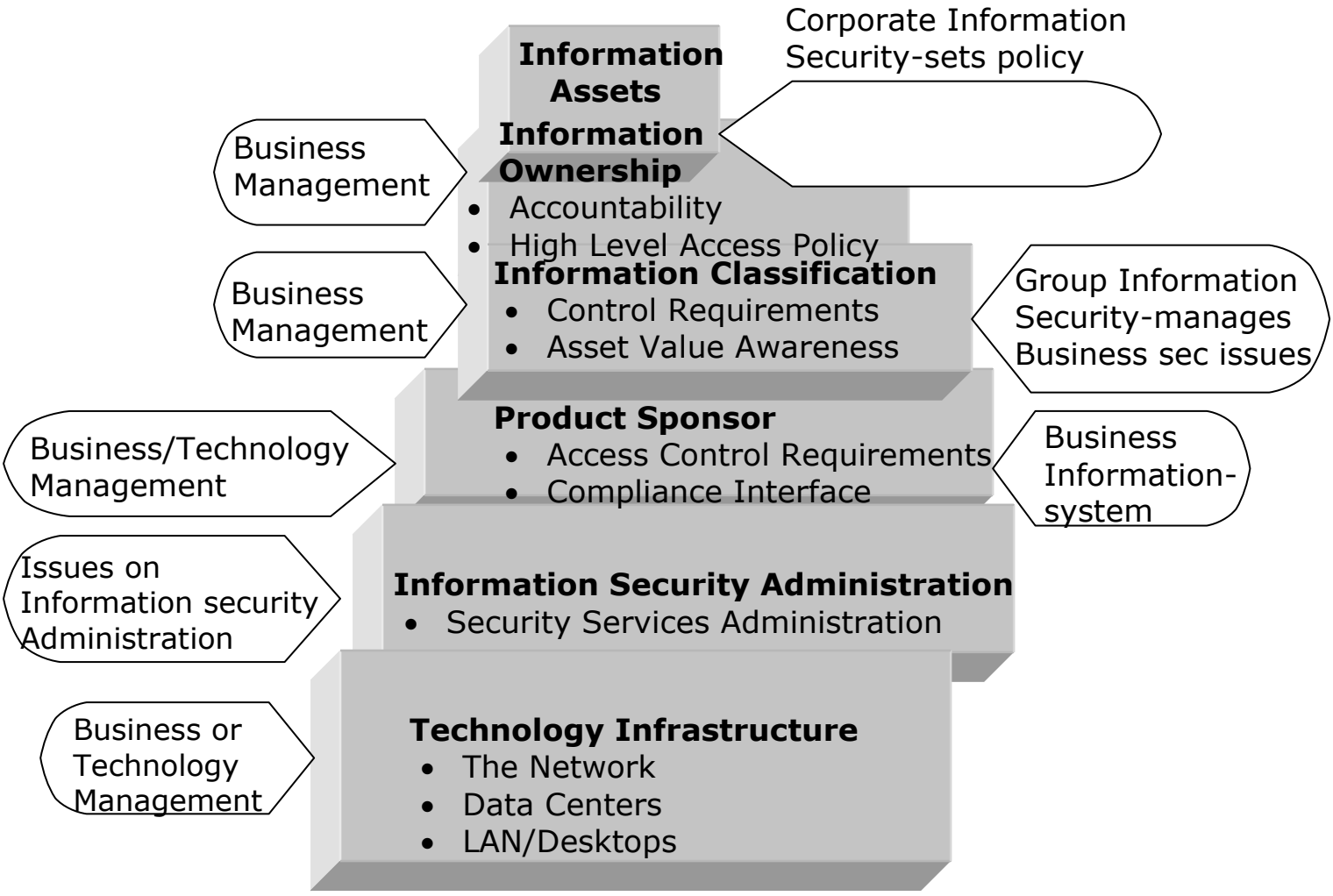


Figure 1.1 Information Security Control Model Of a Bank (adopted from Unity bank journal, 2013)

1.2 Statement of Problem

Considering the business directions of the bank, the new deliverance channel, which is the internet banking, should be analyzed with a view of identifying vulnerability thereof and proffer an enhanced model for online access to their systems. The number of 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.

Several security models had been implemented by banks in Nigeria. However, banking trojans had continued to successfully operate via pharming and phising, directing security to reactive fraud identification rather than prevention (Laerte, et al, 2011). Furthermore, it must be considered that the responsibility for maintaining security is always transferred to the weakest link in the security chain, which means, in most cases, the final user. 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 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.

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.

1.3 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.

1.4 Significance of the Study

Internet usage and the online banking sector are experiencing spectacular growth. The biggest problem facing Internet banking today is the thorny issues of trust and security of online transactions. In fact, the vast majority of customers are concerned about the safety of their transaction, and they can't simply trust the web fearing that their transactions and credentials might not be safe due to the increasing number of online Internet attacks.

Internet banking fraud can be performed internally by genuine staff or externally by customers or suppliers. Several modern models in preventing and detecting fraud are evolving and being applied to many banking systems. However, they have no effective detection mechanism to identify legitimate users and trace any unlawful activities. "Fraud detection and prevention systems have become crucial requirements as many banks and business increasingly rely on electronic transactions" (Donald, 2001).

Internet banking fraud involves legitimate users with some legitimate activities but also includes illegitimate activities by users other than the account holder. Therefore, banks are seeking to minimize huge losses through fraud detection and prevention systems (Joris, et al., 2002). Many different advanced fraud technologies are being applied to fraudulent Internet banking transactions detection and prevention (Zhauang, et al., 2004). Also they are not secure enough to prevent fraudulent users from performing fraudulent transactions over the Internet.

These increasing dangers posed for the internet by dire-devil hackers and fraudsters have continually devalued the degree of confidence placed in internet banking. Online fraud has become major source of revenue for criminals all over the globe. This has made detecting and preventing these activities a top priority for every major bank. Hackers and intruders are always on search to get some loop wholes in existing internet banking models to exploit corporate sector especially banks of vital financial data and other sensitive information. The existing technology has kept failing as new vulnerability techniques are being discovered by hackers, thus demanding a completely new approach to the pandemic.

In all these scenarios, data integrity and security can never be compromised. Therefore developing an enhanced secured network model that can protect internet banking transactions more and increase confidentiality, integrity and availability for the users becomes very necessary.

1.5 Scope of the Study

The current business directions of banks in e-banking, demands a clear need for enhanced internet banking security model for banks in order to offer safer online access to their systems. This is because as the online internet banking application is increasing, the unauthorized users are also increasing and developing different means of attacking the banking system to defraud authorized users. Based on this, Hope Enhanced Internet Banking model (HEIBM) which is an intelligent system, was developed to enhance the vulnerability of existing internet banking models. The enhancement was achieved by using a stronger authentication and authorization mechanisms of Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi-factor Authentication (ZTMA).

These mechanisms provide comprehensive, secure and sophisticated authentication that effectively confirm user identity and protect payment transactions details. These mechanisms were also used to analyze the security of the model to show that the model has better security than existing models.

The methodology used in developing the model is a combination of Neural networks and Fuzzy system model. The Neuro-Fuzzy methodology provided simple effective decision making tool using Artificial intelligence technology to process uncertain information and control HTTP request traffic.

Java server Pages (JSP) language from a suite of Java programming language was used for the development of the application software as it helps to create dynamically generated web pages for online real time transactions.

1.6 Limitations of the Study:

Challenges encountered in this work include:

1. The PCs and mobile phones used by the model are prone to theft which can make it possible for an unauthorized user to have access to privileged information.
2. The systematic authentication mechanism required by the model is dependent on network which most times may be unavailable.

3. Users of the model may be impatient or in a hurry to carry out the systematic authentication required, hence become frustrated and abandon the use of the stipulated authentication process.
4. There may be incidence of false alert to the user.
5. Model upgrade and updates may not be done timely due to resources and administrative bottlenecks.
6. The model requires experienced personnel to effectively conduct an auditing or security evaluation process.

1.7 Overview of Project Stages

To design the system is to develop a prototype model on the basis of which a real system can be built, developed, or deployed that will satisfy all its requirements (Wymore, 1993).

The overview of the work stages of the project is as shown in figure 1.2 below. The general introduction of the growing importance of internet banking in Nigeria and the need for enhanced security of transaction to increase confidence and trust among users was discussed. Thereafter, statement of research objectives, significance, scope and limitations of the study was addressed.

Review of related literature on earlier works on the subject was done. This was followed by analysis of present and proposed models. The methodology and authentication mechanisms applied to achieve enhanced security for model.

The next step to these was system design and implementation, followed by system testing and performance evaluation. The summary and conclusion was the last activity.

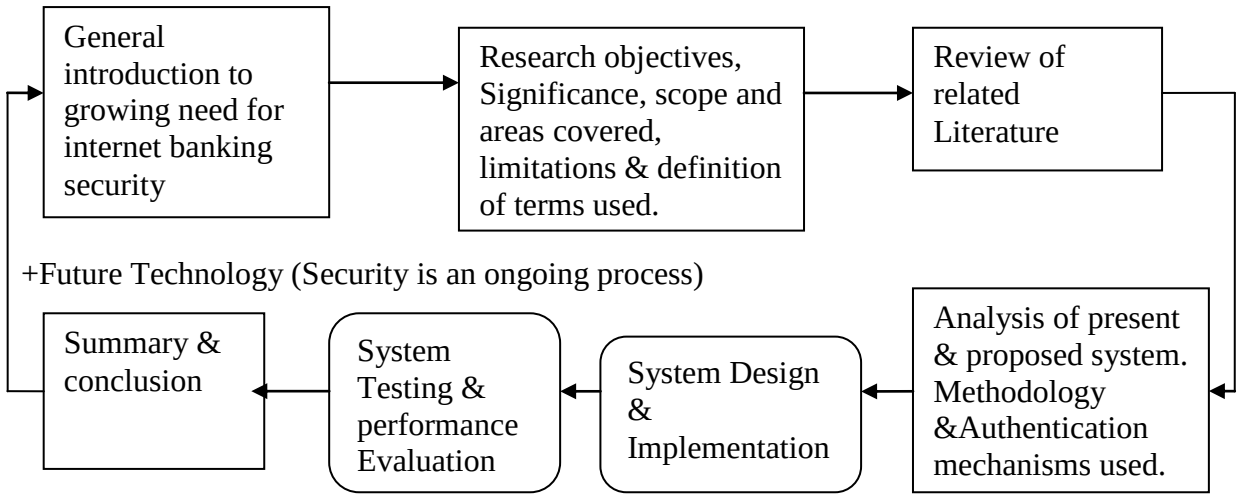


Figure 1.2 Block Diagram overview of project stages

1.8 Definition of Terms

Presented here are definitions of essential concepts that are used throughout this work.

Network - any set of interlinking lines resembling a net, an interconnected system. A computer network is simply a system of interconnected computers.

Network Security: Encompasses both computer and information security. It deals with the deterrence, avoidance, prevention, detection and reaction to events in and affecting a computer network.

Computer security deals with the deterrence, avoidance, prevention, detection and reaction to events in and affecting a computer system that are undesirable to the owner of that system.

Information security consists of the concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use.

Identification - is simply the process of determining the identity of the individual or entity with whom you are communicating.

Authentication - serves as proof that you are who you say you are or what you claim to be.

Usability is "the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or component"

Stakeholders - With regards to computer and software systems, stakeholders include for example users, developers, administrators, owners, security experts and any other party that holds a stake in the system.

Internet – Defined as a global network of computers that connects millions of computers around the world.

Threats - A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system.

Vulnerability – Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

Attacks - An attack is a specific technique used to exploit vulnerability**.**

World Wide Web (WWW) – It is the total set of interlinked hypertext documents residing on the HTTP (Hypertext Transfer Protocol) all around the world.

TCP/IP **-** (Transport Control Protocol/Internet Protocol) is the ``language" of the Internet. It is a suite of protocols that can be used to connect dissimilar brands of computers and network devices.

Workgroup - A collection of computers that are grouped for viewing purposes. Each workgroup is identified by a unique name.

Workstation - A powerful personal computer.

Uniform Resource Locator (URL) - A way of specifying the location of available or Universal Resource information on the Internet.

Biometrics - A method of verifying a person's identity by analyzing a unique physical attribute.

Domain Name Service - A network service that translates (DNS) external Internet addresses into numerical Internet network addresses.

Nonrepudiation - The undeniable proof of participation by both the sender and the receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and later prevent denial or repudiation by the sender or receiver.

Nonrepudiable Transactions - Transactions that cannot be denied after the fact.

Repudiation - The denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Password - A unique word or string of characters that a programmer, computer operator, or user must supply to satisfy security requirements before gaining access to the system or data.

Payment System - A financial system that establishes the means for transferring money between suppliers and users of funds, usually by exchanging debits or credits between financial institutions.

Protocols – 1) A standardized set of rules that define how computers communicate with each other. 2) An established rule of communication adhered to by the parties operating under it.

System Integrity -The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.

Risk - The risk that the failure of one participant in a funds transfer system, or in financial markets, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due.

Virus - A program with the ability to reproduce by modifying other programs to include a copy of itself.

Vulnerability - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security.

Authentication - A process that grants access to a local or remote computer system, a network, or online information.

CA - (certification authority) - An entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities.

Digital Signature - A coded message added to a document or data that guarantees the identity of the sender.

Electronic Banking - The use of a computer to retrieve and process banking data (statements, transaction details, etc.) and to initiate transactions (payments, transfers, requests for services, etc.) directly with a bank or other financial services providers remotely via a telecommunications network.

Electronic Commerce - The use of an information infrastructure through which businesses can speed the exchange of information, improve customer service, reduce operating costs, and increase global competitiveness.

Encryption - The scrambling, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security.

Hash Code - A unique, mathematical summary or "fingerprint" of a document that serves to identify the document and its exact contents. Any change in the hash code is an alert that the document's contents have been altered.

Private-key security - Also known as symmetric-key security, this is a security mechanism based on both parties have the same encryption key, as in secret-key cryptography. The client and server share a key to encrypt and decrypt information on a network.

Public-key security - Also known as asymmetric-key security or public-key encryption technology, this is a security mechanism for securely distributing encryption keys that are used to "lock" and "unlock" data across an unsecured path. Public-key security is based on encryption key pairs, in contrast to private-key security, which is based on having a single, shared key.

Public Key Infrastructure (PKI) - Involve the use of a public key and private key pair for authentication and proof of content. A PKI infrastructure gives its users the certainty of the quality of information sent and received electronically, certainty of the source and destination of that information, assurance of the time and timing of that information (providing the source of time is known), certainty of the privacy of that information, assurance that the information may be introduced as evidence in a court or law.

Social engineering- awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

Access Control (Authorization) - Refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive.

H***yper***T***ext*** M***arkup*** L***anguage*** **-** the authoring language used to create documents on the World Wide Web

Availability- Refers to whether the network, system, hardware, and software are reliable and can recover quickly and completely in the event of an interruption in service.

Confidentiality -This can also be called privacy or secrecy and refers to the protection of information from unauthorized disclosure.

Integrity - This is the accuracy in protecting information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations in a network system.

CHAPTER TWO
LITERATURE REVIEW

2.1 Importance of Network Security

The use of new distribution channels such as internet and electronic commerce increases 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. Banks realize that doing business with the internet involves big risk, but if secure procedures are in place, internet banking is not riskier than other business. On the contrary, it becomes riskier if banks avoid the use of internet banking. However, Forcht observed that while the internet banking provides opportunities for banks to increase their customer base, lower transaction costs, sell more of their products, security issues hinder its use (Forcht et al, 1996). Forcht's statement showed that maintaining network security is critical to every banks' continued economic growth. A glimpse of other peoples view on network security and approaches made to prevent attack and increase trust and confidence is provided here.

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).

The department further reported that "The complexity, interconnectedness, and scale of information systems suggest that important lessons can be learned from similarly complex systems that require integrity, confidentiality, and availability. For example, the Department-sponsored workshop in May 2008 brought together academics, industry experts, national laboratory scientists, and policy makers to explore metaphors such as biological immune systems, ecosystems, and markets and risk management. A key conclusion was that any effective approach to cyber security must address complexity at scale, necessitating the use of scientific tools and techniques appropriate for such complex systems."

As the citations above demonstrate, ensuring network security is a difficult problem that is growing more difficult daily. It is a social problem of the most difficult type to solve, a "wicked problem." In order to face such a challenge, there is need to continually improve on the security of current models to internet banking network.

2.1.1 Two types of network security approaches

John E. Canavan noted in his Ph.d work identified two current categories of network security procedures. One category of procedures inspects traffic passing through the network, as well as the connections and types of services requested in order to allow traffic to flow. The other category centers on user authentication—verifying that a user is who the user claims to be (Canavan, 2000).

The first category is more complex, and includes:

· Installation of firewalls to control traffic coming into and going out of a network

· Inspection of incoming traffic for viruses, worms, and other types of malware

· Observation of activities carried out by users of the network and verification that users are authorized to carry out those activities.

· Creation and installation of rules for carrying out these activities

· Updating and upgrading security software to respond to newly-discovered threats.

There are well-known drawbacks to these procedures as they are carried out at present:

· Firewalls can be tricked to admit new types of worms, viruses, and other malware

· Users modify their activity patterns and become irritated if they are prevented from carrying out legitimate activities by a security system

· If sufficiently irritated by them, users avoid or ignore security measures

· Malicious, trusted users can do significant damage to an organization's assets without triggering warnings

· Network security rules and the parameters of those rules arrive with default settings, and need to be tuned in order to improve their performance, but many administrators use the default security rule settings

· Updates of virus detection software can arrive well after the viruses have done their damage

· Minor modifications of viruses allow them to slip through current anti-virus database-based programs

The other category of network security procedures, center on user validation, and includes the following:

· Password requirements to log in

· Badges, tokens or other physical items required to log in

· Biometric requirements such as retinal scans or fingerprints required in order to log in

There are well-known drawbacks to these procedures as well:

· User passwords can become known by attackers, and users are resistant to changing passwords or using passwords that are meaningless sequences of letters and therefore impossible to guess

· "social engineering" and other tactics can be used to hijack user sessions or install software that observes user sessions and captures user passwords, account data, and other vital information badges, tokens and other items can be stolen or lost.

He concluded that damage done by malicious but trusted network users cannot be prevented through user verification, since these users can log into the network without difficulty. There is therefore need to design a model which will use a mechanism for identifying and verifying all users of the internet banking system for any transaction.

2.1.2 Why Computer and network security is important to a bank

Sundaram in his work edited and updated by Stonecypher, stated that: The purpose of network security is essentially to prevent loss, through misuse of data. There are a number of potential pitfalls that may arise if network security is not implemented properly. Some of these are:

I. Breaches of confidentiality: Each business will identify with the need to keep certain critical information private from competitor eyes.

II. Data destruction: Data is a very valuable commodity for individuals and enterprises alike. Destruction of data can severely cripple the victim concerned.

III. Data manipulation: A system break-in may be easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is a more insidious threat than that. Data values can be changed and, while that may not seem to be a serious concern, the significance becomes immediately apparent when financial information is in question (Sundram et al, 2010)

Canavan (2000) also stated that Network security is important to a bank for the following reasons:

1. *To protect banks assets:* The assets are "information" which is housed in the company's computers and networks.
2. *To gain a competitive advantage:* Developing and maintaining effective security measures provides a bank with a competitive advantage over its competitors. It can mean the difference between wide acceptance of a service and a mediocre customer response.
3. *To comply with regulatory requirements and fiduciary responsibilities:* Organizations that use computers for their continuing operation must develop policies and procedures that address organizational security requirements to protect company from liability and its assets.
4. *To ensure job security:* Protection of organizational assets, ensure job security for its employees and future career prospects.

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.

2.2 The Rise in Online Banking Fraud

Internet usage and the online banking sector are experiencing spectacular growth. Worldwide, there are 423.5 million people accessing banking sites which constitute 28.7 percent of the internet audience at present Middle East and Africa usage is 8.8%.(World Internet Stats, April 2012).

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.

As Online fraud has become major source of revenue for criminals all over the globe, it has made detecting and preventing their activities a top priority for every major bank. Even most disturbing is the recent increase in the number of attacks and the evolution of their techniques. “The media almost on daily basis carries the news of security breach on banks, credit cards, Facebook accounts, email accounts, phone records and more. Cyber thieves are constantly on the increase and looking for new ways to get around even the most complex firewalls and security systems” (Jackson, 2013). It is important to note that most banks do not report their experiences with these attackers for fear of impact on their reputation and customer reactions.

To help combat fraud, the FFIEC (Federal Financial Institutions Examination Council) issued guidance on October 12th, 2005 related to stronger authentication for Internet banking services. Financial Institutions were made to achieve compliance by year-end 2006.

Highlights of the FFIEC Guidance stated:

a. Financial institutions offering Internet-based products and services should use effective methods to authenticate the identity of customers using those products and services.
b. Single-factor authentication methodologies may not provide sufficient protection for Internet-based financial services.
c. The FFIEC agencies consider single-factor authentication, when used as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

They saw the common approach of front-door authentication as an important hurdle to place in the way of fraudsters, though identity thieves often have the information to pass through

that gateway. However, with the addition of real time fraud detection, single users and group-level activity can be intelligently monitored for patterns that are an instant tip-off to fraud.

2.2.1 Key Types of Online Fraud

The council also identified two classes of fraud that commonly affect online operations:

1) User Identity Theft: The user information required to obtain access to the online systems is stolen through means that include:

Phishing attacks which trick the user into providing access information.

Key-loggers and "spyware" which transparently capture access information.

2) User Session Hijacking - an attack in which a user's activities are monitored or falsified using malicious software ("malware"). Session hijacking malware can operate on a user's local computer, or remotely as part of a "man-in-the-middle" attack.

Local malware session hijacking uses techniques such as host file redirects.

Remote malware session hijacking attacks use techniques such as DNS hijacking and Content Injection.

Strong authentication at the "Front Door", provides only partial protection against User Identity Theft. However, this approach provides no protection against Session Hijacking.

2.2.2 Modeling

Steinmuller (1993) defined model as information

On something (content, meaning)

Created by someone (sender)

For somebody (receiver)

For some purpose (usage context)

Webster's new encyclopedic dictionary (1994) also defined model as a

a) A small but exact copy of something

b) A description or analogy used to help visualize something that cannot be directly observed.

An example for this type of model is a network security model to protect online banking transactions. Here exact "refers to the properties one wants to retain but must not be misunderstood to mean complete".

H,Stachowiak (1990) opined that a model is expected to possess three features namely:

- Mapping feature: A model is based on an original.
- Reduction feature: A model only reflects a (relevant) selection of the original's properties.

- Pragmatic feature: A model needs to be usable in place of the original with respect to some purpose.

The first two features are covered simultaneously if one speaks of a model as a “projection" as this implies both something that is projected (the original) and that some information is lost during the projection. Of course exactly what information is dropped by an activity called “abstraction" and what is retained depends on the ultimate purpose the model is going to be used for.

The third feature can be further elaborated by detailing what the pragmatic use of the model is. Developing a network security model as contained in this work is therefore a projection of the original that is expected to provide protection for internet banking transactions.

2.2.3 Systems modeling

System modeling is a technique to express, visualize, analyze and transform the architecture of a system. Here, a system may consist of software components, hardware components, or both and the connections between these components. Complete systems are then developed by composing these components. In this way, a system model can satisfy different requirements such as documenting the system, providing a notation for tools such as consistency checkers and can also be used in the design stage of system development.

Systems modeling or **system modeling** is therefore the interdisciplinary study of the use of models to conceptualize and construct systems in business and IT development. A common type of systems modeling is Business Process Models Notation (BPMN) which this work will be interested in. The model can be extended using functional decomposition, and can be linked to requirements models for further systems partition. Thus, system modeling is used to ensure that a developing piece of software evolves in a consistent manner and that the task of integrating software components is simplified.

As a type of modeling, system modeling is based on systems thinking and the systems approach such as:

1. Agent based modeling
2. Data modeling
3. Mathematical modeling
4. Neural Network modeling
5. Fuzzy modeling

A combination of Neural and Fuzzy modeling will be adopted for this research to create an intelligent system. Neuro–Fuzzy model targets non-stationary processes by developing novel on-line learning methods and uses computationally efficient algorithms for real-time applications. “The tasks of the system design include the decomposition, statement of the design problem, the architectures, functional and physical representation of the system. These functions can be formalized as detailed functions with both inputs and outputs” (Buede, 2000). Table 2.1 gives the name of functions and their input and output information.

Table 2.1 Design Process Functions

DESIGN FUNCTIONS	INPUTS	OUTPUTS
Define Design Problem	Stakeholders Requirements	Originality Requirement Operational Concepts
Develop System Functional Architecture	Original Requirements Operational Concepts	Functional Architecture
Develop System Functional Architecture Physical Functional Architecture	Originating Requirement	Physical Architecture
Develop System Functional Architecture Interface	Function Architecture	Interface Architecture
Develop System Functional Architecture Qualification System	Originating Requirement	Qualification System Design Documentation

2.3 People's Perceptions of Security of Internet Banking

Security has always been a central issue in banking. Banking made the promise that customers' money will be kept safe. Security issues have become more intense in the domestic context with Internet banking. The fear of loss of money through internet banking, had been escalated by media stories of hackers, fraudsters sending phishing emails purporting to be from banks, and sophisticated malware such as key logger software that could siphon off money from your bank account as you keyed in your access codes.

Security has most often been seen as a matter of getting the right technology and mathematics in place. It has been difficult for theoretically oriented security system developers to move from theoretical security to usable security. Schneier (2000) said, he was wrong to think that mathematics alone could ensure digital security as he did not take into account users. He stated that security is a multi-layered process, rather than a product. He realized that "the fundamental problems in security are no longer about technology; they're about how to use the technology". This approach places the user at the centre of security development..

There are at present three approaches to user-centered security. The first is to recognize that people are not focused on security but on an activity. This emphasis aligns security and usability. The second is to move from a focus on security to an emphasis on trust. Control and comfort with the transaction, together with a perception that the customer is being looked after, is essential for trust. The third is the close connection between privacy and the control of personal information. This emphasis on control of personal information connects security, trust, privacy and identity.

Users' main goals are at the centre of usability. Karat said: the use of security and privacy solutions is generally not the user's main goal. Users value and want security and privacy functionality as secondary to completing their primary tasks (Karahanna et al, 1999). But Cranor said: "Many people believe that there is an inherent tradeoff between security and usability… But people need to use computers, and if there is not a secure one available, they will use insecure computers.... systems that are usable but not secure (Cranor and Garfinkel, 2005). A focus on the psychological dimensions of security has emphasized ease of use. D'Hertefelt also argued "that the feeling of security experienced by a user of an interactive system does not depend on technical security measures alone. Other (psychological) factors play a determining role". This then suggests that "The feeling of security experienced by a

user of an interactive system is determined by the user's feeling of control of the interactive system." (D'Hertefelt, 2000). Aligning security and usability is a core aspect of user-centered security. As (Tognazzini, 2005) says: The goal of security is not to build systems that are theoretically securable, but to build ones that are actually secure.... It requires close examination not only of the technology, but also of the human beings that will use it.

Wassermann (2002) in his Ph.D work on Techniques and Tools for Engineering Secure Web Applications said that “Web applications have brought with them new classes of computer security vulnerabilities, such as SQL injection and cross-site scripting (XSS), that in recent years have exceeded previously prominent vulnerability classes, such as buffer overflows, in both reports of new vulnerabilities and reports of exploits. SQL injection and XSS are both instances of the broader class of input validation based vulnerabilities. At their core, both involve one system receiving, transforming, and constructing string values, some of which come from untrusted sources, and presenting those values to another system that interprets them as programs or program fragments.“ (Gary Michael Wassermann, 2002)

Building on this characterization, his work also contributed practical algorithms for runtime protection, static analysis, and testing-based analysis of web applications to identify vulnerabilities in application code and prevent attackers from exploiting them. This dissertation additionally reports on implementations of these algorithms, showing them to be effective for their respective settings. They have low runtime overhead, validate the definitions, scale to large code bases, have low false-positive rates, handle real-world application code, and find previously unreported vulnerabilities. His work depends on user experience and centers mainly on the input validation to secure the network of computers in the web from vulnerabilities and thus secure the network.

2.3.1 Challenges for a mobile banking solution In Internet Banking

Key challenges in current internet banking application are:

1. **Handset operability:** There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. The desire for interoperability is largely dependent on the banks themselves.
2. **Transaction Security:** Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most

complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

Based on this challenge, the following issues need to be addressed in order to offer more secure infrastructure for financial transaction over wireless network:

i. Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
ii. Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
iii. Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
iv. User ID / Password authentication of bank's customer.
v. Encryption of the data being transmitted over the air.
vi. Encryption of the data that will be stored in device for later off-line analysis by the customer.

3 **Scalability and reliability:** Another challenge for M-banking is to scale-up the mobile banking infrastructure to handle exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find mobile banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence.

4 **Application distribution:** Due to the nature of the connectivity between bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates and download necessary patches.

5 **Personalization:** It would be expected from the mobile application to support personalization such as :

a. Preferred Language
b. Date / Time format
c. Amount format

d. Default transactions
e. Standard Beneficiary list
f. Alerts.

2.3.2 Security Concerns in Internet Banking

The concerns of internet banking users about security issues differed in their nature and extent. The users comprise of four categories. The first group comprised of people who did not use Internet banking because of a lack of Internet access or perceived lack of usefulness and so did not grapple with the security and privacy issues of Internet banking. The second group had Internet access but did not use Internet banking because of security fears.

They felt that the necessary infrastructure are not in place and so Internet security could not be achieved; had little expertise on the use of Internet or had experienced financial loss personally or in their circle of friends and family. The third group included people who used Internet banking but continued to be intensely worried about the security. The convenience and usefulness of Internet banking together with risk minimization strategies helped them overcome their security fears and use Internet banking. The fourth was a larger group of Internet banking users who were somewhat concerned about security, or thought they should be, but trusted that the bank would look after them.

End users of the internet banking model are those users who put the entire network to use and put on risk at the same time. They are mainly the third and the fourth category. Their education is very crucial and has importance as well. The end user education on security threats and how to avoid them play major role in keeping network up and securely running. There are threats in the use of internet banking which can be avoided if such incidences are updated with a view to putting in place a countermeasure. Bener concluded in his Ph.d thesis that users of internet banking system perceives risks based on trust and credibility they assign to the bank and disregard the security measures taken by the bank (Bener Ayse, 2000). This informs why majority of internet banking users fell into the fourth category. The researchers Hoffman et al (1999) found out that the reason more people have yet to shop on-line or even provide information to companies on the internet is because of inherent **risk** associated with such transactions. Hence in internet transactions, customers' trust and loyalty will always remain important features of Bank-customers relationship just as they are in the physical world. To this end, an enhanced model for internet banking that will be able to address security of all possible avenues of entry which affect data integrity is necessary. The security

of that entry point must be consistent with the company stated policy on acceptable **Risk** levels.

2.4 RISK

What is Risk?

For banks to tackle and enhance network security, there is need to determine the threats and subsequently design a system that will address those threats.

Douglas (1990) explained that, "Risk refers to external dangers such as natural disasters and threatening behaviors by enemies".

Webster's dictionary defines risk as: "Possibility of suffering harm or loss, a factor, course or element involving uncertain danger."

Vlek and Stallen (1981) gave a more detailed definition of risk. They took an approach that risk can be measured. According to them risk is the probability of a loss or the size of the possible loss. Therefore risk is a function, mostly the product of probability and size of loss. Courtney (1977) and Fitzerald (1978) came up first with risk analysis methods.

Courtney (1977) defined risk as the "*product of probability of an exposure occurring a given number of times per year (p) and the cost (or loss) (c) attributed to such exposure:*

Therefore risk (R) is;

$$R = P \times C \ldots\ldots\ldots\ldots (1)$$

For example if the risk exposure is once in three years (P = 1/3 or 33.33% probability in one year) and the estimated loss =N=100,000, then the magnititude of risk would be =N=33,333. The security professionals would then be analyzing the cost of establishing new controls and justify the cost vis-à-vis the risk quantity. Baskerville (1993) argues that this approach to quantifying risk is inadequate. The reason is that risk probabilities (P) and loss estimates (C) are highly interpretative and these values are manipulated with positivistic and logical mathematical calculations. However, it lacks ability to establish feedback regarding the effectiveness of the security mechanism. Lictenstein's research has revealed that, although each organization or institution chooses a different method for risk assessment prior to development of an information system, most use economic or statistical approaches and in

their approaches seven common factors have emerged as significant: usability, credibility, complexity, completeness, adaptability, validity and cost.

2.4.1Types of Risks in Internet Banking

Internet banking hand book (1998) identifies the following risks in internet banking:

a) Operational Risk: -

i. Operational risk, also referred to as transactional risk is the most common form of risk associated with i-banking.

ii. It takes the form of inaccurate processing of transactions, non-enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access/intrusion to bank's systems and transaction, etc.

iii. Such risks can arise out of weaknesses in design, implementation and monitoring of banks information system.

iv. Besides inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers/hackers, etc. can become potential source of operational risk.

b) Security Risk: -

i. Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc.

ii. Other related risks are loss of reputation, infringing customers' privacy and its legal implications, etc.

iii. Attackers could be hackers, unscrupulous vendors, disgruntled employee or even pure thrill seekers.

iv. In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employee being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank.

v. Unless specifically protected, all data/ information transfer over the internet can be monitored or read by unauthorized persons.

c) System architecture and design: -

i. Banks face the risk of wrong choice of technology, improper system design and inadequate control processes.

ii. Numerous protocols are used for communication across internet. Each protocol is designed for specific types of data transfer.

iii. A system allowing communications with all protocols, say HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), telnet, etc. is more prone to attack than one designed to permit say, only HTTP.

iv. Many banks rely on outside service providers to implement, operate and maintain their e-banking system.

v. Security related operational risk include access control, use of firewalls, cryptographic techniques, public key encryption, digital signature, etc.

d) Reputational Risk: -

i. Reputational risk is the risks of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship.

ii. The main reasons for this risk may be system or product not working to the expectations of the customers, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if, there are, no alternative means of account access.

e) Legal Risk: -

i. Legal risk arises from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established.

ii. A customer inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions.

f) Money Laundering Risk: -

i. As internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities.

Application of money laundering rules may also be inappropriate for some forms of electronic payments.

ii. To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, and frame policies in internet transactions.

g) Cross-Border Risks: -

i. Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks.

ii. Such considerations may expose banks to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record keeping and reporting requirements, privacy rules and money laundering laws.

iii. The foreign-based service provider or foreign participants in internet banking are sources of country risk to the extent that foreign parties become unable to fulfill their obligations due to economic, social or political factors.

h) Strategic Risk: -

i. For reducing such risk, banks need to conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance.

ii. Also they need to analyze the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage.

i) Other Risk: -

i. Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in internet banking.

ii. These risks get intensified due to the very nature of internet banking on account of use of electronic channels as well as absence of geographical limits.

iii. Credit risk: Is the risk that a counterparty will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the creditworthiness of the customer while extending credit through remote banking procedures, which could enhance the credit risk.

iv. Another facility of internet banking is electronic money. It brings various types of risks associated with it. If a bank purchases e-money from an issuer in order to resell it to a customer, it exposes itself to credit risk in the event of the issuer defaulting on its obligation to redeem electronic money.

v. Liquidity risk: It is important for a bank engaged in electronic money transfer activities that it ensures that funds are adequate to cover redemption and settlement demands at any particular time. Failure to do so, besides exposing the bank to liquidity risk, may even give rise to legal action and reputational risk.

j) Risk of unfair competition: -

i. Internet banking is going to intensify the competition among various banks. The open nature of internet may induce a few banks to use unfair PRACTICES to take advantage over rivals. Any leaks at network connection or operating system, etc. may allow them to interfere in a rival bank's system.

ii. Thus, one can find that along with the benefits internet banking carries various risks for bank itself as well as banking system as a whole.

k) Legal and Reputational Risk Management: -

i. Appropriate disclosure for e-banking services.

ii. Privacy of customer information

iii. Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services.

iv. Incident response planning.

2.4.2 RISK COMMUNICATION

The attention to risk communication has grown as a result of the failure of the risk communicators "to get the message across". DeVito risk communication as "the act of sending and receiving messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback (DeVito, 2000). That denotes that even when the goals of communication suggest the need for one-way transfer of information, it is critical to obtain feedback from the recipients in order to ensure that the message has indeed been understood.

According to US National Research Council; "Risk communication is an interactive process of exchange of information and opinion among individuals, groups and institutions. It involves multiple messages about the nature of risk and other message not strictly about risk, that express concerns, opinions and reactions to risk messages or to legal and institutional arrangements for risk management" US Department of Defence (1986).

Therefore, figure 2.1 shows that risk communication consists of a complex 'tangled web' of messages, signs and symbols Krimsky and Plough (1988). This highlights that, besides the intended risk messages, there may be other unintended messages transmitted through signs

and symbols. These unintended messages may result in outcomes which are not predicted and there is always some degree of uncertainty about the outcome, before a message is transmitted. In addition, because most hazards have a history, this influences the receiver's interpretations of the messages.

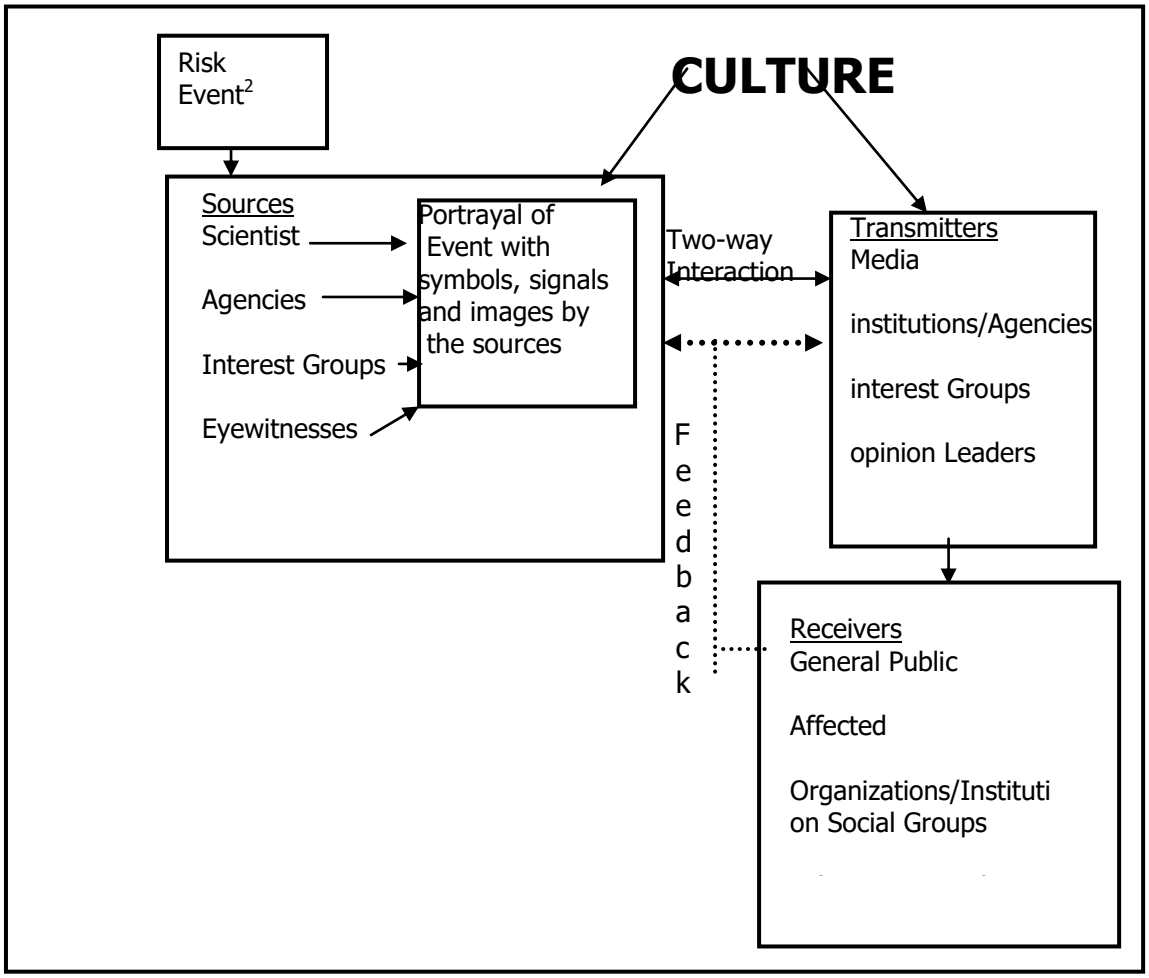


Figure 2.1 Risk Communication Process (Adapted from Renn 1991)

For risk communication is essential for effective risk assessment. The concept of *risk assessment* is crucial to developing proportionate defenses. To perform a risk analysis, organizations need to understand possible threats and vulnerabilities. Risk can then be summarized as the probability that a vulnerability will be exploited. The basic steps for risk assessment are as listed:

1. Identifying and prioritizing assets;
2. Identifying vulnerabilities;
3. Identifying threats and their probabilities;
4. Identifying countermeasures

5. Developing a cost benefit analysis

6. Developing security policies and procedures.

To identify and prioritize information assets and to develop a cost benefit analysis, it is helpful to ask a few simple questions such as the following.

a. What do you want to safeguard?
b. Why do you want to safeguard it?
c. What is its value?
d. What are the threats?
e. What are the risks?
f. What are the consequences of its loss?
g. What are the various scenarios?
h. What will the loss of the information or system cost?

Response to these questions provides the risk assessment which is paramount in developing appropriate internet banking system.

2.5 Trust And Credibility of Internet Banking

2.5.1 Trust and Confidence vs. Credibility

Trust is a wider concept than security. Trust plus Confidence breeds security in internet banking. People speak of trust most clearly when they speak of a lack of trust. This is especially so in situations where there is a greater risk and where information is less easily available (George 2002). Issues of trust and the use of electronic money are increasingly being discussed (Sohail and Shanmugham, 2003, , Suh and Han, 2002).

It is important to disentangle the concepts of security and trust, because even "usable security" is not always a sufficient condition for trust. Fishcher emphasised the importance of human values in establishing and maintaining trust for the effectiveness of the information infrastructure. They said that: "The common good of our information infrastructure depends on designs through which users can establish and maintain trust and accountability. Without preserving such human values, users will be reluctant to embrace this infrastructure as a means for conducting their daily affairs -- commerce, communication, health, work, and education" (Fishcher, 1998).

Separating trust and security means distinguishing between "issues of 'hard trust,' which involve authenticity, encryption, and security in transactions, and issues of 'soft trust,' which

involve human psychology, brand loyalty, and user-friendliness..” (Gefen, 2003). Sohail and Shanmugham (2003) unpack issues of soft trust and electronic money. They conclude that the user has to feel he or she is in control of the information, that he or she has comfort in the use of the service or channel.

Trust is an important ingredient in any trade transaction (Pavlou, 2003). As Jarvenpaa et al, (2000) describes: “Trust is a highly problematic but recurrent feature of social relationships. Thus trust cannot be fully understood and studied without the examination of institutions as repositories of a legacy of values and without addressing a practical issue of how far human beings’ concepts of duties and obligations are influenced by the societal institutions which organize ways in which people are bound together”

Trust acts as the mitigating factor for the risks assumed by one party on the party in the trade. Therefore as trust increase, the risk either reduce or become manageable by the trusting party. The existence of trust also allows reduction of the transaction costs in any transaction (Pavlov, 2003), as other costly means to reduce or manage the risks would be unnecessary. To understand better the meaning of trust, the various Authors’ definitions of trust are looked into in Tables 2.1

Table 2.1 Definitions of Trust

Relevant Findings	
Jarvenpaa et al. (2000)	Willingness to buy in an Internet store was affected by attitude and perception of risk. Attitude and perception of risk were affected by trust, which in turn was affected by consumer’s perception of size and reputation of the store.
Suh and Han (2002)	Trust had a significant effect on intention to use and attitudes toward using Internet banking.
George (2002)	Privacy and Internet trustworthiness were significant determinants of attitude toward Internet purchasing. In turn, attitude had a significant effect on

	intent to purchase.
Gefen (2002)	Purchase intention was influenced by trust, which in turn, was affected by integrity and benevolence.
Bhattacherjee (2002)	Consumers' willingness to transact online was influenced by trust, which in turn was affected by familiarity. Familiarity was significant on consumers' willingness to transact.
Gefen et al. (2003)	Trust was a significant predictor of purchase intention for both potential and repeat customers. Familiarity and disposition to trust were significant on trust for both customers.
Sohail and Shanmugham (2003)	Trust in one's bank had a significant influence on him or her to use Internet banking. Other factors were Internet accessibility, attitude towards change, computer and Internet access costs, security concerns, ease of use, and convenience.
Pavlou (2003)	Trust was a significant predictor of intention to transact in both samples. Trust had a significant effect on perceived risk, perceived usefulness, and perceived ease of use.

The definitions explained that the literature on the sociological concepts of trust can be grouped into three:

1) Individual attributes such as feelings, emotions and values.
2) Social attributes such as a common goal to be achieved by an organization.
3) Public value such as institutional trust.

Although the term "confidence" is used by many to mean trust, there is a slight difference in the meaning of confidence from various definitions of trust. According to Giddens (1994) trust is a matter of individual determination and involves choosing from alternatives while confidence is more habitual expectation. Confidence actually builds up over a long period of time, if a trusted party does not disappoint the trusting part. Hence, "Confidence denotes the subjective expectation of receiving trustworthy information from a person or an institution" (Renn and Levine 1991). Furthermore, if more than one person has the same level of confidence for the trusted party, then the trusted party is said to be "credible".

Figure 2.2 illustrated these levels.

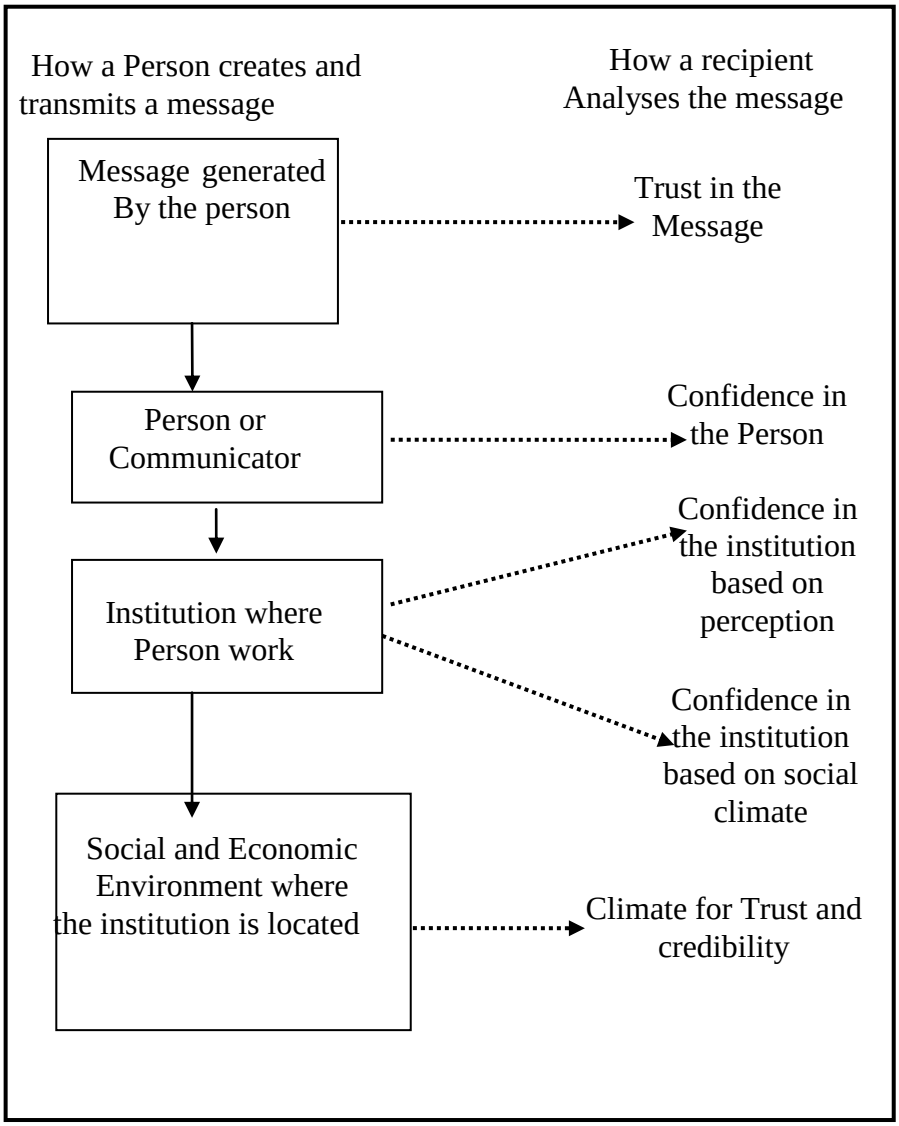


Figure 2.2 Five Levels of Trust Analysis Frame Work (Giddens 1994)

2.6 Computer Security Background

An overview of the historical developments (Bener, 2000) showed that computer security has four different fields as shown below:

1. Software engineering,
2. Computer security design,
3. Information systems security,
4. Human-computer interaction in security (HCISec).

The review of the different fields identified the main weakness to be the need to accommodate human factors in the design of a secure computer system. Access authorization restricts access to a computer or group of users through the use of authentication systems. These systems can protect either the whole computer – such as through an interactive logon screen – or individual services, such as an FTP server. There are many methods for identifying and authenticating users, such as passwords, identification cards, and, more recently, smart cards and biometric systems. Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message, but eavesdroppers cannot.

Firewalls are systems which help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic which can pass through them, based on a set of system administrator defined rules.

Honey pots are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.

Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

Pinging -The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer they can try a port scan to detect and attack services on that computer.

Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.

2.7 Participation in System Design

The intrinsic notion of participation implies the involvement of more than one party. It is a process in which two or more parties influence each other in making plans, policies or

decisions. It is restricted to decisions that have future effects on all those making the decisions or on those represented by them. Participation in information system design is very important to the success of a system.

2.7.1 Information and Computer Security

The most widely held definition of information security by Wikipedia is described as a set of properties that must be upheld. Commonly referred to as the CIA of security, the BS7799/ISO17799 standard describes information security as the protection of information for:

1. **Confidentiality**: protecting sensitive information from unauthorized disclosure or intelligible interception.
2. **Integrity**: safeguarding the accuracy and completeness of information and computer software.
3. **Availability**: ensuring that information and vital services are available to users when required.

Berner defined Computer security as the technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system. Berner also argued that the CIA definitions are incomplete in that they are only aspects of access control and put their emphasis exclusively on the prevention of undesirable events. He therefore proposes other desirable properties, such as:

Accountability: audit information must be selectively kept and protected so that actions affecting security can be traced back to the responsible party.

Dependability: the property of a computer system such that reliance can justifiably be placed on the service it delivers.

He defines security as relating to the protection of assets. Protective measures can be roughly classified into prevention, detection and reaction:

Prevention: Measures that avert damage to an asset.

Detection: Measures that afford the knowledge of when, how and who has damaged an asset.

Reaction: Measures that stop ongoing damage and recover from damage to an asset.

Additional categories of avoidance and deterrence should also be included in this list:

Avoidance: Measures that discontinue the possibility of a given threat, or transfer liability to a third party.

Deterrence: Measures that discourage the abuse of and damage to an asset.

Although deterrence could be subsumed under the notion of prevention, it is useful to distinguish that deterrence is both aimed only at people (i.e. the source of attacks) and is understood to be fallible (i.e. it does not prevent an attack, it merely discourages an attacker from engaging in one). A number of authors have pointed out that the assumption that there is a "silver bullet" – protective measures must be absolutely perfect in order to be of any use for security. This assumption can still be seen in attitudes and statements from experts, for instance:

"Firewalls can be effective only if all traffic must go through them to get from the outside of the protected network and vice versa".

This implies that unless they satisfy the given condition of *"all traffic must go through them"*, firewalls are completely ineffective, as opposed to having a diminished effectiveness.

Parker proposes new definitions of security which should be rated in terms of:

Availability: usability of information for a purpose.

Utility: usefulness of information for a purpose.

Integrity: completeness, wholeness and readability of information and quality being unchanged from a previous state.

Authenticity: validity, conformance and genuineness of information.

Confidentiality: limited observation and disclosure of knowledge.

Possession: the holding, control and ability to use information.

The difficulty with these new definitions is that they involve highly subjective notions, such as usefulness, genuineness, or readability. It is more important to discuss the need for and extent to which these concepts are necessary in a given system.

Yet other experts prefer to describe security as ideals to be achieved. Ross Anderson, for example, describes the field of security engineering as "building systems to remain dependable in the face of malice, error or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves."

For the purposes of the following, a system represents the combination of technical, managerial and human components working together for the accomplishment of specified goals:

Security deals with the deterrence, avoidance, prevention, detection and reaction to events in a system that are undesirable to the owner of that system.

This definition is useful in that it distinguishes between:

1. How security works – deterrence, avoidance, prevention, detection and reaction.

2. What security applies to – undesirable events in a system.

3. Who requires security – the owner of the system.

2.7.2 Human-Computer Interaction (HCI)

Central to HCI is the notion of usability. Usability can be defined as the ease with which a user can learn to operate, prepare inputs for, and interpret outputs of a system or computer. Given this definition, a significant portion of HCI is concerned with user interfaces to software systems. While usability and user interface design can be said to be looking at the issues of making a given interaction easier, HCI design has come to develop a broader picture, which includes identifying and resolving conflicting goals in a socio-technical system consisting of the stakeholders and their activities. These properties can strongly influence the design of a system, most visibly at the interface level, but also at a more fundamental level such as the underlying model of operation of the system. For example, problems can arise if users' mental models of the operation of the system differ from its real operating model.

2.8 Computer Security Design

It is commonly argued that the security must be designed into a system and not added as an afterthought. However in practice, most systems have security added-on, which can result in security that is ill-suited, expensive to maintain and inefficient. The reasons why some systems continue to be designed without security can fall into three categories:

1. Security is deliberately sacrificed in the design, for example, because of time and cost concerns.

2. Security is not viewed as important. For example many security problems in the Internet or email have their roots in the fact that security was not considered to be necessary during their initial design – a design that was originally viewed as a proof of concept.

3. Security is desired, but the wrong decisions are made during design and implementation.

Computer security design aims to address the problem identified in point 3, which is to ensure the means of building good security. There are three separate aspects to designing security that are necessary for a successful system:

1. Knowledge of security.

2. Reasoning and decision making.

3. Knowledge of the system.

2.8.1 Knowledge of Security

Much of the literature about computer security relies on anecdotes to relay information about past exploits and crimes. These give insight into the inventiveness, mistakes and methods that attackers have used in the past. Anecdotes prove to be useful in two distinct ways:

_ They supply information about past attacks and defenses.

_ They provide an insight into future attacks.

The disadvantage of using anecdotes is that they are not:

_ Succinct.

_ Versatile.

The information contained within an anecdote is hard to summarize and therefore hard to impart to third parties. In addition, the lessons that can be learned from one given attack can only be applied to a different area with great care, as the environment will probably be completely different.

2.8.2 Reasoning and Decision Making on security

The most widespread methods for reasoning and making decisions about security can be grouped into four categories:

· Descriptive and *ad hoc* methods,

· Checklists,

· Guidelines,

· Risk management.

2.9.0 Descriptive and ad hoc Methods

Descriptive and *ad hoc* methods tend to follow from the experience of an individual or a small group of practitioners. Much of the advice generally given in these methods is in the form of stories or case studies. They describe in detail many aspects of computer security and illustrate them with appropriate examples. They do not, however, prescribe a method for securing a system or developing a system securely.

2.9.1 Checklists

Checklists are fixed, sometimes numbered, lists of steps that you are told to take in order to secure a system. The advantage of checklists is that they provide easily used and applied information about security and also provide a means of measuring or auditing the security in a system.

A main disadvantage with checklists lies in their rigidity, making them ill-suited for more specialized security tasks. Although checklists can be useful in providing a baseline for computer security, they are not intended to be complete and the temptation exists to assume that by complying with a checklist no further security actions are necessary.

2. 9.2 Guidelines

Guidelines are words of wisdom, intended to impart security developers with the principles they should follow in order to make computers secure. Sometimes mislabeled as checklists, they impart advice as to desirable properties of a system, but do not describe means of achieving this in practical terms.

The biggest problem with guidelines is that they do not provide practical assistance in building security – rather they state what the intent of the security should be. A particular example relating to the need for usable security states frequently that the system should be *"usable"* and *"understandable"*, yet fails to explain means of achieving these laudable goals.

2.9.3 Risk Management

Risk is defined as the probability that a threat will act on a vulnerability to cause an impact. In security terms, a threat is the potential source of an attack and a vulnerability is an area of the system that is susceptible to exploitation. Risk management is the method many experts consider to be the most flexible and comprehensive for securing a system.

Through risk mitigation, the onus is put on developing countermeasures to reduce risks which are deemed to be too high in relation to the impact of an attack.

2.9.4 Knowledge of the System

In HCI design techniques, knowledge of a system is gained by gathering and understanding information about the users of the system, as well as the technical requirements of the system. In security design, knowledge of the system tends to be gained through the *evaluation* of the security of the system.

2.9.5 Human-Computer Interaction in Security (HCISec)

2.9.51 Usability and Security

Adamsom cited , "… attributes the Russian disasters of World War 1to the fact that their soldiers found the more sophisticated army cipher systems too hard to use, and reverted to using simple systems which the Germans could solve without great difficulty".

This statement expounds the notion that mechanisms for strong security are hard to use.

Bruce Schneier makes the point that "… security is only as good as its weakest link, and people are the weakest link in the chain". Other authors also argue that secure systems are broken through human issues, e.g. because an administrator makes a mistake in configuring a system. This indicates that ease of use is necessary in order to get people to behave securely, and therefore good security should be easy to use if it is to be applied.

Zurko & Simon identify three major groups of people whose usability needs must be addressed:

1. Users
2. Administrators
3. Developers

Other research also suggests that actually improving the usability of secure systems for users results in more effective security mechanisms, which benefits a fourth group:

4. System owners

2.9.52 Usability of Security and Dependability

It has been argued that in security research "correctness' is not the issue; but dependability". The point is that knowing that the system will behave and be used in the expected manner (dependability) is as much of a problem as knowing that a system will counter a threat if used correctly (correctness).

The ***owner*** of the system benefits from security by **dependably**:

1. Allowing *desirable* interactions
2. Avoiding, deterring, preventing, detecting and reacting to *undesirable* interactions.

The ***user*** of a security mechanism in that system benefits from good usability because it:

1. Facilitates the correct execution of the user's *desired* interaction
2. Impedes the incorrect execution of the user's *desired* interaction

In effect, increased usability results in fewer errors and a smaller mental or physical cost to the ***user***.

As a result, the ***owner*** of the system benefits from usability because it increases the dependability of the security – *but only if the user's desired interactions match the owner's desired interactions.* It should also be noted that a user refraining from engaging in a *desired interaction* can be considered an *undesirable interaction*.

This now highlights three different security issues (see Table 2.3):

1. A user intentionally desires an interaction the owner does not with malicious intent (e.g. criminal intent)

2. A user intentionally desires an interaction the owner does not without malice.

i. The user does not perceive the interaction as being detrimental to the owner. Either the user comes to an inaccurate conclusion through incomplete information (about security, the system, the risks, etc.), or comes to a different conclusion based on the same information (differences of judgment in security)

ii. The user has greater incentive than disincentive to engage in the interaction (e.g. a user may decide to break the security policy because the user's bonus is only tied to achieving production targets – not achieving security that interferes with these targets.

Another example may be that disciplinary measures for security breaches are not enforced, therefore the disincentive for breaking the policy is very small)

iii. The user cannot behave in the manner desired by the owner

3. A user unintentionally desires an interaction the owner does not (e.g. misunderstanding, errors or confusion)

Points (2) and (3) are generally those that are exploited through *social engineering*, either by manipulating users through their desire to be helpful (2.i) or by deceiving them into unintentionally breaking the rules (3).

Social engineering is the term used to refer to attacks that target authorized users of the system – as opposed to technical components – and attempt to manipulate them into revealing information (such as passwords) or otherwise compromising the system.

Interaction– Intentional, Unintentional. Desirable - Good security, Chance

1. Malicious Undesirable

2. Non-malicious Crime

i. User perceives interaction as harmless

ii. Greater user incentive for undesirable interaction

iii. User incapable of desirable interaction

3. Error

Table 2.3: Analysis of user intention vs desirability of an interaction.

Interaction	Intentional		Unintentional
Desirable	Good Security		Chance
Undesirable	1. Malicious	2.Non-malicious	3. Error
	Crime	User perceives interaction as harmless. Greater user incentive for undesirable interaction. User incapable of desirable interaction.	

2.9.53 Usability in Security Technologies

Anthonio (2008) in their work pointed out that "Security technologies are making advances in protecting valuable information systems assets such as data and networks. However, this is of no use if the users that these systems are intended to assist in their day-to-day work find them obstructive. This is a serious problem facing information security experts, because traditionally more attention was focused on the functionality of systems – especially security systems – with little or no consideration to the usability of such systems. Achieving total security is impossible, as security is a moving target."

There are, however, noticeable advances in developing security technologies that enhance the functional aspects of a security system so as to mitigate the ever-increasing sophisticated threats that prevail in today's internet environment. The main challenge is getting the buy-in of users and embedding their behavior in a real security culture where they take responsibility and show accountability. This task is extremely challenging and proving nearly impossible, since human behavior cannot be predicted or guaranteed. From their stand point, it highlights the necessity of designing a more sophisticated internet security model that will not impact on users experience and knowledge.

2.9.6 Summary

The use of new distribution channels such as the internet and electronic commerce increases the importance of security in information systems – internet banking system. This is because these systems are opened up to the environment and therefore leave organization more vulnerable. Hence in internet transactions, customer trust and loyalty will always remain important features of company-customers relationship just as they are in the physical world.

Companies realize that doing business on the internet involves some risk just like any other business transaction. However, if the companies install secure procedures, the internet is not riskier than other business. Various work reviewed in this work on internet banking security model recognize the user as the weakest point. Security should not be an add-on but should be considered and incorporated while designing the model, for it to serve the desired purpose. Use of internet banking system in Nigeria had been on the increase from a paltry sum of 0.06% in 2002 to 32.9% in 2012 according to Nigerian minister of information.

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. A healthy security culture is created by taking into consideration human aspects that make it difficult for users to comply with security requirements. 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 twenty two banks in the country becomes necessary.

CHAPTER THREE

SYSTEM ANALYSIS AND METHODOLOGY

3.1 Introduction

Online banking systems require efficient Network security models capable of identifying users and authorizing transactions, thus mitigating fraud. However, existing current models are focused more on fraud identification and less on fraud prevention, which means that most times actions are taken only after fraud had occurred instead of performing a series of preventive procedures. 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.

3.1.2 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 3.1 below showed some of the security models currently adopted in internet banking by banks in Nigeria. However, banking trojans had continued to successfully operate, hence directing security to reactive fraud identification rather than prevention.

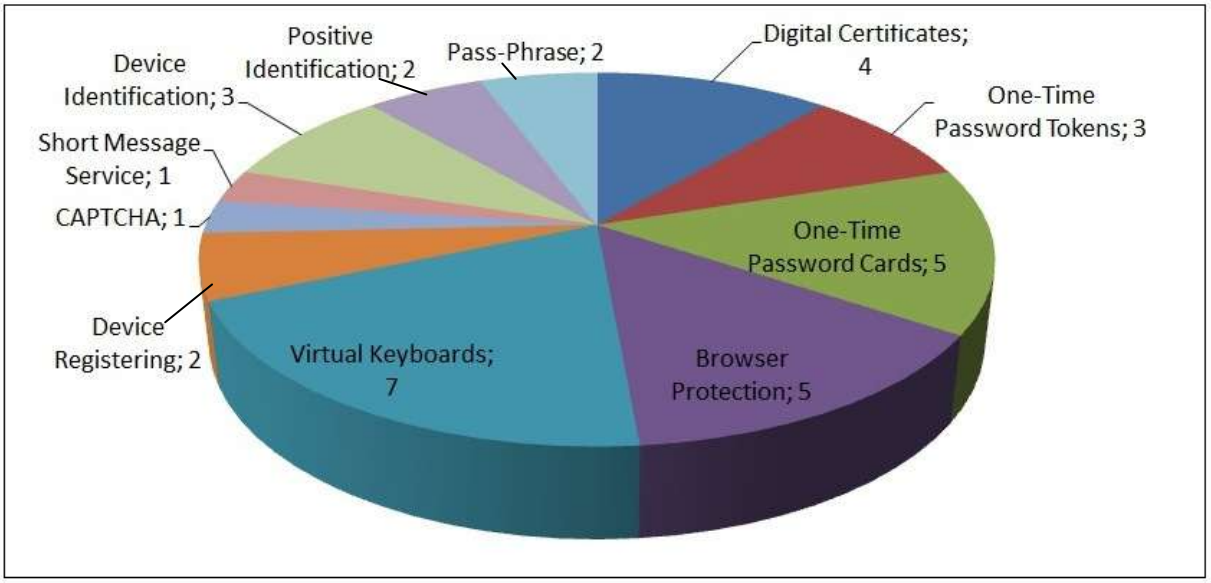


Figure 3.1: Current Internet Banking Security Models (adopted from International Journal of Computer Science & Information Technology (IJCSIT), 2011).

These models in figure 3.1 function as follows:

Digital Certificates: Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity.

One-Time Password Tokens: One-Time Password devices are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices will render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.

One-Time Password Cards: One-Time Password Cards constitute a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, there is a tendency that passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.

Browser Protection: In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.

Virtual Keyboards: In this model, the system is secured at the Internet browser of keyloggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

Device Registering: This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.

CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans: This is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.

Short Message Service (SMS): This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a

set of characters which have to be informed in order to authorize and process the transaction through the online banking system.

Device Identification: Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.

Positive Identification: Positive identification is a model where the user is required to input some secret information only known to him in order to identify himself. It is applied as a second authentication method.

Pass-Phrase: It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involve money movement.

Transaction Monitoring: It is currently applied in all online banking systems, using different techniques like Artificial intelligence, transaction history analysis and other methods that identify fraud patterns in previously processed transactions.

3.2 Advantages/Disadvantages Of The Existing security models

3.2.1 Advantages

a) The models easily identify the user and authorize access to banking transactions.
b) The identification schemes are based on two main factors: unique secret information previously shared by the user and the bank (such as passwords) and unique characteristics of the device which is being used to access the service (device fingerprinting).

3.2.2 Disadvantages

The disadvantages in existing Internet Banking Systems security models are shown in the table below.

Table 3.1

Security Models	**Vulnerabilities**
Digital Certificates	It is possible to export certificates and remotely utilize them. The certificates can be used by more than one user at the same time, allowing adversaries to use stolen certificates.
OTP Token	The generated password may be captured

	and used in real- time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering.
Browser Protection	New malware remain active until they are identified by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data (such as passwords) in an unsafe environment.
OTP Card	Malware may collect passwords or lure the user into informing them.
Virtual Keyboard	Known tools such as Screenloggers or mouseloggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied.
Device Registering	Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device.
CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information.
Short Message Service	The attacker may alter the cellular phone number to which the authorization

	messages are sent.
Device Identification	Characteristics thought to be unique to the user's device may be reproduced.
Positive Identification	Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information.
Pass-Phrase	Tools such as screenloggers, keyloggers or mouseloggers can be used to capture the secret information; Decryption techniques may be applied.
Transaction Monitoring	Recent malwares are creating behavior profiles which enable them to impersonate the user profile.

From the table above;

1. Most of the attacks directed at online banking systems target 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.
2. Indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related information leaks and security issues affecting the system and leading to fraud.
3. If any of the media through which information are collected (including the user's device) is compromised, the security system is compromised as a whole because it would allow an adversary to insert and capture information at a point of the system.
4. It is important to understand how banking systems employ security mechanisms and why they do not efficiently mitigate system subversion and consequent frauds.
5. Lack sophisticated and strong fraudulent payment detection and prevention mechanisms
6. Cannot deal with security and trust issues associated with internal user behaviour. They mostly rely on the username and password security

7. Have no strong authentication mechanisms in place to protect legitimate users' confidential information as the possibility to access other users' information remains high.
8. Has no group key (GK) mechanism which can identify users, manage them into groups and verify their authorization levels.
9. Are unable to trace and detect fraudulent transactions performed by internal legitimate users.

3.3 Analysis of The Proposed System

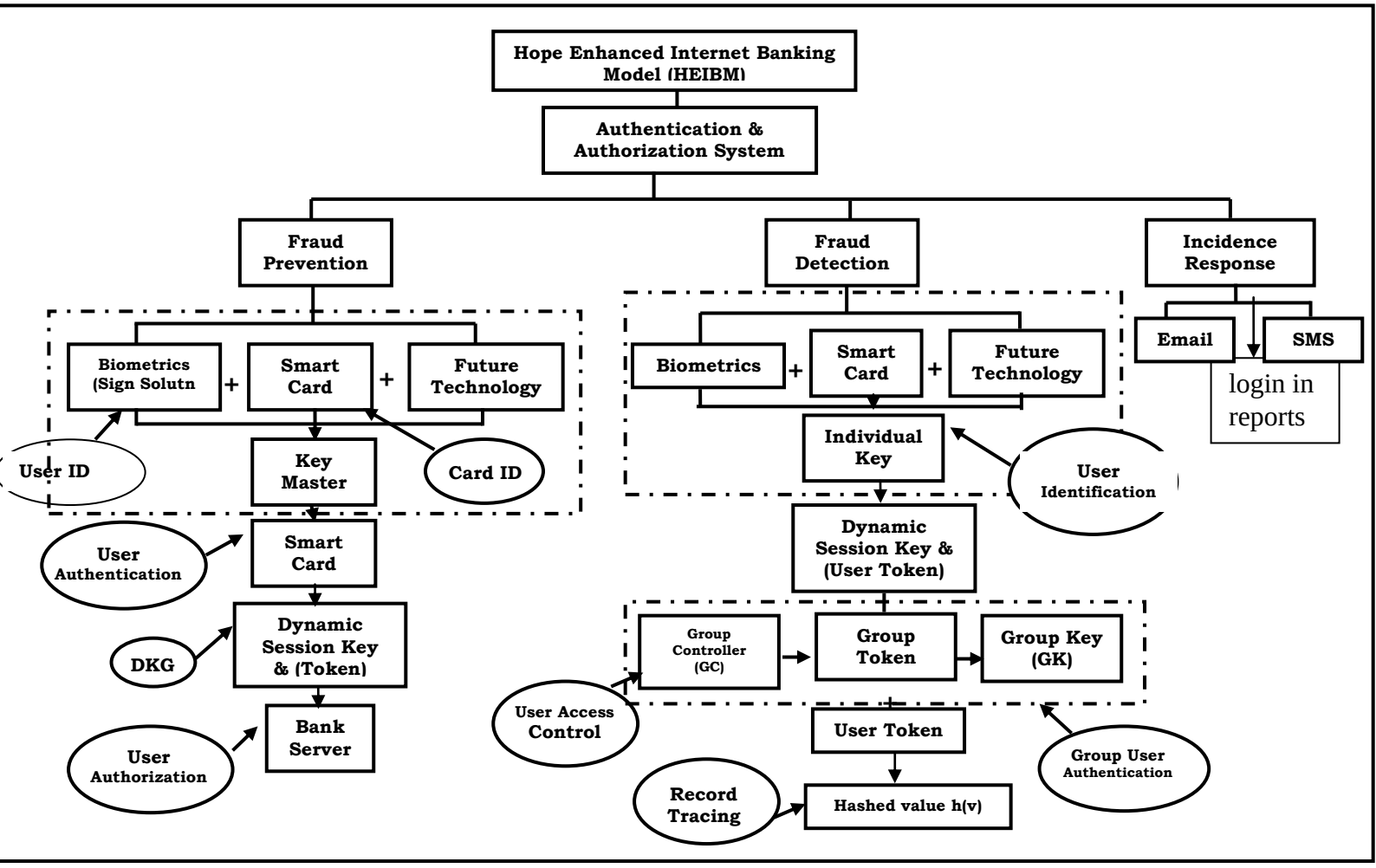


Figure 3.2: Illustration of the concept of Hope Enhanced Internet Banking Model (HEIBM).

The model considered the main target of attack on internet banking system which is the customers' 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 3.2). This is updated with more sophisticated future technologies as they emerge to ensure continuity and relevance.

Emphasis is on consistency and integrity of data, convenience and security of the model. Subsequently, fraud detection, prevention and alert systems are the crucial requirements as many banks and businesses increasingly rely on electronic transactions. Internet banking fraud involves legitimate users with some legitimate activities but also includes illegitimate activities by users other than the account holder. The model minimizes huge losses by incorporating fraud detection, prevention and alert systems. The enhanced combination of these systems made the developed security model continually effective as attackers are continuously improving in their level of sophistication.

The enhanced system combined a range of advanced authentication technologies such as smart card (Elliot S, 1998) and biometrics (Dugelay J.-L et al, 2002). It provided comprehensive, secure and sophisticated authentication mechanisms to effectively confirm user identity and to protect payment transactions details. The main concept is to apply one hash algorithm with cyclic shifting of a master secrete each time a session key is generated. Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi-Factor Authentication (ZTMA) are the major contributions of the proposed architecture as it strengthens the security of users' authentication and uses random keys to protect the sensitive data during transactions. The conceptual architecture employs a Group Key (Harney H., 1997) mechanism to maximize efficiency and security for individuals and group users. The major role of the GK mechanism is to restrict access to a different object in the system by the user, and to assure only authorized users can have access to sensitive client information and at the time protect clients by maintaining different access levels to their sensitive information, hence securing the transmitting information through open networks.

The ZTMA approach is to supplement standard authentication with "intent-based" detection, which keeps a behavioral profile of each customer based on his or her activity, examines deviations from the normal and detects fraudulent intent - providing transparent, adaptive, and continuous protection. These mechanisms satisfy all transaction security properties of payment systems as they enforce stronger authentication and authorization methods and allow protection of customers' online businesses without impacting on user's experience.

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.

3.4 Advantages/Disadvantages of the Proposed model

3.4.1 Advantages

The proposed model combined various authentication mechanisms of smart card technology, biometric details and password to identify, authenticate and authorize transactions and improve on:

a) **Operability:** The model achieves the desire for better interoperability among banks by being more "user Friendly", less complex to understand and apply among the banks and at the same time allow development of more complex capabilities with future technology.

b) **Security of financial transactions**: Being executed from some remote location, financial information and transactions are transmitted over the air. The model provides better security for financial information and transactions through:

i. Current access rules that require a stronger structure in terms of applying specific access rules using combination of Tokens and GK to apply restricted access control and security policies, which assign and manage different rules and privileges.

ii. DKG (Dynamic Key Generation) mechanism to prevent access by fraudulent users by confirming that involved parties can meet the secret keys generation requirements before they are allowed to perform transactions.

iii. Examines deviations from the normal and detects fraudulent intent using ZTMA (Zero Touch Multi- Factor Authentication) which keeps a behavioral profile of each customer based on his or her activity ("intent-based" detection), and also consider these risk factors to enhance security profile:

Credential Risk*:* Does the user have the correct password and other personal data expected?

Transaction Risk: Is the user trying to make a payment over a threshold amount or change passwords or other personal security information.

Location Risk*:* Is the user coming from an approved or previously authenticated Internet location with an expected Browser Profile and Computer Profile?

Behavioral Risk: Is the user coming at an unusual time of day, performing a transaction involving an unusual payee, or unusual amount given that users past behavior? This then provided transparent, adaptive, and continuous protection.

c) **Application distribution:** The model application allows for necessary upgrades and updates to be made, hence customers can enjoy continuously updated model without visiting the bank.
d) **Scalability and reliability*:*** The model has the capacity to scale-up the internet banking infrastructure to handle exponential growth of the customer base.

With these advantages customers' trust and confidence, as well as convenience in the use of the system is enhanced despite possible security threats.

3.4.2 Disadvantages of the proposed model

1. The proper foundation for internet banking system to optimally operate and be accepted is yet to be well established. The constant Power outage is not helping matters.
2. The literacy level of the populace is very low, hence, it may be difficult for the people to fully use and enjoy the model.

3.5 Justification Of The Proposed System

One of the biggest problems facing Internet banking today is the thorny issues of trust and security of online transactions. In fact, the vast majority of customers are concerned about the safety of their transaction, and they can't simply trust the web fearing that their transactions and credentials might not be safe due to the increasing number of online Internet attacks.

Dandash (2007), stated that "In face of the growing number of transactions processed through online banking systems, several new security technologies and models which aim at providing authenticated secure communications through known insecure channels have been introduced".

Nami (2009) also noted that "The number of malware and exploits focused on online banking systems vulnerabilities has been steadily growing during past years. Currently there is a clear need for efficient more secured models by banks which will offer online access to their banking systems".

These observations pointed out the need for something to be continuously done to address the attacks and increase people's perception of internet banking usage. Hence looking at the listed advantages of Hope Enhanced Internet Banking Model (HEIBM) over the existing models, the proposed system is justified.

3.6 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.

The Neuro-Fuzzy model does not only provide simple decision making tools but also complex adaptation algorithm using Artificial intelligence technology to control HTTP request traffic. Krzysztof (2012) said "The newly established concept of evolving intelligent systems is a result of the synergy between conventional systems, neural networks and fuzzy systems as structures for information representation and the real time methods for machine learning". 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.

Gerard (2011) said "The application of web server clusters currently has the most common technique for increasing the efficiency of a web service. Web clusters are used in services when the clients are spread over a geographical area". The model uses Web cluster technology. Web cluster consists of web switch, www servers and back end servers such as database servers.

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).

For maximum efficiency, the web uses an adaptive distribution algorithm. Adaptive algorithm learns the behavior of the service during the work to improve the quality of the decision made. It makes the best decisions while achieving the assumed goals.
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. These mechanisms satisfied all transaction security properties of payment systems as they enforced stronger authentication and authorization methods. In order to reduce the inconvenience to the end user, DKG and GK authentication mechanism is used for high-value or high risk transaction. In other words, a bank may allow users to logon and check their balances stopping with ZTMA authentication, but DKG, GK will be required to perform a funds transfer or change the account password.

Zero Touch Multi-Factor Authentication allows online businesses to protect their customers with behavioral authentication without impacting user experience. The fundamental approach is to supplement DKG and GK authentication with “intent-based” detection, which keeps a behavioral profile of each customer based on his or her activity, examines deviations from the normal and detects fraudulent intent - providing transparent, adaptive, and continuous protection.

ZTMA has a Business Signatures solution and Business Signature e-Fraud Library to the authentication. The business signatures solution considers a number of factors which are used to determine whether to admit the user after a given step or ask for more validation information.
Some of the factors considered by the Business Signatures solution are:

1. ***Credential Risk:*** Does the user have the correct password and other personal data expected?
2. ***Transaction Risk***: Is the user trying to make a payment over a threshold amount or change passwords or other personal security information.
3. ***Location Risk:*** Is the user coming from an approved or previously authenticated Internet location with an expected Browser Profile and Computer Profile?
4. ***Behavioral Risk:*** Is the user coming at an unusual time of day, performing a transaction involving an unusual payee, or unusual amount given that users past behavior?

3.7 Business Signature e-Fraud Library

Business Signatures has Real Time e-Fraud Detection (RTFD) product which continuously processes all online customer interactions, at the individual level, in real time. With this incisive visibility into all aspects of your customers' online interactions, the system can detect suspicious behavior and interdict with unprecedented precision before fraudulent transactions occur. This means uninterrupted, safe, and secure online transactions for the banks' customers without having to change their behavior.

Business Signatures e- Fraud Library offers a continuously refreshed library of e-Fraud Rules that emanate from any fraudulent activity of users. This provides out-of-the-box protection (example - Is this logon location, payee or wire transfer destination on a "black list"?) against possible fraudulent transactions.

The Fuzzy approach in the model made it possible to use inaccurate, uncertain, and sometimes, not up to date information for decision making. The neural networks provided the ability of learning and adapting to time varying environment. Some of the information handled by the fuzzy approach include:

a) Has the user changed their security information and is now trying to make an unusually large payment
b) Is this session being initiated from a referring URL from an "email" location?
   Patterns of activity from other sessions and other users are also considered.
c) Have there been multiple failed login attempts from this same location in the last 24 hours?
d) Have there been multiple successful logins from this same location in the last 24 hours?
e) Have other users recently added the same payee and made large payments in the same session?

f) Has this same user logging on from another geographically distant locations within a given time period?
g) Has a combination of the above occurred?

3.8 Unit of Analysis

The study focuses on modeling enhanced network security for internet banking transactions in Nigeria environment.

This study was chosen for these reasons:

First of all, the leading roles of wireless banking in the present Nigerian consumer banking, and the need to enhance the current technology in internet banking thereby fast tracking implementation of the currently introduced cashless transactions.

Second, there is need to build more confidence in the use of the internet banking technology, by putting in place more sophisticated model to improve existing security models.

Third, as banks are geared towards improvement in information technology to cover all e-banking services, a more trusted secured system will be an advantage for good competition.

3.9 Data Collection

Collection of data will be done through Data farming instead of Data mining. Data mining capture data from past activities in order to discover regularities and interesting correlations. Data mining has been the traditional way to assess risk and plan for the future. Unfortunately, using past data to predict what will happen can work badly, for complex systems like the Web. Neuro-Fuzzy modeling is a wonderful counter to this tendency. For systems like our internet banking networks, in which the future often differs significantly from the past, we can be deceived by the past.

The use of Neuro-Fuzzy models that include uncertainty uses data farming (a way of creating data about events that have never occurred and that, while possible, may never occur) rather than data mining. The model farm data through:

1. The process of uncertain information;
2. Automatic extraction of the rule-base;
3. Learning from examples;

This means that our model will have the ability to generate data on plausible scenarios unlike any that have occurred before. This is an important feature of Neuro-based simulations. The simulated system will farm highly useful data. Data obtained from application of Neuro-

Fuzzy technique on Hope Enhanced internet banking model (HEIBM), was used to compare the security of existing internet banking transactions, detect possible vulnerability and thus apply appropriate countermeasure(s).

3.9.1 Data Analysis

The level of risk during customer transaction for the existing models and HEIBM for authorized users were analyzed. The results were analyzed and compared so that alerts and countermeasures are set accordingly. The library of countermeasures application brings about enhancement and maximizes the banks' internet model competitive advantage.

CHAPTER FOUR
SYSTEM DESIGN

4.1 Introduction

The System modeling is intended to enhance on the performance of existing internet banking models. Currently, there are three basic kinds of Internet banking being offered by banks to their customers, namely: informational, communicative and transactional. The emphasis of the design is on transactional which is where the bulk of the internet banking risk applies.

"Recent results from usability studies of security systems have shown that end users find them difficult to adopt and use" (Smetters D.K et al, 2002). Their argument was that improving the usability of security technology is only one part of the problem. The main attention should be on designing a usable and useful systems that provide security to end users in terms of the applications that they use and the tasks they intend to achieve..

Organizations are researching new ways to improve network security, and are faced with adversaries who are continually changing their tactics and increasing the level of sophistication of their attacks. The goal here is to create an intelligent model using Neuro-Fuzzy systems to enhance the performance of our network security for internet banking. Hope Enhanced Internet Banking Model (HEIBM) used Neuro –Fuzzy modeling technique which 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 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.

4.2 HEIBM Software System Design

This starts with building a use case description for the whole system. This is done by:

1. Considering the three arms of internet banking application areas and the level of financial activity it permits the customers.

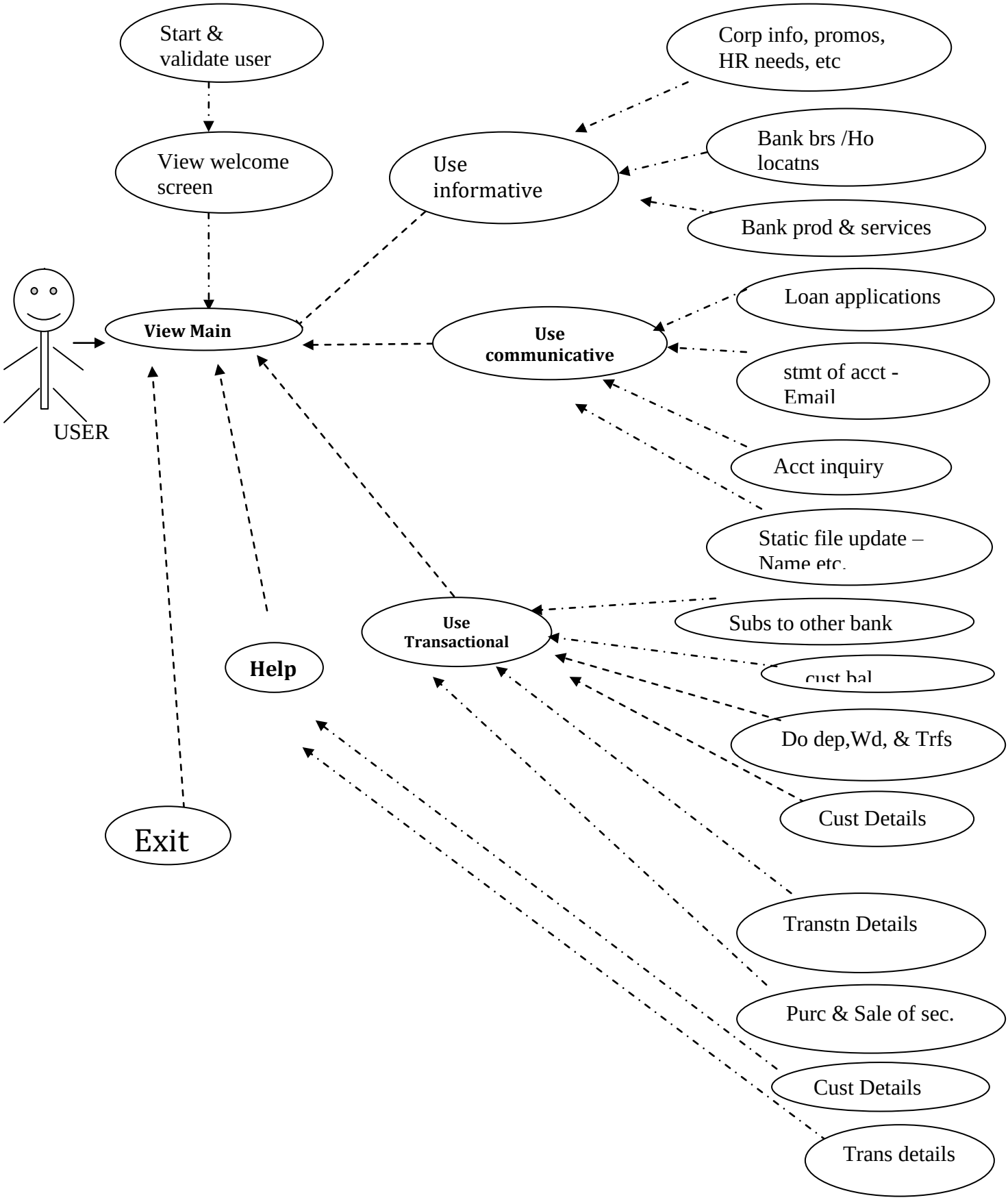


Figure 4.1 System High level diagram for the model.

2. Building a UML Use Case diagram at the system level (Figure 4.1) and at the same time provide sub use case diagrams where necessary.

The Main Menu Use case follows just after the user starts the application. The system using validation Use case validates the user, and displays the main menu. The main menu has eight modules: User Registration, User Login, Transaction, Hacking Simulation, Report, About us, Help and Exit. Transaction and Hacking Simulation modules have these sub modules of username, password, account name, account type. The use case ends when the user selects Exit from the modules.

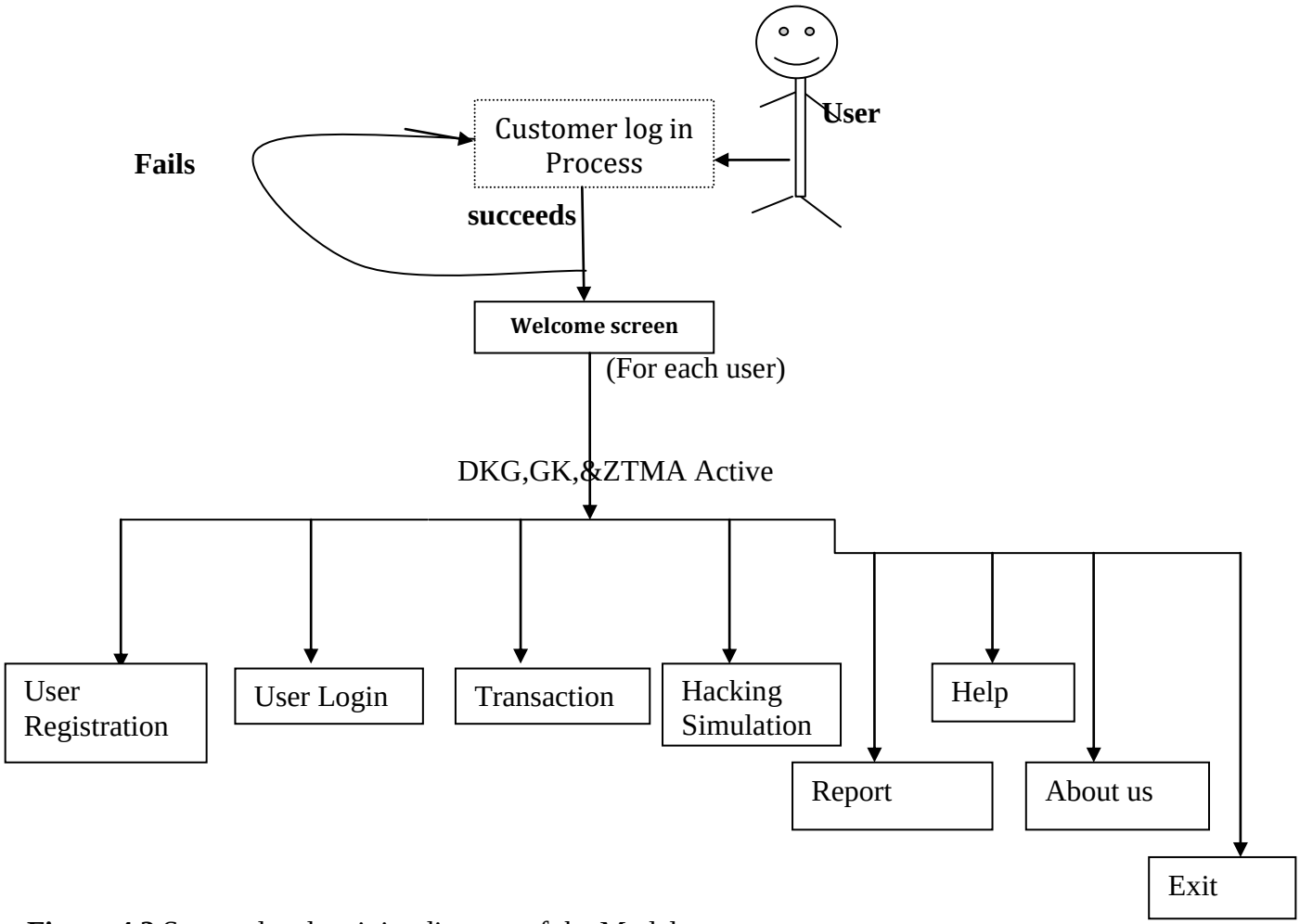


Figure 4.2 System level activity diagram of the Model.

The Start and User validation use case commences when the user starts the model application. As the application starts and welcomes user to HEIBM, it displays the login which prompts the user to enter his/her username and password. If an invalid username or password is entered, it prompts the user to enter a valid username and password. The use case ends when a valid username or password are entered or thrown out after three trials as shown figure 4.1 and 4.2.

4.2 .1Main Menu (Control Centre)

The main menu is on the transactional internet banking operations. It is the screen that appears after the welcome page. From here customer selects activity of interest. It has a total of seven subroutines.

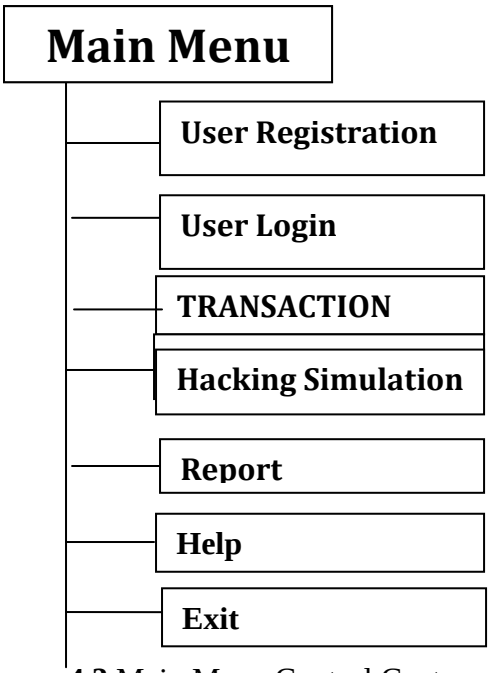


Figure 4.3 Main Menu Control Centre

Application User: This is the client who double clicks on the application to start it. The client is required to type his/her username and password when shown authorization request window. The system mutually authenticates the customer's request to open to welcome screen which leads to the main menu. 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

4.2.3 Customer Registration

To use the internet banking model, the user is already a customer of the bank. The processes are:

1. The customer applies for internet banking service by completing a form which has these details: account number, account name, bank branch and address.
2. The customers' personal and biometric details are captured by the model server.
3. The registered user is issued with a smart Card which has a unique security number and also given access password which should be used within 48hrs.

4.2.4 User Login

Access password and smart card number is used to log into the system and must be changed after the first time the user entered the banks internet banking site. Customer subsequently is admitted to welcome screen which opens up to the main menu from where activity of choice can be selected.

4.2.5 Transaction

On successful log in, customer on selection of transaction submenu, the Model server:

1. Recognizes the personal computer or the mobile of the user on the first use of the model.
2. Authenticate the user using ZTMA, DKG and GK.
3. ZTMA confirms personal characteristics of the user which is already resident in the bank server example customer geographical location, MAC address of the device, time and date of login and number of login attempts. This authentication level covers customer account enquiry, loan application etc. If the geographical location or Device is changed the model will require the user to answer personal questions. Wrong answer will throw the user out and alert users' mobile phone or email. User starts authentication process again. The user however, will be completely disabled to try after three attempts and will be enabled again for another attempt after 24hrs.
4. For more serious transaction like money transfer, cash withdrawal or change of password, ZTMA, DKG and GK will be involved.
5. On accurate supply of the smart card security number and password which is combined with existing customer biometric detail of ZTMA, the Bank server through the process of dynamic key and group key generation confirms the users request. Group controller says that customer Identification of ZTMA and smart card (SC) is in the group and generates its key which will match with that generated randomly by DKG in the bank server on

acceptance of smart card security number. Any deviation will reject users request and the users' mobile phone number or email supplied to the bank will be alerted.

6. User is required to start authentication process from the beginning again. This time around, a new security number generated dynamically for the smart card is supplied to user through SMS to mobile phone or Email for the user to supply back to the bank server. Three wrong attempts throw the user out completely and block the smart card number for 24 hours. Further failed trials after the 24 hours grace will require the user to visit the bank and apply for fresh new smart card.

4.2.6 Hacking Simulation

An unauthorized user which is an attacker with wrong smart card number or access password will be allowed three trials and then automatically thrown out by the model and record of the attack reported for audit trail.

4.2.7 Report

Reports of various transactions of each user, both authorized and unauthorized can be printed for use.

4.2.8 About Us

This handles the communicative and informational arm of the internet banking. It gives information on banks' branch locations, products and services.

4.3 Frame Chart Architecture of HEIBM

To capture the abstract description of the system, state charts are used for the specification of the reactive behavior of the system. The components of the system are active and communicate with each other as shown in Figure 4.4. To monitor the execution of the state chart, visualization framework of hammock diagram and Real - time state charts are used. "Visualization can either be in on- line mode, visualizing current behavior of a system or in off-line mode, visualizing older monitoring data" (Holger Giese et al, 2003).

Hammock diagram is a network diagram which showed the visual flow of sequence, interrelationships and dependence of all activities of the model (Mathew Sorvaag, 2011).

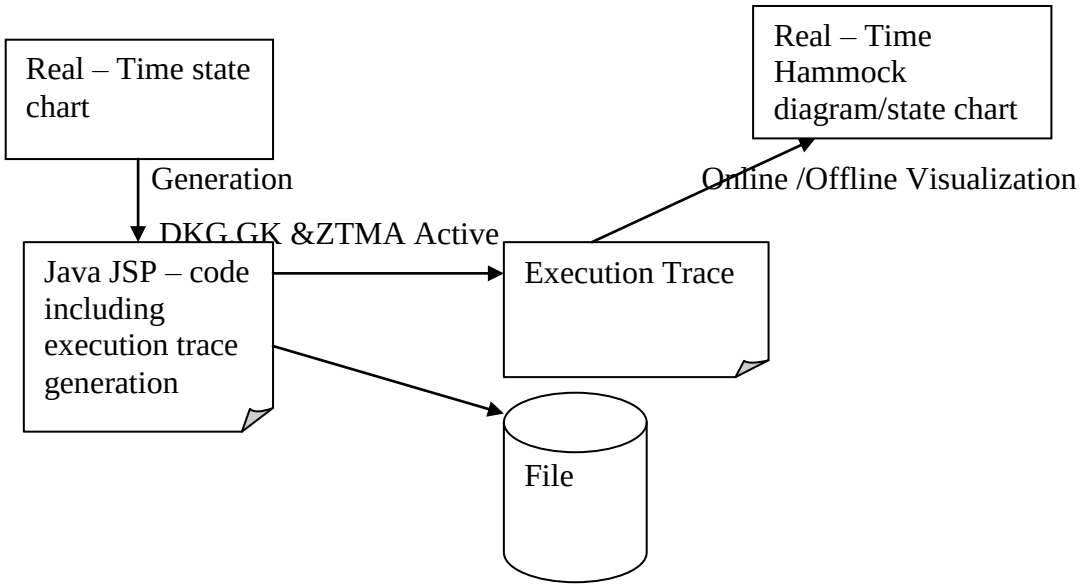


Figure 4.4: Block diagram of System Frame Chart Architecture

The execution trace generation supports gathering of data which contain the behavior of the executed state chart. For each monitored state chart, an execution trace will be created during execution. These execution traces of different states of the state charts are merged for complete system visualization. The state chart notation applied in this work was adopted from the one used in (Vaiya, 2011). The state chart starts with the notation label Root directory which is the application user who on logging in is required to provide password/ token (Hard or Soft) as shown in figure 4.5.

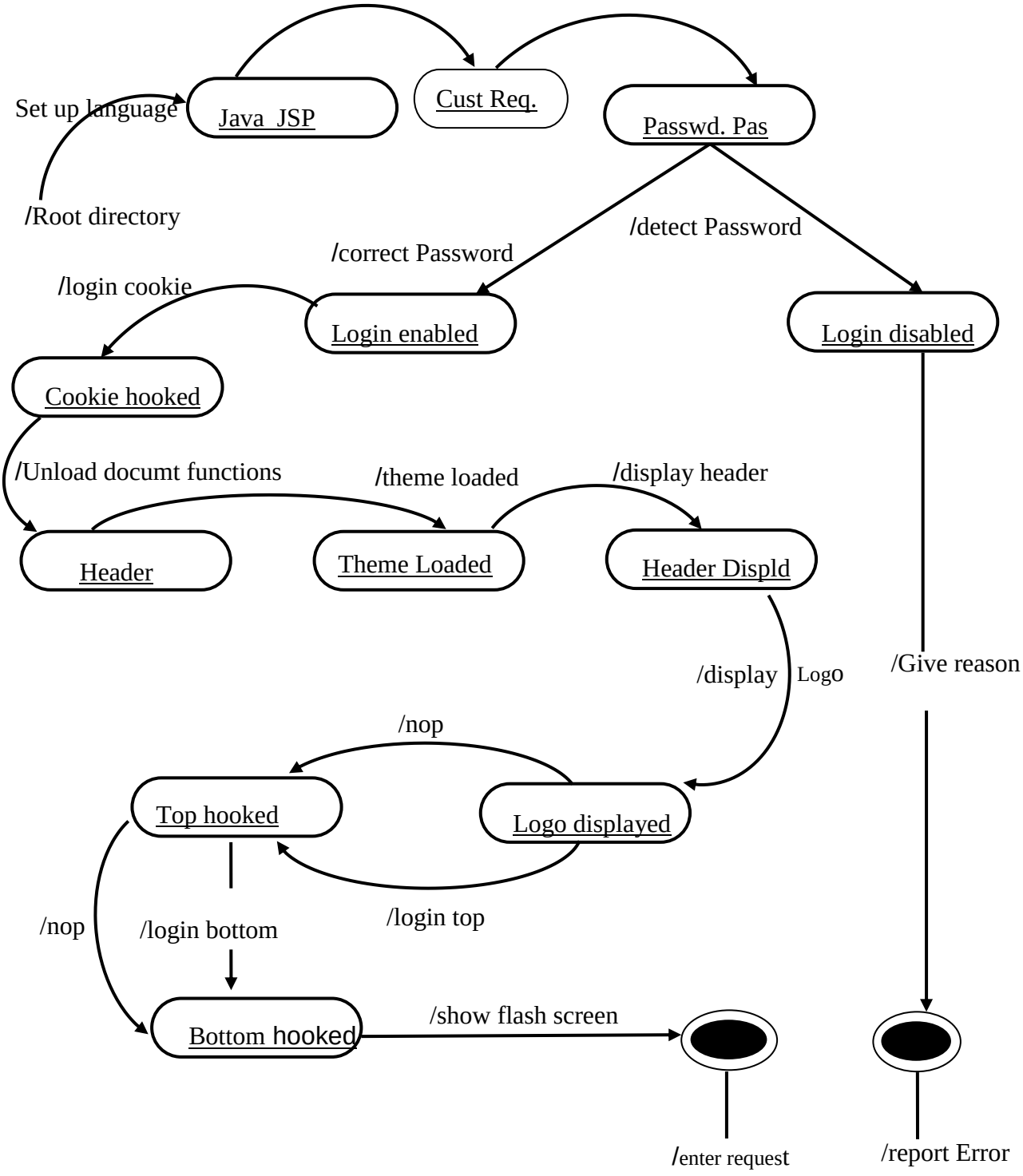


Figure 4.5: Login and display of flash screen state chart

An event can be added to the left of the slash in the transition label to specify the triggering condition for transition to new state.

4.4 OBJECTIVES OF THE DESIGN

The model was designed to:

1. Facilitate interoperability of transaction for its users in the Nigerian banks in different locations.
2. Ensure that the information viewed by the users remain private and can't be modified by third parties.
3. Ensure scalability and reliability to handle exponential growth, and adapt itself with future technologies.
4. Provide effective detective and preventive mechanism for legitimate users by alerting the users of the model of unauthorized access to their accounts via email and sms.
5. Allow customers and banks to authenticate each other, and sign processed transactions online.
6. Create database history for each user by keeping details of user's transaction for audit trail.

4.5 COMPONENTS OF THE DESIGN

The components of the system consist of the following:

Inputs

Input requirement is determined largely by the outputs expected. Consideration therefore was given to:

a) Design of input layouts
b) Types of input media available
c) Volume of input documents
d) Data collection methods

Processing

These are the steps that join the whole design that links everything together to produce the desired output. This will involve the user's computer network and that of the banks' network. This starts with the users need to do transaction in his/her account and ends on the desired output. The proposed model adopts the mechanisms of DKG & GK and ZTMA to provide comprehensive, secure and sophisticated authentication that effectively confirm user identity and protect payment transactions details. The application program used Java sever page (JSP) language which is made up of multiple threads of execution to simultaneously execute instructions and give expected outputs. The processing mode contains the program code and its current activity.

Outputs

Output is the outcome of the transactions both by authorized and unauthorized.

Files: This element is closely linked to input and output. Input is processed against the files to produce the necessary output. Considerations necessary for the design of the files include:

1. Storage media
2. File security
3. Method of file organizations and access
4. Record layouts

4.6 Systems Specifications

4.6.1 Input Specifications

The inputs to this system include:

Customer: Customer Name, Customer's Street, Customer's City

Branch: Branch Name, Branch City, Assets.

Account: Account Number, Account Balance. All are connected by links.

Other inputs are the use of the mouse to point, drag and move over to achieve desired effects, keys on the keyboard. While input is the items fed into the system, output is the outcome of the system manipulations of the inputs.

The design process can be described as a set of iterations of trying out alternative clients. Based on the requirements, the design will set up a set of initial clients and carry out the simulation. After obtaining the simulation results, the data will be analyzed to check for possible attack and subsequent countermeasures.. This kind of model-simulate-analysis procedure will be iterated many times until the analysis results from modeling and simulation match the requirements or the "best" result are found (Wasson, 2006).

Tables 4.1 and 4.2 specified the input and output specifications for the system.

Input Specifications:

Table 4.1

Field Name	Width	Data type
Customer Name	40	Text
Customer street	25	Text
Customer City	15	Text
Branch Name	15	Text

Branch City	15	Text
Branch Assets	15	Numeric
Account No	25	Numeric
Account Bal	Auto	Currency
Type of Transaction	30	Text

4.6.2 Output Specifications:

Table 4.2

Field Name	**Width**	**Data Type**
Customer Name	40	Text
Customer street	25	Text
Customer City	15	Text
Branch Name	15	Text
Branch City	15	Text
Branch Assets	15	Numeric
Account No	25	Numeric
Account Bal	Auto	Currency
Type of Transaction	30	Text
Customer Profession	20	Text
Nature of business	25	Text
Mobile phone No	15	Numeric
e-mail	25	Text
Sex	8	Numeric
Date of birth	Auto	Date/Time
Closing Balance	Auto	Currency
No of log in attempts	3	Numeric
Transaction	20	Text

History		
Marital Status	15	Text

4.6.3 Input Formats

Input Form

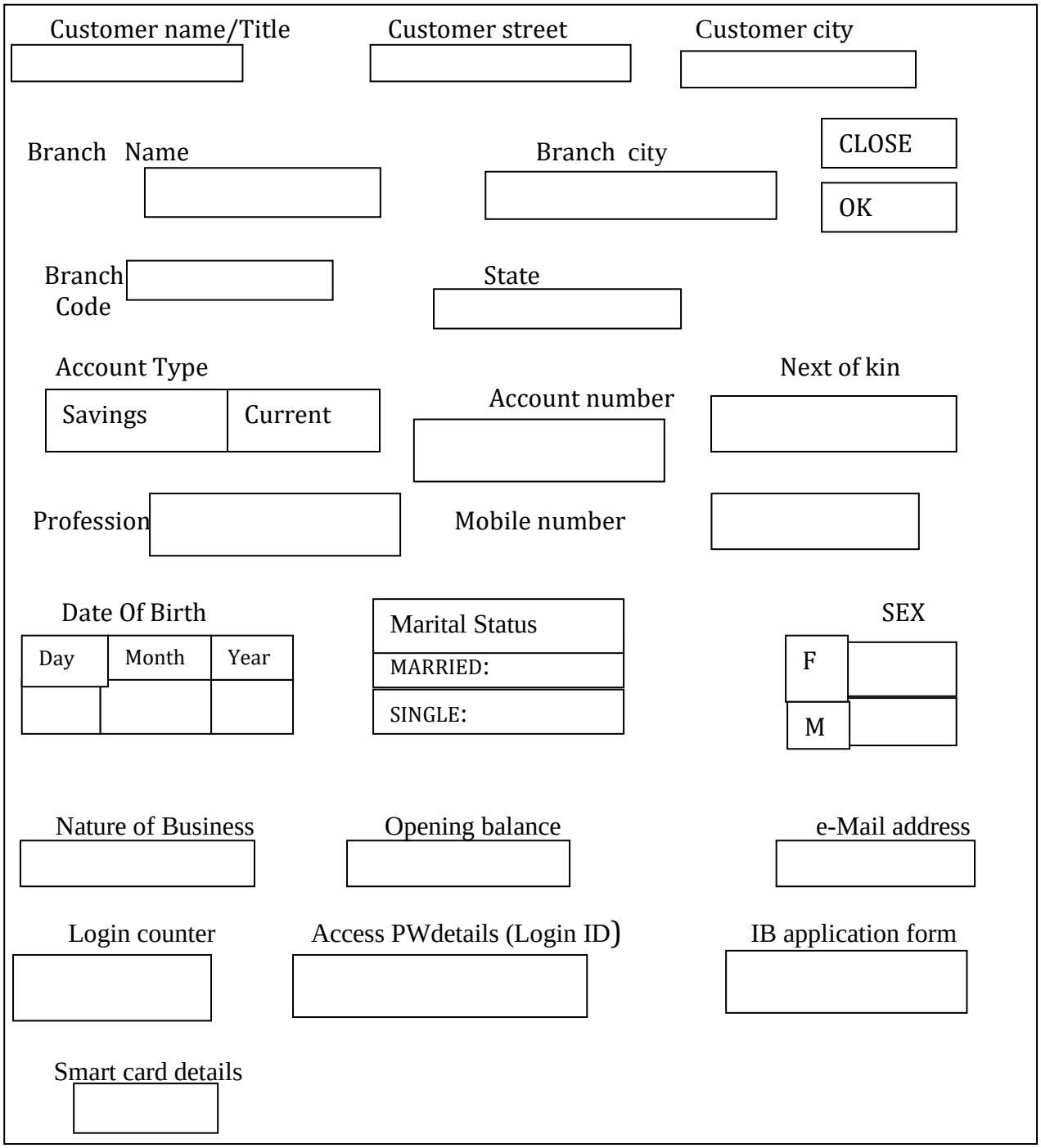


Figure 4.6a: Sample Input Form

4.6.4 Output Form

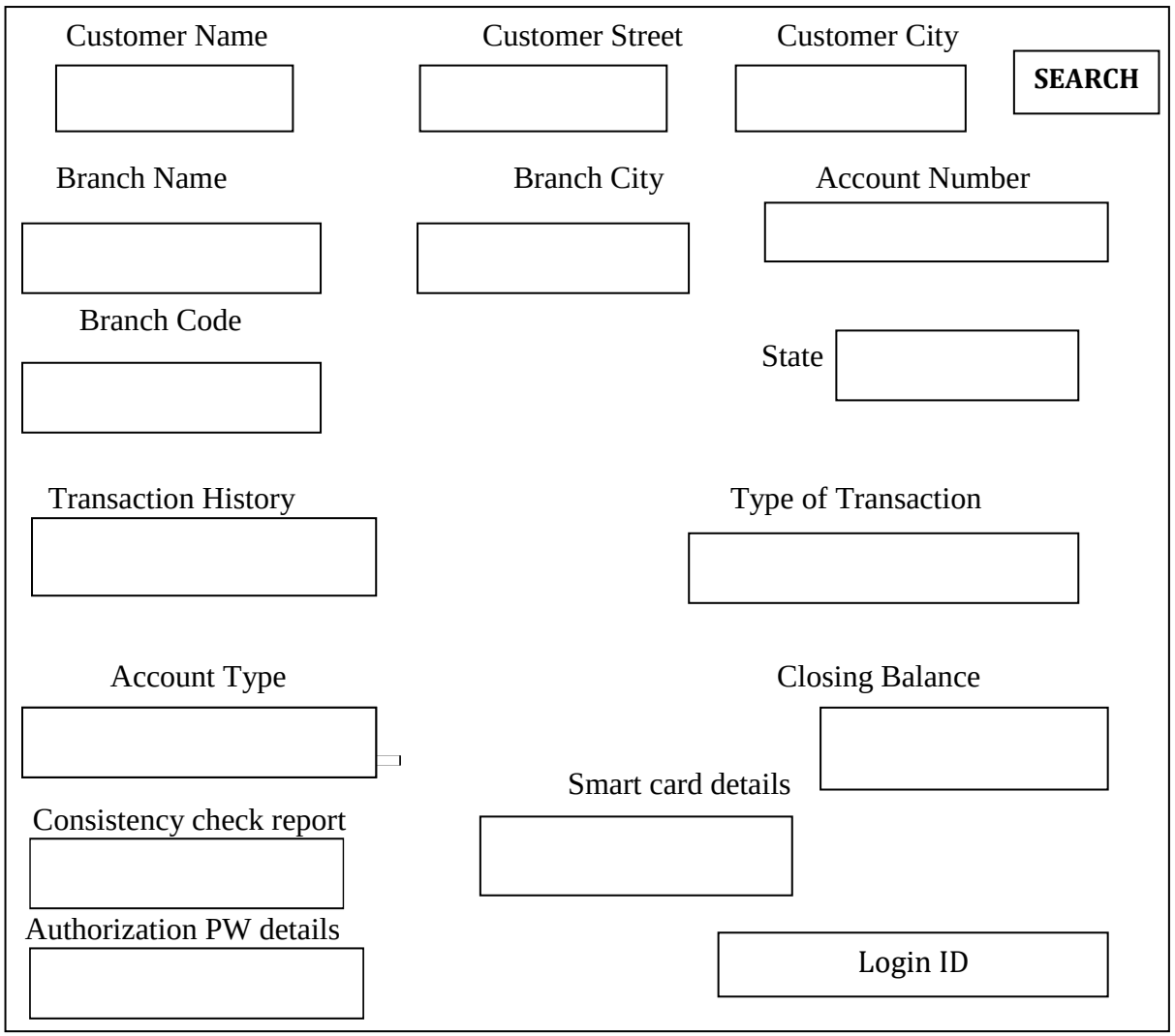


Figure 4.6b: Sample Output Form

4.7 DATABASE DESIGN

A network database is considered the most ideal for this work. It consists of a collection of records connected to one another through links. A record is in many respects similar to an entity in the E-R model. Each record is a collection of fields (attributes), each of which contains only one data value. A link is an association between precisely two records. Thus, a link can be viewed as a restricted (binary) form of relationship in the sense of the E-R model. In the relational model, the data and the relationships among data are represented by a collection of tables. The network model differs from the relational model in that data are represented by collections of *records*, and relationships among data are represented by *links*.

As an illustration, consider the inputs of customer/account in the database (fig 4.6) representing a *customer-account* relationship in a banking system.

There are two record types, *customer* and *account*. Customer record type is represented thus:

Type *customer* = **record**

customer-name: string;

customer-street: string;

customer-city: string;

End

The *account* record type can be defined as:

Type *account* = **record**

account-number: string;

balance: integer;

End

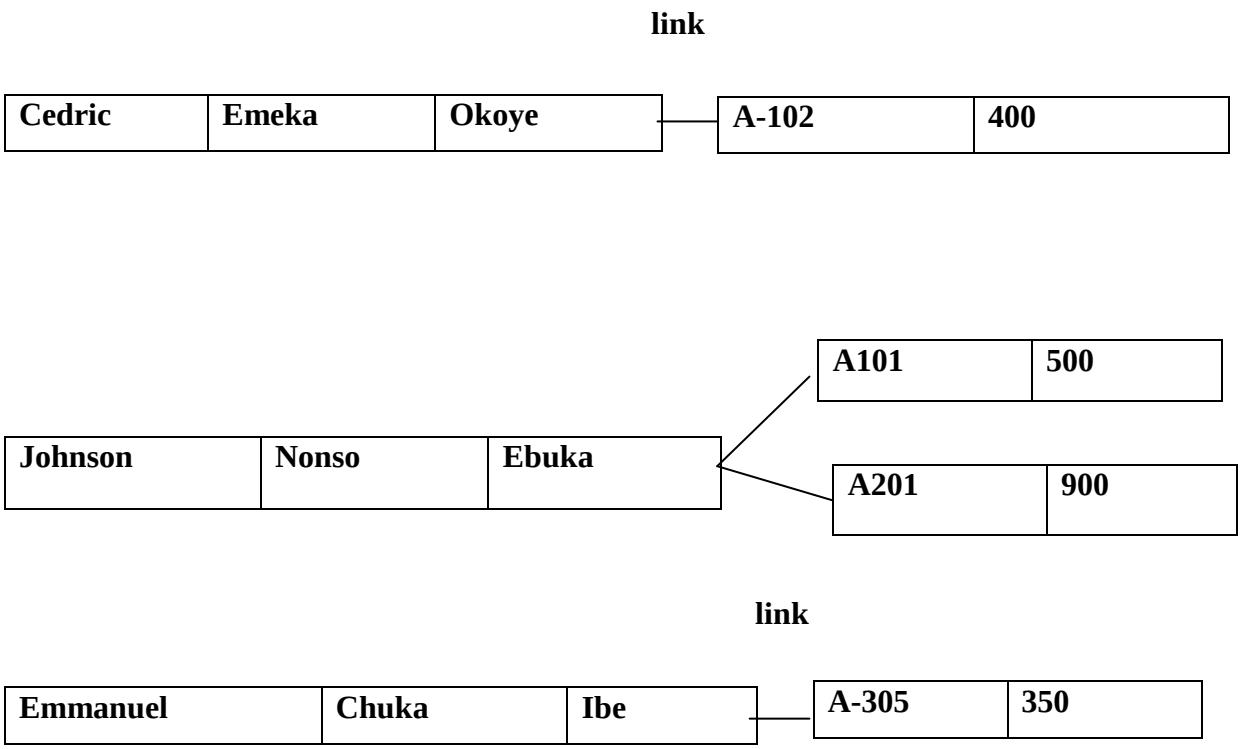


Figure 4.7a Network model example

The schema, subschema, and data management language are a few of the key components that make this database model unique. The schema used for this model is conceptual organization of the entire database.

4.7.1 Database Structure

The database structure is Network Database which can be defined as:

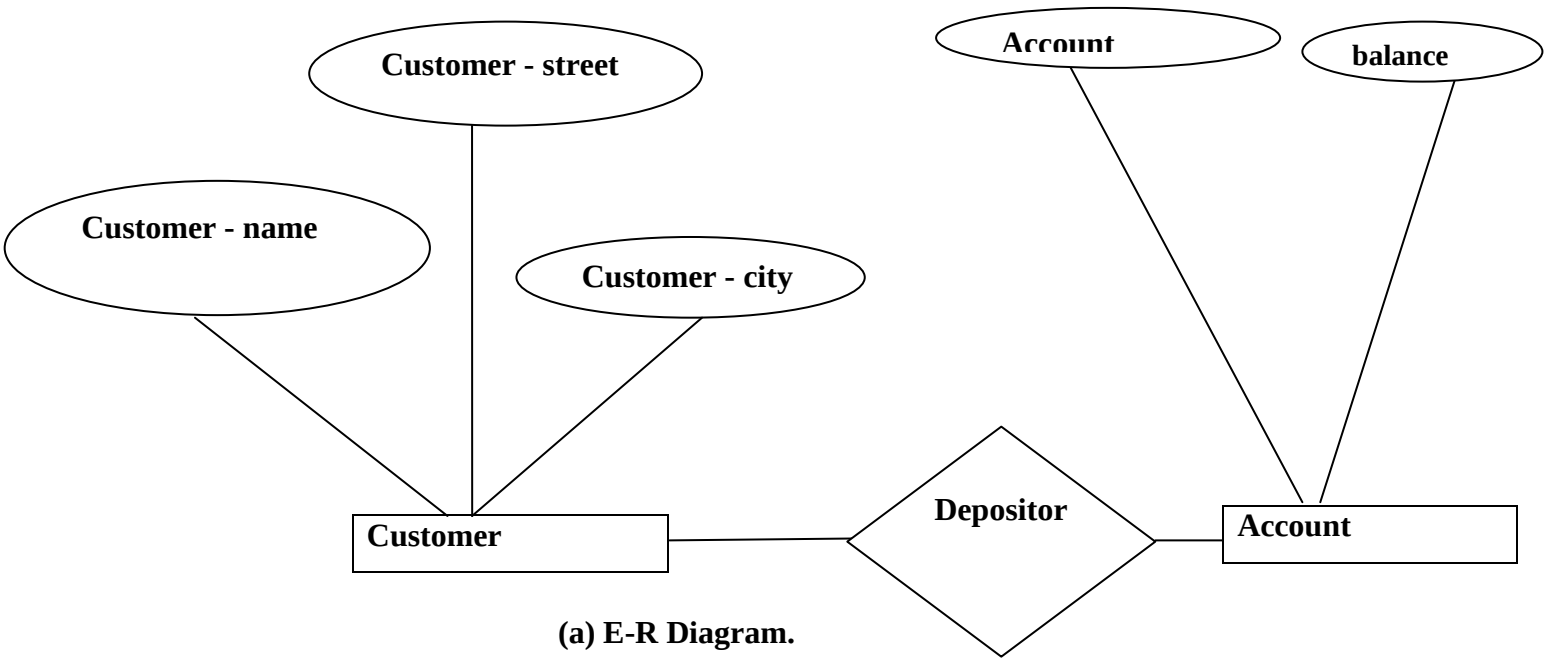
(1) A database that runs in a network. The DBMS was designed with client/server architecture.

(2)A database that holds addresses of other users in the network.

(3) A database organization method that allows for data relationships in a net-like form. A single data element can point to multiple data elements and can itself be pointed to by other data elements in contrast with relational database and hierarchical database. The advantages of Network Database Model include:

a) Representing a complex data relationship more effectively.
b) Improving database performance.
c) And imposing a database standard.

Network database model also provides Conceptual simplicity, data access flexibility, conformance to standards, handles more relationship types, promote database integrity, and allows for data independence. A representation of Database model using E-R diagram is as shown below in figure 4.7b.



(a) E-R Diagram.

E-R Diagram

Figure 4.7b: Data Structure Diagram – Network Model

A database corresponding to the described schema may thus contain a number of *customer* records linked to a number of *account* records. Since the relationship is many to many, we show that Johnson has accounts A-101 and A- 201 and that account A-201 is owned by both Johnson and Cedric (fig 4.6). Since the relationship is one to many from *customer* to *account*, a customer may have more than one account, as Johnson does—he owns both A-101 and A-201.

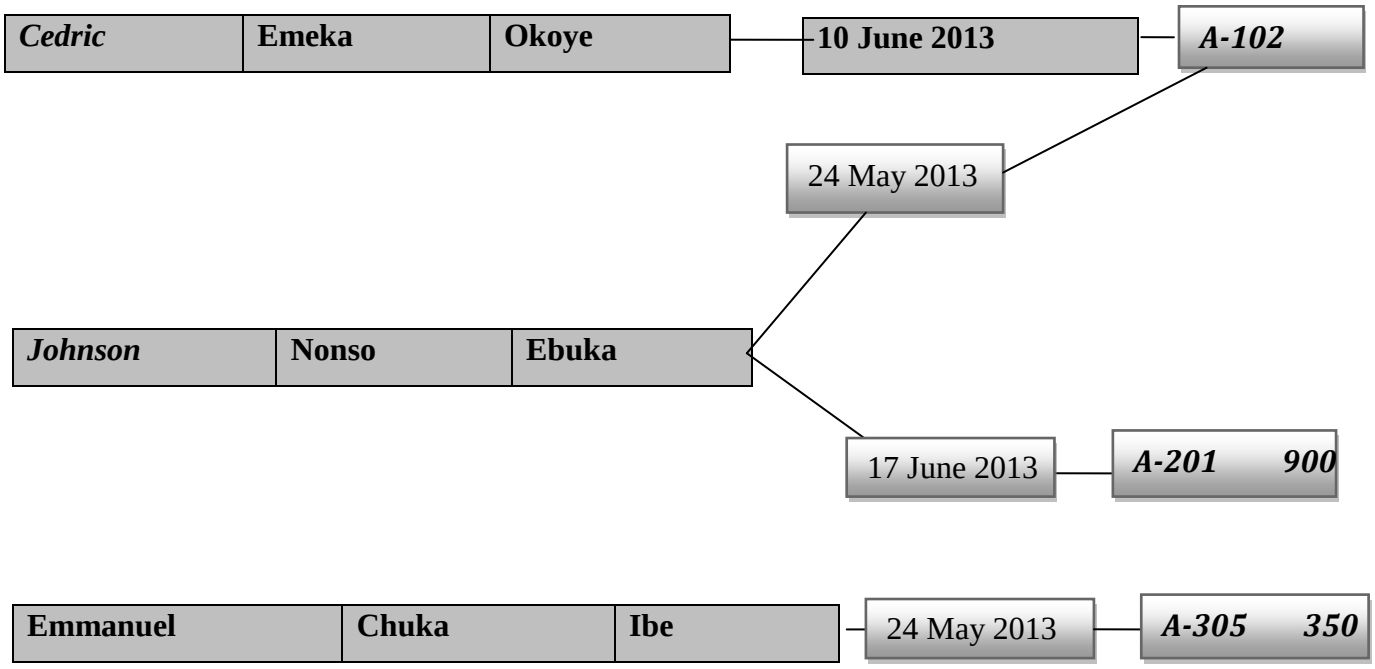


Figure 4.7c: Data Structure diagram linking Customer and account details

Figure 4.7c shows that:

a. Account A-201 is held by Johnson alone, and was last accessed by him on 17 June.

b. Account A-305 is held by Emmanuel alone, and was last accessed by him on 28 May.

c. Account A-102 is held by both Cedric and Johnson. Cedric accessed it last on 10 June, and Johnson accessed it last on 24 May.

4.7.2 List of Database Tables

Below is the list of tables used in this system (Table 4.3):

Table 4.3: Database Table

S/ N	**Field Name**	**Access Table Name**
1	**Customer Name**	**CustN**
2	**Customer street**	**CustS**
3	**Customer City**	**CustC**
4	Branch Name	BrchN
5	Branch City	BrchC
6	Branch Assets	BrchA
7	Branch Code	Brchcode
8	Account Balance	AccBal
9	Account No	AccNo
10	Transaction Type	Transtype
11	User Profile	Userprofile
12	Login Details	Logindetails
13	Biometric Details	Biodetails
14	Access Date	Accessdate
15	Unique Identifier	Rlink
16	Customer Link	CustRlink
17	Branch Link	BrchRlink
18	Account Link	AcctRlink
19	Behaviour detail	Behavdetails

4.7.3 The User Interface

The user interface of the application is the part of the software the user sees and works with. It consists of the screens that are viewed, typed and clicked on. An interface can be intuitive. This implies that its organization makes it easier for the user to move around the software and perform any desired task. The interface used in the system is built as a web of a number of task windows, it is less clustered, and thus made it easier to find what the user needs when carrying out financial transaction.

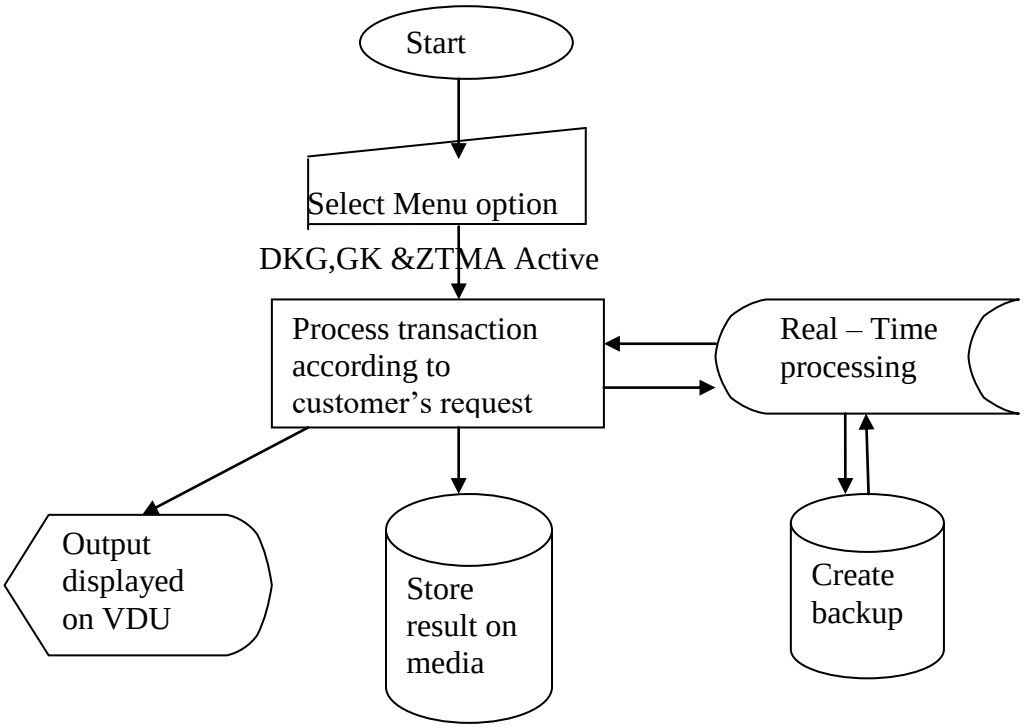


Figure 4.8 Block diagram of user Interface

Once the user starts the application, it validates the user, shows the welcome screen after which it shows the system activity modules: Internet Banking Registration, User Login, Transaction, Hacking Simulation, Report, About us, Help, Exit. Any activity chosen is processed according to customer's request on real time basis. Real-Time processing is backed up to provide both online and offline visualization. Results of processed information are either stored in a media or displayed on a Visual Display Unit (VDU). Clicking Exit activity by the user stops the software immediately.

4.8 Process and Procedure

These are the steps that join the whole design that links everything together to produce the desired output. This will involve the user's computer network and that of the banks' network. This starts with the users need to do transaction in his/her account and ends on the desired output. The proposed model adopts the mechanisms of DKG & GK and ZTMA to provide comprehensive, secure and sophisticated authentication that effectively confirm user identity and protect payment transactions details. Customer supplies the necessary biometric details during account opening stage, and then completes an application form for internet banking. The bank registers the request with Bank Sever [BS] and creates a Smart card for the customer. Customer on activation of the Smart card, changes the initial password with the

bank server [BS]. Since this occurs personally with the user, it is assumed that the shared secrets of personal details will never be disclosed.

These processes and procedures are focused on fraudulent transactions prevention, detection and alert to the user for necessary counter measures.

4.8.1 Security Analysis of Dynamic Key Generation (DKG) - Fraud Prevention

Dynamic Key Generation (DKG) uses dynamic generation of smart card security number to enhance Fraud prevention. The main concept is to apply one hash algorithm with cyclic shifting of a secret security number each time a transaction is attempted.

This technique never reprocesses security number during a transaction. The fraudulent user will find it to succeed to collect the security number sent to the actual users' mobile phone number or email. This security number is expected to be used within 60 seconds of generating it. When the number of incorrect trials exceeds a predetermined limit (the set limit between Client and Bank Server (BS), BS will bounce back the Client out of the system or set alert for the particular member in the group.

To reactivate the service, Client has to start all over again, which means the fraudulent user has to start the process of collecting the required security number again and obtaining unique password from the beginning to generate the numbers.

4.8.2 Security Analysis of Group Key GK) - Fraud Detection

The conceptual architecture also employs a Group Key (GK) mechanism which maximizes efficiency and security for individuals and group users. The major role of the GK mechanism is to restrict access to a different object in the system by the user, and to assure only authorized users can have access to sensitive client information. In addition, it protects clients by maintaining different access levels to their sensitive information and secures the transmitting information through open networks.

4.8 .3 Security of the ZTMA, DKG and GK techniques against possible attacks

It can be seen that the generated set of Keys do not require a long-term shared key. Thus even if the generated key is compromised, it will not be used after 60 seconds. In the proposed technique, generating each security number is based on more than just the unique password. Thus, the compromise of the unique password or shared secret in transactions will not compromise the security of the system.

If the attempts exceed the specified limit, Customer's account is blocked. The system then notifies Customer that there were unauthorized attempts on their account and asks for Customer's update. After Customer has updated, the fraudulent user has to repeat the attacking processes from the beginning.

The only possible successful attack to the proposed technique is that the fraudulent user must be able to do the following:

1. Access each party's device to retrieve the entire set of security number anytime it is generated and use within 60 seconds.
2. Record all transmitted security numbers in all transactions, and
3. Detect the request to update the set of security number.

Being able to successfully do these are difficult because generating each set of keys is based on dynamic parameters that are randomly chosen by the server. Alert for update of Keys of given transaction is sent via SMS to Client mobile phone/e-mail. As a result, regardless of the number of transactions performed, there is less chance that the system will be compromised.

4.9 Systems Flowchart

The application system is as shown in figure 4.8. The user starts the application, then selects activity required from the main menu. As Transaction menu is selected, the operation is performed as shown in figure 4.9.

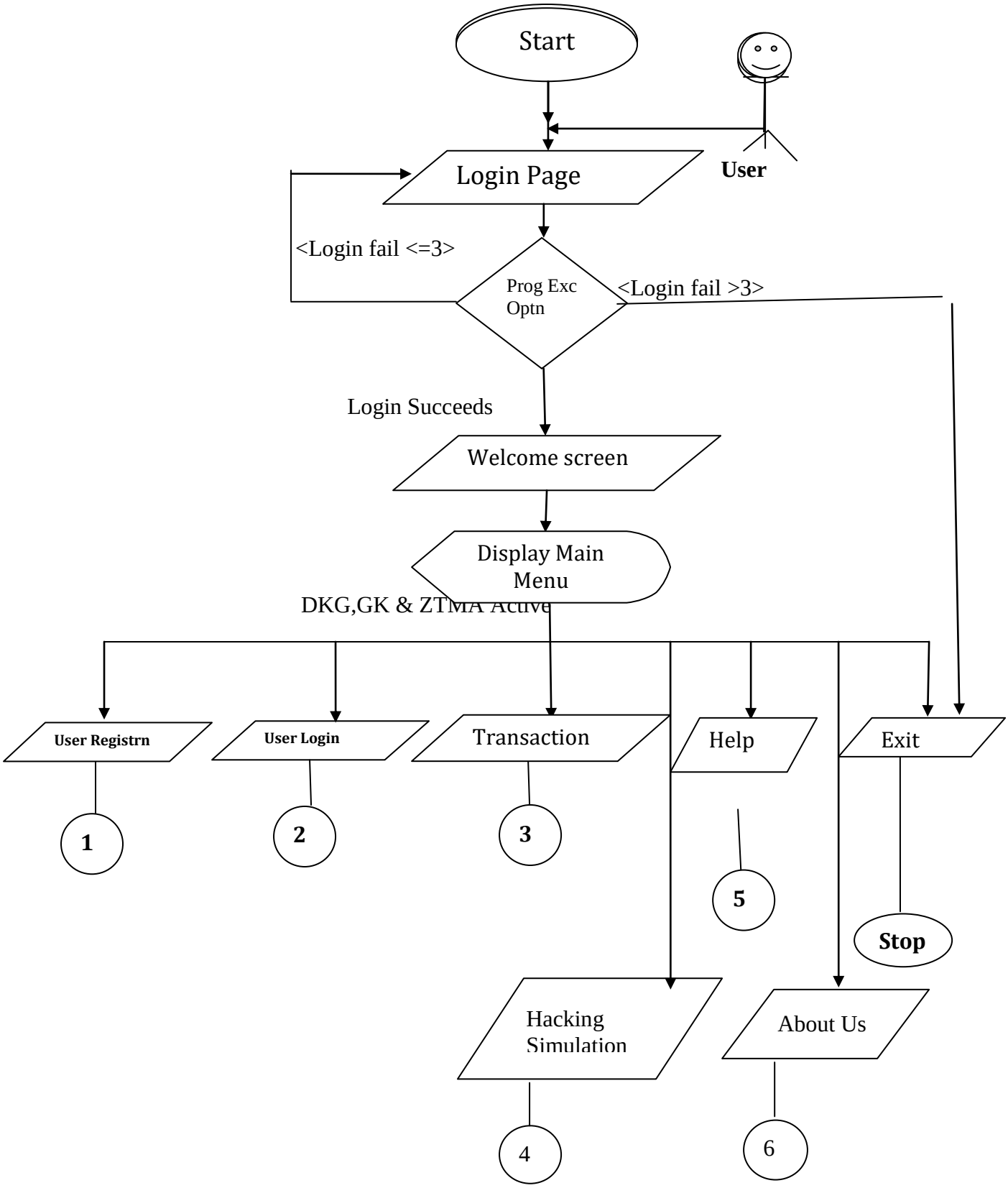


Figure 4.9a Main Menu Flow Chart

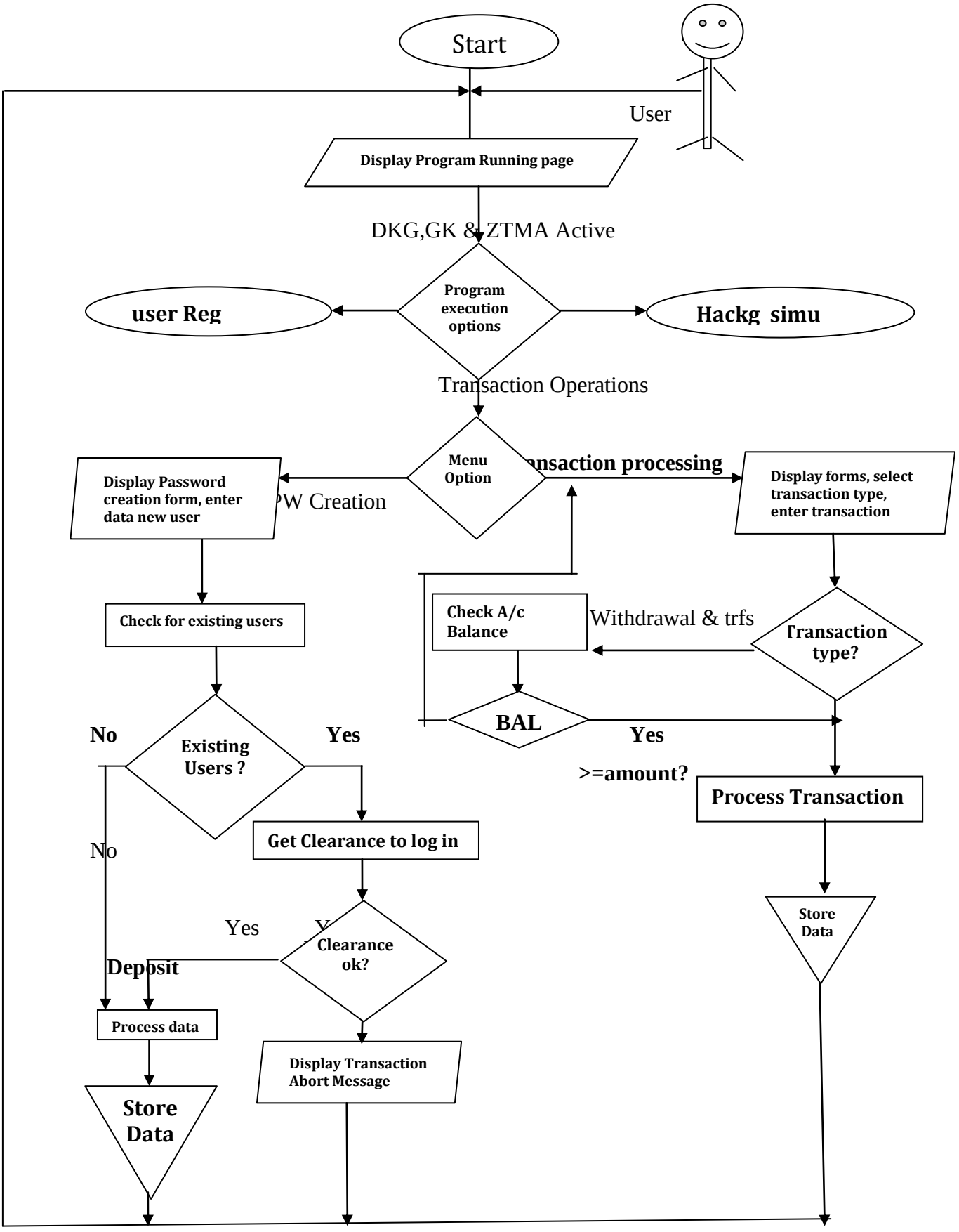


Figure 4.9b: The Transactional Operation Sub-Menu Flow Chart

CHAPTER FIVE

SYSTEM IMPLEMENTATION AND DOCUMENTATION

5.1 Introduction

A comprehensive internet banking security model policy should be proactive. To achieve this, the enhanced design divided 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.

Prevention measures used vulnerability assessment tools and penetration analyses to proactively detect known vulnerabilities such as security flaws and bugs in the model. Vulnerability assessment tools are expected to detect holes that may have allowed unauthorized access to the network, or insiders misuse of the system. Penetration analysis used snap check to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Vulnerability assessment tools and penetration analysis assisted in determining the model enhancement over existing models.

5.2.0 System Requirements

5.2.1 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

5.2.2 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 Explore 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 Band above that will require 1GHz Intel Pentium 4 processor or equivalent

Required Third Party Software:

1. Internet Browser (internet Explorer 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.

5.3 Program Development

5.3.1 Choice of Programming Language

Java server pages (JSP) from a suite of Java programming language was chosen for the development of the application. Java Server Pages is a software technology that helps to create dynamically generated Web pages based on HTML (Hyper Text Markup Language), XML (Extensible Markup Language) and other documents types (Wikipedia). Java is good for cross platform support.

JSP is richer than Active Server pages (ASP) as it allows insertion of externally defined pieces into static Web pages (You can have a set of tools for building the external piece and still have more options regarding the stage of the HTTP response at which the piece actually got inserted). Hence JSP makes it more convenient for the inclusion of a dynamic data thereby providing easier mix of regular, static HTML.

One of the main design considerations for the Java platform is to provide a secure environment for executing mobile code. To maintain integrity of the code, domain specific language (DSL) that supports value-chained business processes will be defined by using Web services. To do this, few abstractions will have to be made to produce efficient, effective distributed applications. DSL can also be called a Web Service Interaction modeling language, or a Web Service Interaction Language. Actual artifacts expressed in this language (Figure 4.7) are known as Web Service Interaction models (Keith, 2003).

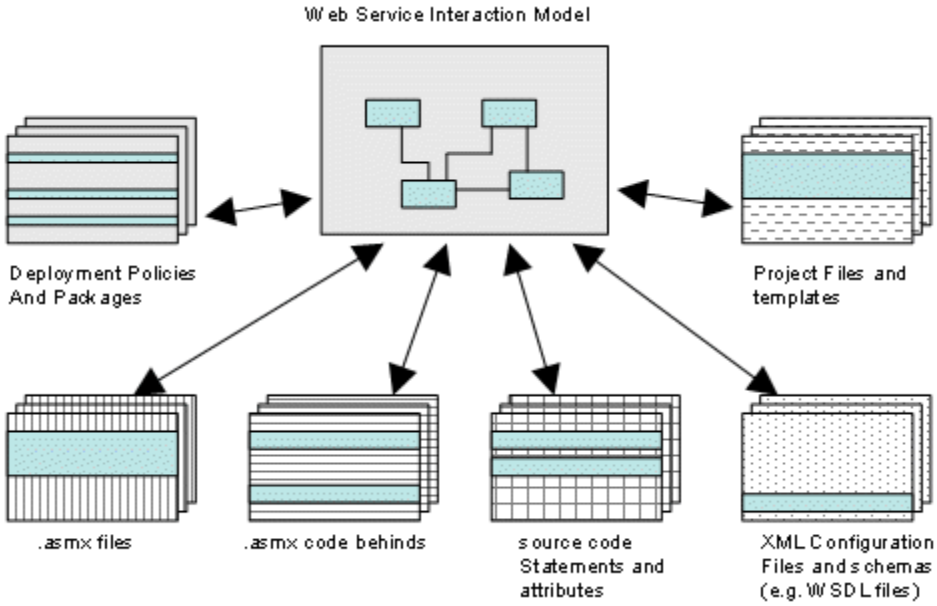


Figure 5.1 Multiple artifacts and fragments of Web service Interaction model (Derived from a model adopted from Keith Short, Architect, Visual Studio Enterprise Tools Microsoft Corporation, October 2003

DSLs work well when they are designed for subsets of a larger set of requirements (such as personalization), subsets of a larger architecture (such as security) or subsets of a larger development process (such as Web service interconnection). A DSL offers abstractions specific to some domain, and adds value by helping to solve problems in that domain in a highly efficient manner.

5.3.2 Language Justification

The development of the application with the Server Side technology called Java Server Pages (JSP) was chosen over other Java suite of programming languages for the following reasons:

1. Operability - It is more powerful and better for complex applications that require reusable components. It is portable to other operating systems and Web servers hence enhancing interoperability among the server products.

2. Extensive APIs (Application Program Interface) are available for networking, Database access, Distributed objects with the use of JSP.

3. It is more convenient to write and to modify regular HTML – you can put different people to different tasks.

4. JSP does not require strong knowledge of Java as writing program with JSP is nothing but making use of tags

5. JSP provides optional mechanism in configuring web application file.

6. JSP environment provides implicit/global exception handling mechanism.

7. The programming environment provides page compilation automatically.

8. The programming with JSP provides an additional concept called custom tags development.

9. JSP is highly preferred due to the fact that it is easy to learn and implement by the programmer through the use of simple tags. It is flexible, and support component-centric programming and cross platform implementation.

10. JSP doesn't provide any capabilities that couldn't in principle be accomplished with a servelet. JSP documents are automatically translated into servelets behind the scene.

11. JSP programming environment provides parallel development of Web applications.

12. JSP environment provides separation between presentation logic and business logic

5.4 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 5.2 shows the dynamics of Java Server Pages (JSP) model architecture.

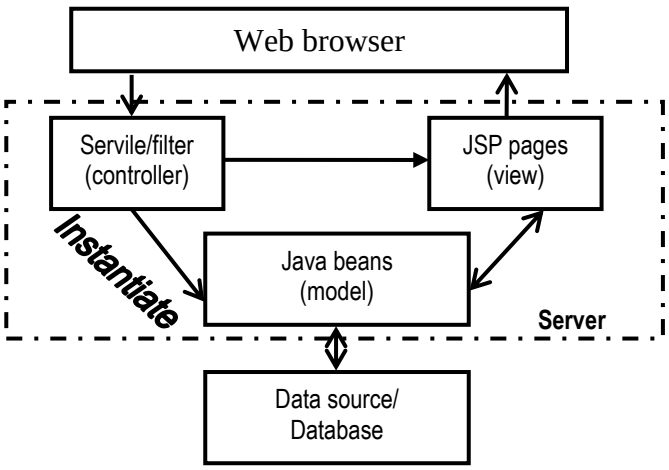


Figure 5.2: Diagram of JSP model architecture (adopted from Libertyenie, 2013)

The following steps below will guide the user of the application program:

1. Copy the Folder HEIBM in a Drive C or hard drive
2. Activate the Web link
3. Load the Open Database Connectivity (ODBC) Application – using the control panel, double click on the Administrator's Tool. Click Add button and select Microsoft Access Driver (MDB). Click Finish button.
4. Load the Application by browsing application folder and double click the HEIBM to welcome user to the main menu of the application.

The Administrator

The user is required to login in order to use the application. User gains access to the application by double clicking on HEIBM data file in the folder and insert your Password. Correct Password gives the user access to the application. On successful display of the Web page, the user can then choose the internet banking operation desired.

5.5 Program Work Area

Open Database Connectivity (ODBC) is a software API (Application programming Language) for accessing Database management systems (DBMS). It operates independent of the programming language or operational systems and offers to different database systems. ODBC has a core and a specific ODBC database drivers. The core also known as drive manager is independent of the database and acts as an interpreter between the application and the database drivers. The database drivers, on the other hand, contain DBMS specific details and offer a mechanism for connecting with different ODBS-enabled database systems.

Each program is called a *run unit*. The program statements access and manipulate database items, as well as any locally declared variables. For each such application program, the system maintains a *program work area* (referred to in the model as a *user work area*), which is a buffer storage area that contains the following variables:

1. **Record templates:** A record for each record type accessed by the application program
2. **Currency pointers:** A set of pointers to various database records most recently accessed by the application program; currency pointers are of the following types:

a. **Current of record type:** One currency pointer for each record type *T* referenced by the application program; each pointer contains the *address* (location on disk) of the most recently accessed record of type *T*

b. **Current of set type:** One currency pointer for each set type *S* referenced by the application program; each pointer contains the *address* of the most recently accessed record of that set

type; note that this pointer may point to a record of either the owner or member type, depending on whether an owner or a member was most recently accessed

c. **Current of run unit:** One single currency pointer, containing the *address* of the record (regardless of type) most recently accessed by the application program

d. **Status flags:** A set of variables used by the system to communicate to the application program the outcome of the last operation applied to the database.

For our customer-account-branch database example, a particular program work area contains the following:

Templates: Three record types:

_ *Customer* record

_ *Account* record

_ *Branch* record

5.5.1 The Find and Get Commands

The two most frequently used commands are

a. **find**, which locates a record in the database.

b. **get**, which copies the record to which the current of run-unit points from the database to the appropriate program work area template as illustrated in figure 5.3 below.

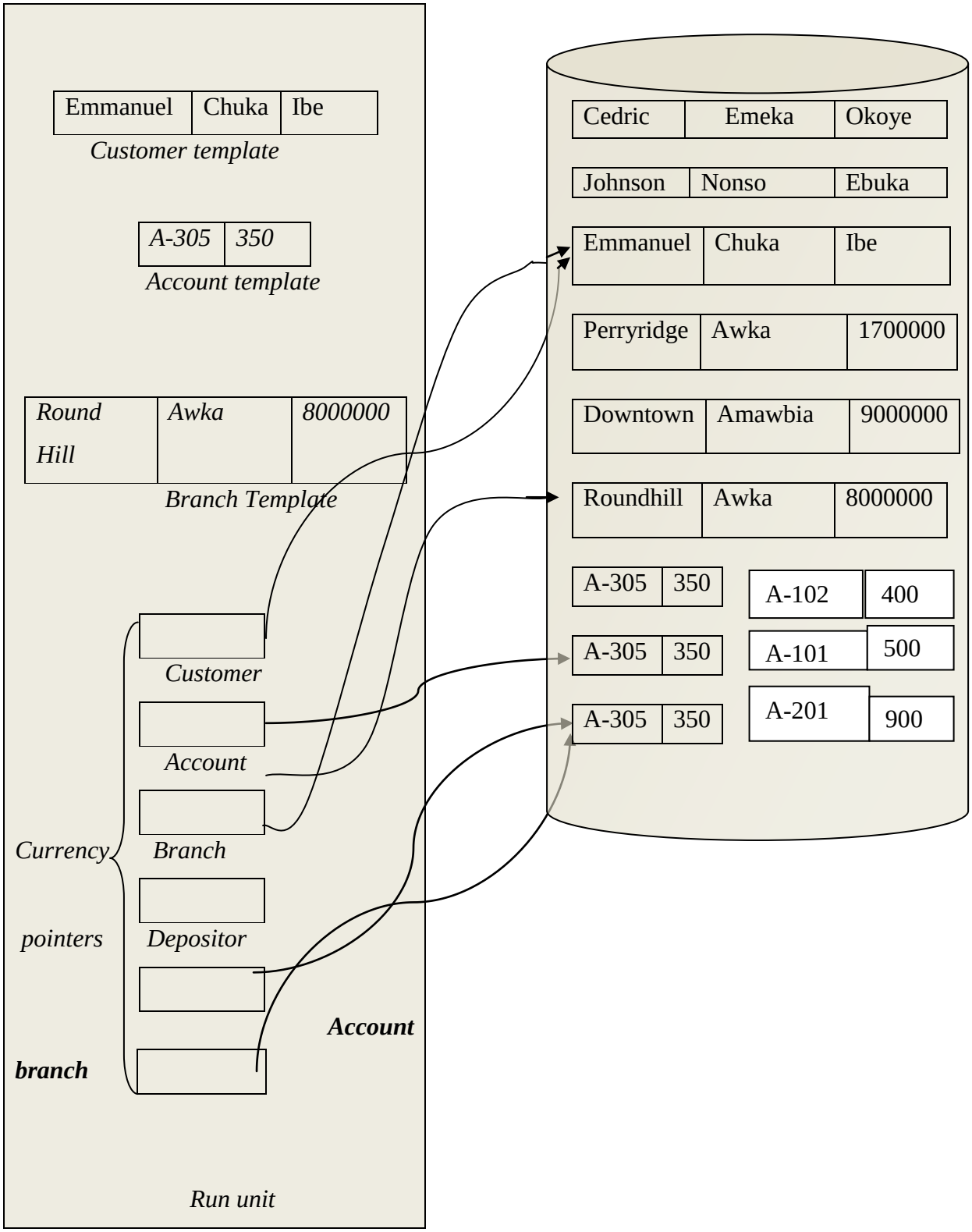


Figure 5.3: Program work Area

5.5.2 Access of Individual Records

The **find** commands locates individual records in the database. The simplest command has the form

find any <record type> **using** <record-field>

This command locates a record of type <record type> whose <record-field> value is the same as the value of <record-field> in the <record type> template in the program work area.

5.5.3 Mapping of Networks to Files

A network database consists of records and links. Links are implemented by adding *pointer fields* to records that are associated via a link. Each record has one pointer field for each link with which it is associated.

An *account* record is associated with only one *customer* record. Thus, we need only one pointer in the *account* record to represent the *depositor* relationship.

5.6 System Maintenance

Organizations, especially the banking sector are researching new ways to improve network security, as they are faced with adversaries who are continually changing their tactics and increasing the level of sophistication of their attacks. Security is a process, not something you can buy in a shrink-wrapped box. 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. Well-designed security models are flexible enough to address most "probable" threats.

An essential part of security maintenance policy development is risk assessment process. That is why, it is important to regularly go through a risk assessment process to determine what you want to protect, why you want to protect it, and from what you need to protect it. The steps associated with risk assessment in the life of the system model include the following:

1. Identifying and prioritizing assets;
2. Identifying vulnerabilities;
3. Identifying threats and their probabilities;
4. Identifying countermeasures;
5. Developing a cost-benefit analysis;

6. Developing security policies.

Maintenance therefore will involve continuous vulnerability and penetration assessment for removal of faults after the model has been completed, tested and implemented. It requires the continual enhancement of the model with emergent future technologies to close mark and forestall the activities of the ever busy unauthorized users and protect authorized users of internet banking system.

CHAPTER SIX

SYSTEM TESTING AND EVALUATION

6.1 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 Internet banking authentication mechanism focused on three different areas: prevention, detection and incident response alert. The user uses password-based authentication, smart card generators, software-based certificates, and biometric details to access the system based on the bank security policy for the end user. Figure 6.1 below shows the testing process for the model framework.

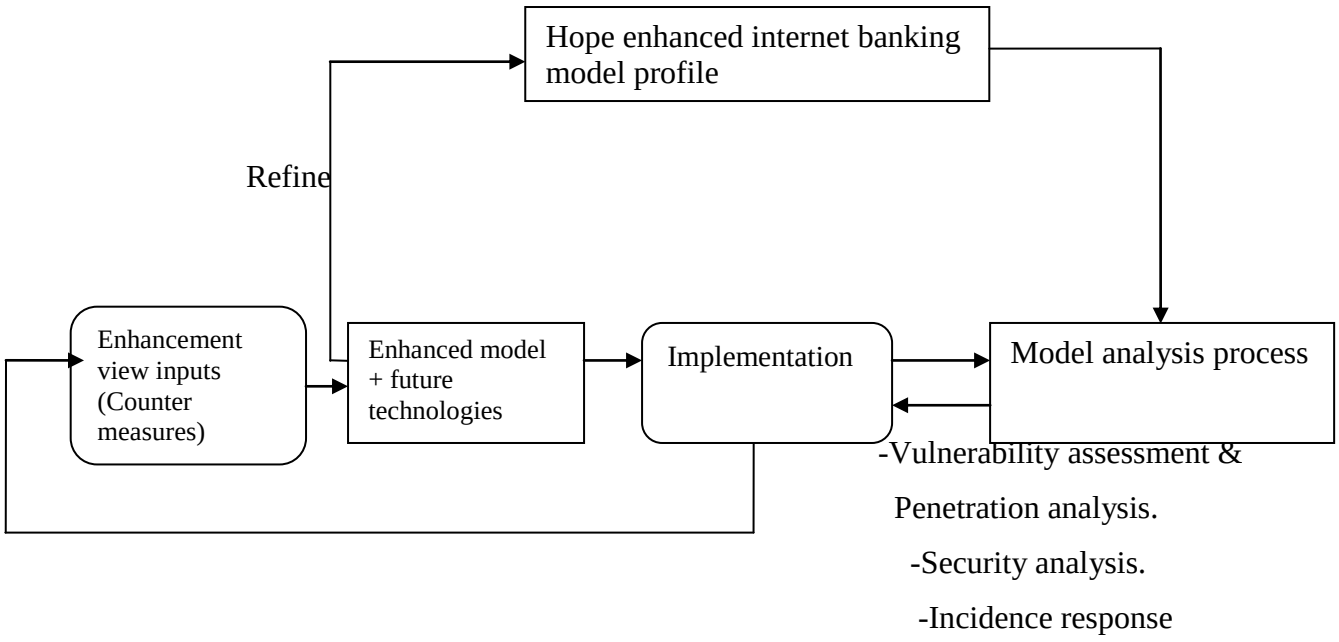


Figure 6.1: System Framework testing

Security analysis for the model was done using the simulation hacking demo menu of HEIBM to check for vulnerability/penetration avenues as shown in the Report menu of the model in appendix iv. From the analysis, appropriate countermeasures were created to provide a blueprint of combined countermeasures to enhance the system's security level during implementation.

As security is a moving target, the enhanced model can further be improved with future technologies to match the ever changing hackers' activities.

6.2 Test Data

Users use browser software such as Mozilla fire fox or Microsoft internet Explorer (MIT) to interface to the HEIBM. The Model server provides HTML forms-based interface through which customers can make requests and conduct transaction.

Hope enhanced Internet Banking Model (HEIBM) when simulated with an attacker using authentication mechanisms of DKG, GK and ZTMA were found to deliver a better security than existing Models. The reported vulnerabilities, possible attacks on the accounts and countermeasures will be used by the bank's management for decision making and further implementation.

6.3 Incident Response

Based on the overall risk assessment and vulnerability observed in vulnerability and penetration analysis, the counter measures were applied and implemented to enhance the systems operation. The software detected attacks in real-time, and automatically responds so that customer is notified on a real-time basis during an attack, rather than detect the attack afterward during a manual log review. Methods of notification include e-mail, audio alarm, or message displays on a computer monitor. Responses include automatic logging out of the websites, logging in additional information, and disabling a user's account (e.g., by disallowing a particular user account or Internet address) for a period sufficient for information systems personnel to review the attack information or verify the user for appropriate counter measure.

6.4 Countermeasures

Countermeasures are used to improve and reduce risk of further attack to the system. To implement enhanced security, authentication mechanisms and countermeasures were combined to complement each other's resistance to attacks. Figure 6.2 shows possible attacks on different vulnerability areas and possible countermeasures to be applied. A combination of different authentication methods, supported by countermeasures produced a more enhanced system.

Attack	Countermeasure
UT/U1a: User Surveillance UT/U1b: Theft of token and handwritten notes	Security policy regarding token and password handling, clear desk policy and screen surveillance.
UT/U2a: Hidden Code	Code installation blockers Antispyware software Antiphishing software (URL inspection) Firewall for blocking inbound and outbound connections to unauthorized ports intrusion/anomaly detection Browser security best practices (cookies, window pop-ups, java support, etc.)
UT/U2b: Worms and bots	Code installation blockers Firewall for blocking inbound and outbound connections to unauthorized ports intrusion/anomaly detection Browser security best practices Antispyware software Custom application secure coding
UT/U2c: E-mail with malicious code	E-mail blocking and sending it to spam Code installation blockers Attachment blocking HTML code blocking Antispam software Antispyware software Antiphishing software (URL inspection) Firewall for blocking inbound and outbound connections to unauthorized ports intrusion/anomaly detection
UT/U3a:Smartcard analyzers	Power-and time-neutral code design
UT/U3b: Smart reader manipulator	Secure smartcard interface design and implementation
UT/U3c: Brute-force attacks with PIN calculators	Increased number of digits-at least an eight-dight code
UT/U4a:Social engineering	Security awareness Simple easy-to-remember URLs Antiphishing software (URL inspection)
UT/U4b:Webpage obfuscation	Use of a predetermined list of valid URLs Prohibiting the use of IP addresses instead of URLs DNS monitoring
CC1: Pharming	DNS security countermeasures: prevention detection, reaction countermeasures (e.g depending on the implementation, appropriate

	firewall, intrusion and prevention) DNS SEC best practices.
CC2: Sniffing	Mutual authentication and encryption through client-server framework Use of predetermined certificates
CC3: Active man-in-the-middle attacks	Mutual authentication and encryption through client-server framework Use of predetermined certificates
CC4: Session hijacking	Management of sessions to protect session ID specification in the message, session ID change.
IBS1:Brute-force attacks	Prevention, detection and reaction countermeasures (firewall, intrusion detection and prevention) detect and block attacks.
IBS2: Bank security policy violation	Security policy implementation according to banks' security policy
IBS3:Website manipulation	Standard prevention, detection and reaction countermeasures (e.g., depending on the implementation, appropriate firewall, intrusion and prevention.

Figure 6.2: Additional countermeasure supporting authentication mechanisms

6.5 Vulnerability assessment Analysis of the model

To ensure that the enhanced model achieved the desired result, a continual vulnerability assessment was performed to identify the system's vulnerability to possible attacks.

This was done considering the following attacks areas and types of attack:

1. The User terminal/user (UT/U)
2. The Communication channel (CC)
3. The Internet banking server (IBS).

UT/U1a: User surveillance (piggybacking), UT/U1b: Theft of token and handwritten notes

E-mails and Sms was used to clearly inform the user of important awareness rules, including rules on using strong passwords and be informed on the importance of token physical security.

UT/U2a: Hidden code, UT/U2b: Worms and bots/UT/U2c: Emails with malicious code—To address this issue within the framework of the assessment, a set of e-mail policies were created for guiding the users in protecting their personal computers. This involved the creation of an e-mail policy for secure attachment handling.

UT/U3a: Smartcard analyzers, UT/U3b: Smartcard reader manipulator—The characteristics provided by the smartcard and smartcard reader manufacturer were noted.

UT/U3c: Brute-force attacks with PIN generators—The PIN generators provided by the bank must have an eight-digit PIN.

UT/U4a: Social engineering - The user policy involved the following:

1. Do not write down passwords.
2. Do not enter passwords with other people watching.
3. Do not share passwords.

UT/U4b: Web-page obfuscation - To address this attack,

1. The users were advised to store the exact URL of the bank and use only this URL for accessing the Internet banking service.
2. The bank should monitor names similar to the bank's domain names in order to be alerted. This is because registration of similar domain names to the legitimate ones is a common method that phishers use to attract victims.

It is therefore important that domain name change is communicated to users and updates should always be conducted on time.

CC1: Pharming—The server's architecture has to be examined with configuration files to prevent DNS poisoning. Also digital signatures was used for message origin authentication and integrity, especially for data involving the DNS zones.

CC2: Sniffing, CC3: ZTMA addressed Active man-in-the-middle attacks.

CC4: Session hijacking—This is achieved using DKG and GK. The session IDs generated were unique, hence the possibility of receiving session IDs within URL was difficult.

IBS1: Brute-force attacks—The model was appropriately configured to discard information from sources that sending abnormal amounts of authentication requests.

IBS2: Bank security policy violation— Any deference from the bank security policy was rejected or thrown back.

IBS 3: Web site manipulation—Vulnerability assessments were done by the bank servers hosting the Internet banking web site.

The vulnerability areas and the type of attacks analyzed is shown in figure 6.3

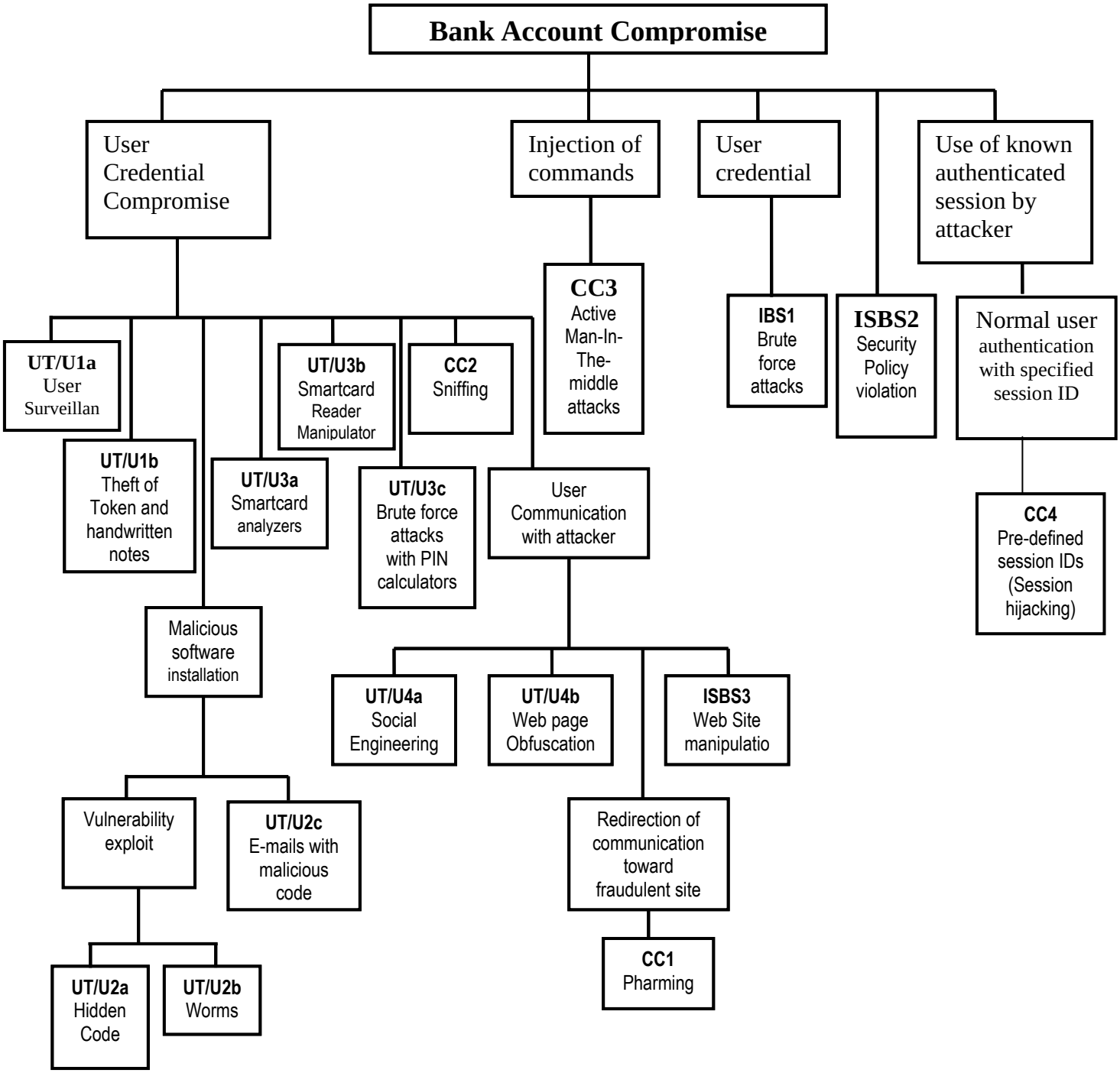


Figure 6.3 Vulnerability Areas and types of Attack.

The attack areas provide a way to ensure that the model make the bank to be proactive about security, capture and reuse expertise about security, and respond to changes in security.

The attack target has one root node, representing the final target of the attacker, which is to compromise the customer's bank account. An intruder may use one of the leaf nodes as a means for reaching the target- Customer Account.

6.6.1 Penetration Analysis of security of existing authentication mechanisms and that of Hope Enhanced Internet Banking model (HEIBM)

Penetration analysis is a snapshot of the security at a point in time to test the effectiveness of security controls and preparedness measures.

Different authentication mechanisms used by existing models were applied to the vulnerability areas and attack types to gain a snapshot view on the effectiveness of security controls at any point in time. The result of which should facilitate the possible countermeasures and its' adequacy.

The authentication mechanisms used are:

Static Password

This is based on proof by knowledge. Password-based mechanisms are most widely utilized in Internet banking applications. This mechanism was found to be prone to all types of attacks.

Soft-token Certificate

This mechanism conducts mutual authentication between the UT and IBS, and it is based on certificates stored in the user's browser. The mechanism was prone to attacks, that compromise the UT, where the user certificate is stored, thus may permit access to the user certificate, resulting in identity theft.

Hard-token Certificate

This mechanism was based on the "proof by possession" principle, since the user possesses an object as a token toward authentication. The use of hardware tokens addresses the vulnerabilities of storing the certificate in the user's browser.

One-time Password/Time-based

This mechanism may also fall in the category of proof by possession authentication mechanisms. One-time passwords are generated by a random calculator, using a seed that is pre-shared between the user's device (protected by a PIN) and the IBS. In mobile banking, the random codes may be submitted to the UT by the mobile operator through SMS, or generated by an application downloaded to the user's mobile device.

Challenge-response

This mechanism adds uniqueness to the authentication process. IBS generates a challenge that is processed by the UT/U for producing a response. Challenge-response is prone to man-in-the-middle and session hijacking attacks (CC), since an entity may intercept the communication between the UT/U and IBS, and capture and replay messages.

Biometrics

Biometrics provide stronger authentication by adding the "proof by property" principle, completing or substituting the existing "proof by knowledge" and "proof by possession" mechanisms.

Knowledge-based

This mechanism consists of a number of questions that the user has to answer to gain access to the account, example, what is the name of grand child?. This could be also considered as behavioral biometric authentication, depending on the content of the questions or, instead, a more sophisticated combined password mechanism.

Hope Enhanced Internet Banking model (HEIBM)

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 figure 6.5.

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**								

Fig 6.4: Applicability of Attacks in different Authentication Mechanisms

6.6.1 Comparison of security of existing model and HEIBM based on authentication mechanisms

The authentication methods used by the models were classified based on resistance to two types of common attacks: offline credential-stealing attacks, and online channel-breaking attacks.

Offline credential stealing attacks aim to fraudulently gather a user's credentials either by invading an insufficiently protected client PC via malicious software or by tricking a user into voluntarily revealing his or her credentials via phishing.

Online channel-breaking attacks, instead of trying to get the user's credentials, the intruder unnoticeably interrupts messages between the client PC and the banking server by masquerading as the server to the client and vice versa. Attack on a system can be local (Trojan Horse) or remote (Phishing, Pharming, DNS poisoning). Attacks are more dangerous when both offline and online attacks are combined.

Existing security models include:

Digital Certificates - This model depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity.

One Time Password Tokens

One Time Password Cards

Browser Protection

Virtual Keyboards

Device Registering

CAPCHA- Completely Automated Public Turing test to tell Computers and Humans

Short Message Service (sms)

Device Identification

Positive Identification

Pass – Phase

Transaction Monitoring

Figure 6.2 below showed the level of security achieved by different authentication mechanisms on existing models.

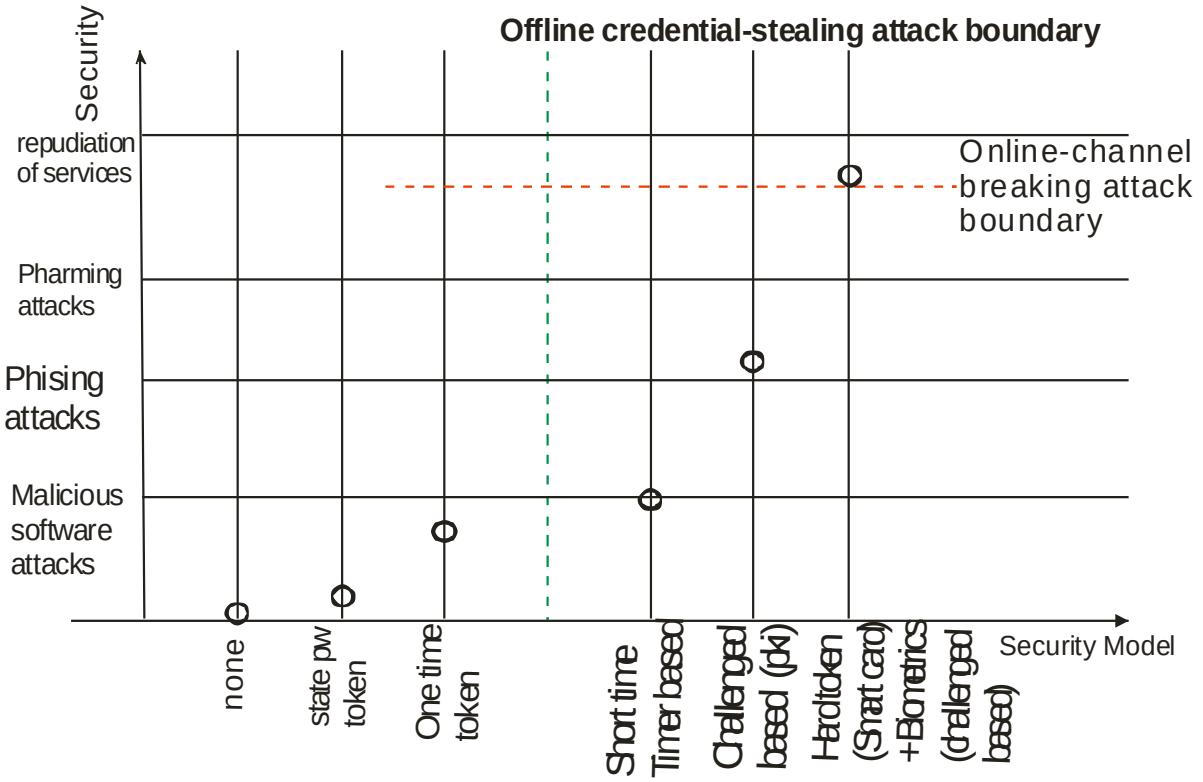


Figure 6.6: Security of existing model based on authentication mechanisms

The level of security on the graph above depends on whether it crosses the offline credential stealing attacks boundary (in horizontal direction) and/or online – channel breaking attacks boundary (vertical direction). Only hard token (smart card + biometrics) model crossed both attack boundaries. However, non-repudiation of transactions by the participating parties (bank and customers) was not achieved. In addition, the user's limited knowledge to determine the difference between fake and authentic servers, secure and non – secure servers, protected and non protected clients, could have been contributory.

6.6.2 Effectiveness of Hope Enhanced Internet Banking Security model (HEIBM) over existing models

Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and non-repudiation. Security level of a model among other things depends largely on authentication mechanism used to counter attacks. To ensure that only qualified people access Internet banking accounts, information viewed remained private and can't be modified by third parties, and that any transactions made are traceable and verifiable. HEIBM authentication techniques considered:

A. Bank/ Customer (Mutual) Authentication.

Customer identity and the target Web site is mutually authenticated to each other. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack.

B. Customer Verification Authentication.

Customer verification complements the authentication process and it is done during account origination. The verification is achieved in three ways:

1. **Positive verification** - This is done to ensure that material information provided by an applicant matches information available from trusted third party sources. The model verifies a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report).
2. **Logical verification** to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).
3. **Negative verification** to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior.

C. Customer/Account access Authentication

The Federal Financial Institution Examination Council (FFIEC) Information Technology Examination Handbook, Information Security Booklet, December 2002, states among others that financial institutions should periodically:

a) Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

b) Implement appropriate risk mitigation strategies.

To this end an enhanced authentication system is necessary for compliance with requirements to safeguard customer information and inhibit identity theft.

The authentication mechanisms of - Dynamic key generation (DKG), Group Key (GK), Zero Touch multi-factor authentication (ZTMA) combined customer mutual, verification and account access authentications to enhance and increase security of the model. The authentications used:

1) Shared Secrets - (*something a person knows)* This involves

1. Questions or queries that require specific customer knowledge to answer, e.g., what is middle name of your first child.

2. Customer-selected images that must be identified or selected from a pool of images.

These shared secrets occurred during the initial enrollment process or via an offline ancillary process. The security of shared secret is enhanced with periodic change.

2) Tokens - Tokens are physical devices (something the person has) namely:

a. USB Tokens with password that allows access on the hardware computer. This device can store digital certificates that can be used in public key infrastructure (PKI).
b. Smart Card – The card has a size of credit card with an embedded microprocessor that enables it to store and process data.
c. Password- Generating Token – it produces a unique pass-code known as a One Time Password (OTP) each time it is used. The OTP is designed to have a life span of 30 seconds.

3) Biometrics – It authenticates the identity of a living person once enrolled on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard.

4) Out of Box – This technique allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. Example, network-based server can generate a telephone call, an e-mail, or a text message for a higher risk transaction like fund transfer. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

5) Internet Protocol Address (IPA) – It identifies several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence" by the user.

6) Geo-Location Technology – This technique limit Internet users by determining where they are or, conversely, where they are not.

HEIBM considering these techniques in its authentication was able to cross both off line and on-line channel attacks without impacting on users' limited knowledge on the architecture of the security management system as shown in figure 6.3 below.

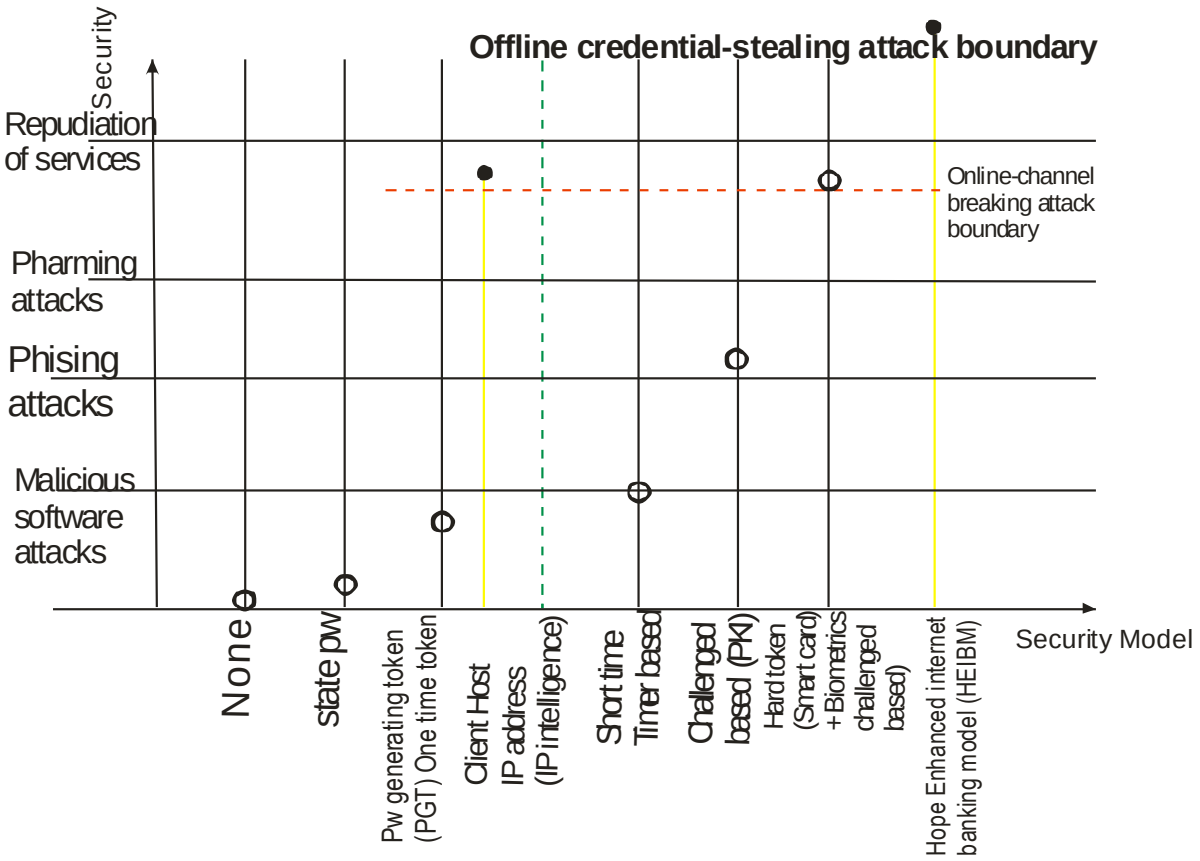


Figure 6.7: Effectiveness of security of HEIBM compared to that of existing models

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 evidence of 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.

6.7 Evaluation Criteria

Achieving the required Security and Trust in internet banking depend on the architecture of the security management system, but the bottom line is to gain users trust, the security

management must convince users that the system is secured and well protected. The criteria used in comparing security of existing model and HEIBM was authentication methods (figure 6.7) which manages access to the system. This is because an effective authentication method ensures customers' acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

The effectiveness of authentication was based on assessment of its ability to cross various attacking techniques used by attackers in the institution's Internet banking systems. The risk was evaluated in light of bill payment, fund transfer, payment/withdrawals, loan origination, the sensitivity of customer information being communicated to both the institution and the customer, the ease of using the communication method, and the volume of transactions, repudiation of services between customer and the bank internet system.

The model used Business Signatures solution to address the mutual authentication needs through use of shared secret, tokens, out of box methods, date and time of use.

The risk assessment process:

a. Identified all transactions and levels of access associated with Internet-based customer products and services;
b. Identified and assessed the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
c. Included the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

6.8 Performance Evaluation

The model performance as compared to that of existing ones was evaluated under the following areas:

A Broad Protection:

a. Fraud Risk Reduction: The model significantly reduced the likelihood of online fraud operations.
b. Fraud Coverage: The model works proactively as it protect, detects and provided alerts for necessary response on the common types of online fraud attacks on internet banking system

B Customer Experience Impact:

a. Impact Minimized: The model solution encouraged users by balancing frictionless access and the risks associated with specific user transactions.

b. User Perception: As the model provided enhanced online operation, users perception was improved and increased customers base and revenue.

Cost of Ownership:

a. Deployment: The software was considered easy to use as it fits seamlessly into the banks internet operation.
b. Operations: The model handling was user-friendly as it required effort to monitor and maintain. Customers' interactions with it does not require frequent calls to the help desk.
c. Availability: The model was considered robust and scalable as it did not decrease availability, thereby resulting in lost revenue.
d. Flexibility: The mode is adaptable to enhancement with future technologies thereby accounting to future types of fraud regulations.

CHAPTER SEVEN
SUMMARY AND CONCLUSION

7.1 Summary

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.

This work presented development of an enhanced network security model for internet banking. This is done by looking at the security of existing models through the several vulnerabilities and attacks that affect the models and subsequently proposed a model that will provide enhanced security of existing models. To this end:

The first chapter presented an introduction to the background of online banking in the banking system and the role internet has played to enhance electronic business activities within the business directions of the bank, and subsequently provide a platform that possesses the attribute of resolvability, interoperability, connectivity and compatibility with the bank's short and long term goals. Internet banking currently has three basic types namely: Informational, Communicative and Transactional. For clearer direction of the work, the objectives, significance, scope of the study were discussed. The terms used in the work were also defined in this chapter.

Chapter two reviewed related literature on network security, people perception of security of existing models in internet banking. Major types of online fraud and the challenges for mobile banking solution in internet banking were x-rayed. Security concern in using existing internet banking models was also discussed. Internet Banking Transactions requires 'secured network' for the users.

Doing business on the internet involves RISK, but banking business without use of internet entails greater RISK. This is because internet provides opportunities for business to increase customer base and lower transaction costs.

Risks and different types of internet banking risks were discussed. The mitigation of these risks brings about Trust, Confidence and Credibility in internet banking. Also analysis of Computer security background relating to field of: Software engineering, Computer security design, Information systems security and Human – Computer Interaction in security was x-rayed. The researcher concluded that a healthy security culture is created by taking into consideration human aspects that make it difficult for users to comply with security requirements and hence the need for an enhanced internet banking system.

The third chapter presented the analysis of existing internet banking models and its vulnerabilities and then went ahead to analyze how the proposed model will work in order to manage those vulnerabilities and enhance the system.

In order to enhance security of existing models, the researcher developed Hope Enhanced Internet Banking model (HEIBM) using the combined methodology of Neural networks and Fuzzy system model of web servers for effective decision making process.

The model combined three authentication mechanisms – dynamic key generation (DKG), group key (GK) and zero touch multi authentication (ZTMA) to indentify and authenticate its users.

Chapter four of the work discussed details of the system design by capturing the high level and broken down level view of the model concept.

Java server Pages technology of Java language and Domain Specific language was used to develop the program in order to support effectively value- chained businesses defined by using Web services. The justification for the hardware and software were discussed as well as testing and maintenance considerations.

Chapter five described the systems implementation and documentations.

An extensive testing and evaluation was done in chapter six. A continuous vulnerability assessment, penetration and security analysis were carried out in order to apply necessary countermeasures which support authentication mechanisms to provide an enhanced internet banking model.

Finally, chapter seven provided the summary of the entire work. Recommendations and suggestions for further studies were made.

7.2 Review of Achievements

The model was designed to make managing customers accounts online easier than ever before with enhanced security, new features and expanded functionality. It offers more convenient access to banking information whenever needed with its new responsive design that makes it convenient for use on computer and mobile devices. The model design offered:

1) Simplified Navigation

2) Optimization for mobile devices

3) New look and security for Login process.

Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and nonrepudiation. Confidentiality and integrity had been built-up by modeling a secured environment which provided high interoperability. The enhanced environment provided by the model crossed credential-stealing attacks as well as channel-breaking attacks, ensured that information viewed remained private and cannot be modified by third parties and ensured that only qualified people can access Internet banking accounts.

Nonrepudiation was achieved by the new model by producing and keeping copies of processed transaction thereby ensuring that any transactions made were traceable and verifiable.

Other achievements include:

1. Ensured interoperability of transactions from different locations and electronic devices.
2. More effectively addresses the online vulnerability in existing models to help reduce possible fraud exposure in the enhanced model.
3. Minimizes impact on user experience and provides flexibility for both the bank and end user to tailor authentication interaction.
4. Minimizes total Cost of Ownership with minimal infrastructure requirements, flexible and painless integration and low operational costs. Ensures scalability and high availability.
5. Allows increasing levels of authentication appropriate to the risk of the activity taking place.
6. A demonstration of how the new model provided better security than the existing models.
7. Application of a combination of Neural networks and Fuzzy system used to develop the model supported the web servers for effective dynamic decision making process.
8. As the enhanced model crossed the two attack boundaries of credential theft and channel breaking, perception of internet banking security and user's trust was positively affected.

9. User profile management was enhanced: Ability to reset Password, activate and deactivate user.
10. E-mail and SMS notifications alerts were provided for authorized users to confirm pending and successful transactions.

7.3 Areas of Application

Internet banking security is a moving target – as software and hardware development continue, and as new products emerge (with new bugs), hackers will seek possible vulnerabilities, and discover new and innovative ways of exploiting them. Internet security therefore is an arms race that the banks must be prepared to win. This race can be won by application of Hope Enhanced Internet Banking Security Model (HEIBM) with its enhanced authentications supported by countermeasures.

7.4 Major Contributions to Knowledge

1. The model developed was completely preventive to attacks instead of defensive by ensuring fraudulent payments detection and prevention as it combined different types of authentication mechanisms which are well adapted to changes in future technology.
2. It combined internal authentication, authorization and identification mechanisms of Dynamic Key Generation (DKG), Group Key (GK) and Zero Touch Multi- Factor Authentication (ZTMA) which is independent of user's experience for enhancement.
3. DKG prevents access by fraudulent users by confirming that involved parties can meet the secret keys generation requirements before they are allowed to perform transactions, GK mechanism which can identify users, manage them into groups and verify their authorization levels. Business Signatures of ZTMA offers a continuously refreshed library of e-Fraud and Rules that emanate from any fraudulent activity of users. This provides out-of-the-box protection (countermeasures) against possible fraudulent transactions.

7.5 Suggestions for Further Studies

Before now, there were existing models in internet banking that operated with different levels of vulnerabilities. The enhanced model considered this and integrated different authentication mechanisms to reduce these vulnerabilities and achieve enhanced security. The basic elements of network and system security addressed in this work are as listed:

i. Identification;
ii. Authentication;
iii. Access control (authorization);
iv. Availability;
v. Confidentiality (secrecy);
vi. Integrity (accuracy);
vii. Accountability.
viii. Addressed operations of physical characteristics recognition (PCR) and behavioral characteristics recognition (BCR) of the biometrics system).

The researcher suggests for future work, the development of more intelligent system that will address the problems of control, prediction, classification and data processing in such environments a system must be able to fully adapt its structure rather than adjust its parameters based on a pre-trained and fixed structure. That is, the system must be able to evolve, to self-develop, to self-organize with a higher level of flexibility and autonomy that can develop their understanding of the environment and ultimately their intelligence. That is the model will:

1. Improve on the physical characteristics recognition (PCR) and behavioral characteristics recognition (BCR) of the biometrics system and reduce False acceptance rate (FAR) and False rejection rate (FRR) to zero. Subsequently, handle the natural changes in people (example as people age, their physical characteristics can change).
2. Update authentication request registration template with the subtle changes in age that naturally occur every time it authenticates the would-be user.

7.6 Recommendations

1. Financial institutions offering Internet-based products and services should have reliable and secure system that will mutually authenticate themselves and their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services.

2. Financial institutions should conduct a regular risk assessment – vulnerability/penetration analysis to identify the types and levels of risk associated with their Internet banking applications and appropriate countermeasures adopted.
3. The level of risk associated with a given transaction should determine the level authentication required – Access control.
4. Bank management will appoint trusted IT personnel whose duty will be to continuously monitor their network by ensuring that their internet banking security checklist are regularly updated and any changes reported immediately for management decision. The checklists below should act as a guide

Internet Banking Security Checklist

1: Internet Banking Risks and Controls

Transaction risks

Security controls

Network and data access controls

User authentication

Firewalls

Encryption

Transaction verification

Virus protection

Monitoring

Security monitoring

Penetration testing

Intrusion detection

Performance monitoring

Audit/quality assurance

Contingency planning/business continuity

Internet expertise

Selection of internet banking providers

Internet banking functions available

2: Internet Banking and Physical Security Risks

Risk management and risk management controls

Security risks

Costs versus security breaches

Controlling client PCs

Desktop computer controls

Password management

Password management alternatives

Retrieving lost passwords

Watching the employees

Surveillance in and around the office

Controlling networks and servers

Managing network administration

EFT switches and network services

Electronic imaging systems

Operational and administrative security

Authentication security

Encryption security

Shutting down compromised systems

Manageable security enforcement

Sample secure applications e-mail security

Internet access security

Physical security

Security monitoring system overview

Major hazards

Riot and sabotage

Fraud or theft

Power failure

Equipment failure

Housekeeping rules

3: Identifying Customers In An Electronic Environment

Establishing the identity of an applicant

Identification documents

Information collection

Verifying identification information

Assisting customers who are victims of identity theft

What to tell to victims of identity theft

Using the Court affidavit

Authentication in electronic banking environment

Risk assessment

Account origination and customer verification

Transaction initiation and authentication of established customers

Monitoring and reporting

Authentication methods: passwords and PINs

Digital certificates using public key infrastructures (PKI)

Tokens

Biometrics

Smart card authentication technology changes

4: Electronic Commerce

The computer network

Security of internal networks

Security of public networks

5: Internet Banking Auditing

Website and internet banking features

Website development and hosting

Internet banking package

Cash management package

Bill pay

Security Options

Internet banking policy

Goals and objectives

Vendor management

Maintaining the institution's image

Insurance coverage

User access devices

File update responsibilities

Account reconciliation

Bill payment services

Bill pay controls

Bill pay processing

Bill pay customer support

Disaster recovery

Employee access

Internet banking services request/fulfillment

Internet banking registration form

User logs and error reports

Privacy external links

Dial-in access (if applicable)

Geographic boundaries

7.7 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. Network security comprise of three legs (security trinity) - prevention, detection, and response (figure 7.1). The security trinity – Prevention, Detection and Response are the foundation of proactive security policies for any organization.

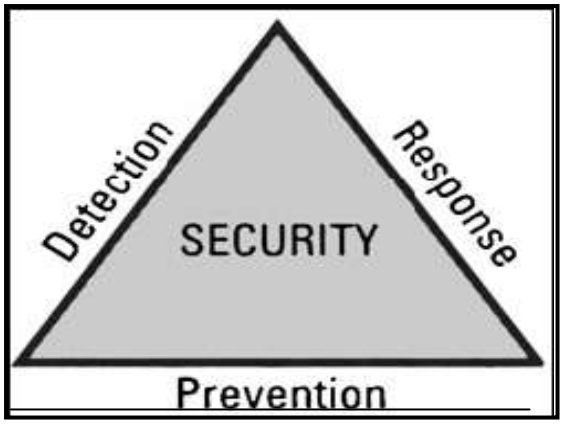


Figure 7.1: The security trinity (Adopted from Canavan, 2000).

Prevention

The foundation of the security trinity is prevention. To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities. In developing network security schemes, organizations should emphasize preventative measures over detection and response: It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one.

However, it is impossible to devise a security scheme that will prevent all vulnerabilities from being exploited, but banks should ensure that their preventative measures are strong enough to discourage potential criminals and force them go to easier target.

Detection

Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event where preventative measures fail. The sooner a problem is detected, the easier it is to correct and cleanup.

Response

There is need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.

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 increased. 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.

Alain Hiltgen, Zurich Thorsten Kramp, and Thomas Weigold (2006), "Secure Internet Banking Authentication", IEEE.

Ali Sanayei and Ali Noroozi (2009), "Security of Internet Banking Services and its linkage with Users' Trust", IEEE.

Antonio San Martino and Xavier Perramon (2008), "Defending EBanking Services; an antiphishing Approach", IEEE.

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

Banking Models", (IEEE 2007) http://www.arx.com/documents/Bank-of-Israel-Case-Study.pdf. 13 August 2009

Baskerkville, (1993). "Information systems security design methods: implications for information systems development". ACM Computing Surveys 25(4): 375-414.

BankNet Electronic Banking Service. Http://mkn.co.uk/bank

Basic Flaws in Internet Security and Commerce.

Basic Reflections On Security. Http://www.esd.de/eng/secu/secu.htm#10

Bener Ayse (2000), Trust and Perception of Internet Banking in India

Bellovin S.M. (1989). *Security Problems in the TCP/IP Protocol Suite*. Computer Communication Review, Vol. 19, No. 2, pp. 32-48.

Benbesat, L., D. Goldstein, et al. (1987), "The Case Research Strategy in Studies of Information System". MIS Quarterly **11**(3): 369-386.

Benesat, L. and R. Zmud (1999). "Empirical Research in Information System: The Practice of Relevance. "MIS Quarterly **23**(1): 2-18.

Bhaskar, K. (1993), "Computer Security–Threats and Countermeasures", NCC Blackwell Ltd.

Bhattacherjee, A. (2002), "Individual trust in online firms: Scale development and initial test". *Journal of Management Information Systems, 19*(1), 211-241.

Boland, R.E., Fitzgerald H.G and Wood-Haper A.T, (1985), "Phenomenology: a preferred approach to research on information systems. Research Methods in Information Systems". Amsterdam, North-Holland.

Brehmer B, Singleton W.T. and Hovden J. (1987), "The Psychology of Risk and Decisions"., John Wiley & Sons Ltd: pp 25-39.

Busines Day Newspaper, August 1st, 2013

Canavan John E. (2000), "Fundamentals of network security". Artech House telecommunications library. pp. 6-7.

Candid Wueest (2006), "Threats to Online Banking, Symantec Security Response", Dublin,

Carneiro B. and Sousa R. T (2010), "Identifying Bank Frauds Using Crisp-DM And Decision Trees", International Journal of Computer Science & Information Technology October, vol. 2, pp. 162-169.

Cavusoglu Hasan and Huseyin (2004), "Emerging Issues in Responsible Vulnerability Disclosure". Workshop on Information Technology and Systems (WITS 2004). Barcelona, Spain.

Checkland P.H, Nissen, H.K and Hirschheim R. (1991), "From Framework through experience to learning: the essential nature of Action Research, Contemporary Approaches and Emergent Traditions", North-Holland.

Chen L., Gillenson M.L. and Sherrell D.L (2002), "Enticing online consumers: An extended technology acceptance perspective". Information & Management journal, vol 39, 705-719.

Courtney R. (1977), "Security risk analysis in electronic data processing". AFIPS Conference Proceedings NC, AFIPS Press.

Covello V and Winterfeldt D. (1986), "Risk Communication: A review of the literature Risk Abstracts" **3**(4): 171-182.

Covello V and Sandman P (1988), "Risk Communication, risk statistics and risk comparison: A manual for plant managers", Chemical Manufacturers Association.

Cranor and Garfinkel (2005), "Security and Usability: Designing Secure Systems that People Can Use", pp 9-10

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

Dandash.O, Dung Le P. and Srinivasan B. (2007), "Internet banking payment protocol with fraud prevention", 22nd International International Symposium on Computer and Information Sciences, November, pp. 1-6.

Dandash O.; Dung Le P. and Srinvasan B. (2007), "Security Analysis for Internet Banking Models". Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, p. 1141 - 1146.

Davis G.B, Nickles K.R (1992), “Diagnosis of an Information Systems Failure: A Framework and Interpretive Process.” Information and Management journal 23: 293-318.

D’Hertfelt Roy (2000), Modelling and Evolutionary Optimization on Multilevel Scheduling, Vol 20.

DeVito, J.A. (2000), “Human Communication, The Basic Course”, 8th edition, Addison-Wesley Educational Publishers Inc., pp 66.

,

Donal O'Mahony, Michael Peirce, and Hitesh Tewari (2001), “Electronic Payment Systems for E-Commerce”. Artech House, Second edition.

Douglas M., Douglas. S.H and Rossi A. (1990), “Understanding the enterprise culture. Themes in the work of Many”. Edinburgh, Edinburgh University Press.

Dugelay J.-L., Junqua J.-C., Kotropoulos C., Kuhn R., Perronnin F., Pitas I., (2002), “Recent advances in biometric person authentication, online, IEEE Xplore, Acoustics, Speech, and Signal Processing, Proceedings”, IEEE International Conference, Volume: 4 , 13-17 May 2002, Pp 4060 4063 vol.4. http://ieeexplore.ieee.org

Electronic Banking. Http://www.electrobank.com/ebaeb.htm

Elliot S. and Loebbecke C., (1998), "Smart-card based electronic commerce: characteristics and roles" System Sciences”, Proceedings of the Thirty-First Hawaii International Conference on Digital Object Identifier.

Electronic Banking Resource Center. Http://www2.cob.ohiostate.edu/%7Erichards/bankpay.htm

Electronic Banking System. Http://www.electrobank.com/ebaeb.htm

Electronic International Banking, Http:/www.wwwebport.com/biz/gendex/elec_bank html

Federal Authority Over the Internet? The Cybersecurity Act of 2009, eff.org, April 10, 2009. Retrieved on June 26, 2010.

Fischer-Hubner S. (1998), “Privacy and Security at Risk in the Global Information Security.” Information, Communication and Society journal 1(4): pp 420-441.

Fischoff B. (1987), “Treating the public with risk communications: A public health perspective.” Science, technology and Human Values pp 12- 19.

Fisher R. (1984), “Information Systems Security”, Englewood Cliffs, Prentice-Hall.

Fitzgerald J. (1978), “FDP risk analysis for contingency planning.” EDP Audit Control and Security Newsletter 6(August): pp 1-8.

Forcht K. and Wex R. (1996), “Doing Business on the Internet: marketing and security aspects.” Information Management and Computer Security. Vol. 4, No. 4, pp 3-9.

Fulk J. and Boyd (1991), “Emerging Theories of Communications in Organizations.” Journal of Management 17(2) pp 407-446.

Galliers R.D. (1990), “Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy. The Information Systems Research Arena of the 90s: Challenges, Perceptions and Alternative Approaches”. Proceedings of the IFIP TC 8, WG 8.2. Working Conference, Copenhagen.

Galliers R.D. (1991), “Strategic Information Systems: Myths, Reality and Guidelines for Successful Implementation”. European Journal of Information Systems 1(1): pp 55-64.

Gary M. Wassermann (2002), “Techniques and Tools for Engineering Secure Web Applications”, dissertation submitted in partial fulfillment Doctor of Philosophy in Computer Science, University of California, Davis .

Gefen D. (2002), “Reflections on the dimensions of trust and trustworthiness among online consumers”. The DATA BASE for Advances in Information Systems, 33(3), 38-53.

Gefen D., Karahanna E., and Straub, D.W. (2003), “Inexperience and experience with online stores: The importance of TAM and trust.” *IEEE Transactions on Engineering Management, 50*(3), pp 307-321.

George F.F (2002), “Influences on the intent to make Internet purchases. Internet Research: Electronic Networking Applications and Policy”, 12(2), 165-180.

Gerrard P and Cunningham, J.B (2011), “The diffusion of Internet banking among Singapore consumers”. International Journal of Bank Marketing, 21(1), 16-28.

Ghosh, S. and Reilly D.L (1994), "Credit card fraud detection with a neural network", IEEE System Sciences. Vol.III: Information Systems: Decision Support and Knowledge-Based Systems, Proceedings of the Twenty- Seventh Hawaii International Conference, Volume: 3, pp 621-630.

Giddens A. (1994), “Risk, Trust and flexibility, Reflexive modernization” Cambridge polity press: pp 97

Goguen Alice, Feringa Alexis and Stoneburner Gary (2002), “Risk Management Guide for Information Technology Systems”, Computer Security Division Information Technology Laboratory ; National Institute of Standards and Technology Gaithersburg. Nist Special Publication 800, Julho.

Harney H and Muckenhirn C. (1997), “Group Key Management Protocol (GKMP) Architecture” RFC 2094.

Hole J.K., Moen V., Tjostheim T., (2006), "Case Study: Online Banking Security," IEEE Security and Privacy, vol. 4, no. 2, p. 14-20.

Holger and Sven Burmester; (2010) “Real – Time statechart Semantics, Technical Report tr-ri-03-239, Computer science Department, University of Paderborn

Http://www.ibm.com/Newsfeed/bankingpr.html, 15 North American banks and IBM form company to offer electronic banking and commerce services.
Http://HTTP.CS.Berkeley.EDU/~gauthier/endpoint-security.html

Http://www.f5.com/pdf/white-papers/intelligent-layer7- protection-wp.pdf , 22 August 2009

H.R.4962 - International Cybercrime Reporting and Cooperation Act, OpenCongress.org. Retrieved on June 26, 2010.

Herbert Stachowiak, Allgemeine Modelltheorie, Springer-Verlag, and Higgins, R. (1990), "Analysis for Financial Management." Singapore, Irwin Inc.

Hiltgen A., Kramp T., Weigold T., (2006), "Secure Internet-banking Authentication," IEEE Security and Privacy, vol. 4, no. 2, p. 21-29.

Hirst, A. (1999), "Channel Crossing.- The Banker". September 1999, p. 72-73.

Hoffman D. and Novak T. (1999), "Building Consumer Trust Online". Communications of the ACM 42(4): 80-85.

Hoffman J. and Michelman E. (1978), SECURATE- Security evaluation and analysis using fuzzy metrics. AFIPS National Conference Proceedings.

Ioannis V. Koskosas (2009), "Communicating Information Systems Goals:A Case in Internet Banking Security", ComSIS 84 Vol. 6, No. 1, June 2009

Information Security. United States Department of Defense, 1986

Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html

International Journal of Computer Science and Information Technology (IJCSIT), 2011

Introduction to PGP. Http://sun1.bham.ac.uk/N.M.Queen/pgp/pgp.html

Jackson Lee (2013) "Why Network Security May Become the Most Important and Profitable Tech Sector" China Sourcing fair, September 2013.

Jackson, N. and Carter P. (2013), "The Perception of Risk. Risk: Analysis, Assessment and Management", West Sussex, John Wyley & Sons Ltd.

Jarvenpaa, S.L, Tractinsky, N., and Vitale, M. (2000), "Consumer trust in an Internet store". Journal of Information Technology and Management, 1, 45-71.

Jochen Ludewig (2003), "Models in software engineering|an introduction". Journal on Software and Systems Modeling, 2(1):5{14, March 2003.

Johnson M. (2008), "A new approach to Internet banking". University Cambridge. (PhD) 2008, p. 113.

Joris Claessens, Valentin Dem, Danny De Cock, Bart Preneel, and Joos Vandewalle (2002), "On the Security of Today's Online Electronic Banking Systems. Computers & Security", 21(3): pp. 265.

Journal of Unity bank, Security Analysis for effective e- banking, (2013), ISSN 0197-6679

Karahanna E, Straub D.W and Chervany N.L (1999), "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs". MIS Quarterly, 23(2), pp 183-213.

Kelley E. (1999), "Y2K and Public Confidence in the Banking System" NY, Media Studies Centre.

Kirmsky S and Golding D (1992), "The Role of Theory in Risk Studies. Social Theories of Risk." Westport, CT, Greenwood Publishing Group, Inc.: 13-22.

Kirmsky S and Plough O (1988). Environmental hazards: Communicating risks as a social process, Auburn House.

Krzysztof Zatwarnicki (2012), "Adaptative control of cluster based systems using Neuro-Fuzzy model" International Journal of Applied mathematics and computer science, vol 22, No 2, p. 1.

Kuslick J.J and Rose Calroline (2013),"Server-Side Scripting; the Java way" Java on Tips posted 1st September, 2013.

Land, F and Hirschheim R (1983). "Participative systems design: rationale, tools and techniques." Journal of Applied System Analysis vol 10, pp. 91-107.

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

Laudon K and Laudon J (1996), "Management Information Systems: Organization and Technology". New Jersey. Prentice-Hall Inc.

Lawrence E., Corbitt B. et al. (1998), "Internet Commerce: Digital Models for Business" Singapore, Wiley

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

Liebenau J. and J Backhouse (1990), "Understanding Information". London Macmillan.

Mayer, R.C, H.J. Davis et al. (1995), "An Integrative Model of Organizational Trust." Academy of Management Review 20(3): 709 -734.

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

Mathias Mujinga and M.M. Eloff "Towards Usable Online Banking Security"

School of Computing University of South Africa, South Africa, p 1

Mathias Tichy and Margrete Kudak (2011), "Visualization of execution of Real – Time Statecharts", Software Engineering group, University of Paderborn.

Mathew Sorvaag (2010), "Rules for developing Network Diagrams – Network Diagram Management", Melbourne, Australia.

Martino A.S. and Perramon X. (2008), "A Model for Securing E-Banking Authentication Process: Antiphishing Approach", 2008 IEEE Congress on Services - Part I, Jul.2008, pp. 251-254.

Martino A.S. and X. Perramon (2008), "Defending E-Banking Services: Antiphishing Approach", 2008 Second International Conference on Emerging Security Information, Systems and Technologies, Aug. 2008, pp. 93-98.

Harkavy Michael and (1994), "Webster's new encyclopedic dictionary. Black Dog & Leventhal publishers Inc., 151 West 19th Street, New York 10011.

Microsoft, (2008), "An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008". Security Intelligence Report.

Morris R.T (1985), "*A Weakness in the 4.2BSD Unix TCP/IP Software* Computing Science" Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey.

Nami M. R (2009), "E-Banking: Issues and Challenges". 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, pp. 263-267.

Newman, M. and Sabherwal R. (1996), "Determinants of Commitment of Information System Development: A Longitudinal Investigation." MIS Quarterly 20(1) 23-54.

Nilson, M. A, Herd S (2005), "Building Security and Trust in Online Banking". Conference for human-computer interaction, Portland - Oregon – USA.

Ngwenyama, O, Nissen H. (1991), "The critical social theory approach of information systems: problems and challenges". The Information Systems Research Arena of the 90s: Challenges, Perceptions and alternative Approaches. Amsterdam North-Holland.

McNiven Valerie (2005), Online Banking: A Pew Internet Project Data Memo, www.pewinternet.org/PPF/r/149/report_display.asp US Treasury computer crime advisor in an interview with Reuters while speaking in Riyadh at a conference on information security in the banking sector.

Ollman, G. (2004), "The Phishing Guide—Understanding and Preventing Phishing Attacks", NGS-NISR.

Osuagwu O.E. (2008), "Insight into the new Frontiers of computer Forensics, Cyber-Criminality & internet security", OIPH, Owerri Nigeria, pp.11.

Osuagwu O.E. (2005), “Data Communication & Network Engineering Today” OIPH, Owerri Nigeria, pp 3

Otway, H and D Winterfeldt (1992). “Expert Judgement in Risk Analysis and Management: Process”, Context, and Pitfalls.” Risk Analysis 22(1), pp 83

Parthasarathy, M., & Bhattacherjee, A. (1998). Understanding post-adoption behavior in the context of online services. *Information Systems Research, 9*(4), 362-379.

Peotta, Laerte, Amaral Dinoet al (2007), Proceedings of the First International Conference on Forensic Computer Science Investigation, Braslia, pp. 38-42, ISSN 1980-1114.

Pavlou, P.A. (2003), “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model”. International Journal of Electronic Commerce, 7(3), 2003. p.101-134. JIBC August 2007, Vol. 12, No. 2, pp 10.

Parker D (1981), “Computer Security Management”. Reston Virginia, Reston.

Pfleeger, Charles P (1997), “Security in Computing”, Prentice Hall.

Powell, P. and Klein J (1996), “Risk management for information systems development.” Journal of Information Technology, vol 11: p.309-319.

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

Marsh Stephen P.(1994), “ Formalising Trust as a Computational Concept”, University of Stirling. - Scotland, UK, pp. 198.

Renn, O. (1987), “Evaluation of risk communication: Concepts, strategies, and guidelines. Managing Environmental Risk”. Proceedings of an APCA International Speciality Conference, Washington D.C.

Renn, O and Levine D. (1991), “Credibility and trust in risk communication. Communicating Risks to the Public” Academic Publishers, 1991. pp.175-178.

Rossmoore, D. and H. G. Levine (1993). “Diagnosing the Human Threats to Information Technology Implementation: A Missing Factor in Systems Analysis Illustrated in a Case Study.” Journal of Management Information Systems, 10 (2) pp. 55-73.

Ross J. Anderson (2001), “Security Engineering: A Guide to Building Dependable Distributed Systems”, pp. 185-206

Saltmarsh, T. and P. Browne (1983). “Data processing-risk assessment - Advances in Computer Security Management”. M. Wofsey. Chichester, Wiley, pp. 93-116.

Schaaf, J.(2005), "E-banking—Five Online Banking Trends in 2005," Deutsche Bank research paper no. 13.

Schneier (2000), “Secrets and lies: Digital security in a networked world” *pp. 398*

Senators Say (2010), “Cybersecurity Bill Has No 'Kill Switch'", informationweek.com. Retrieved on June 25, 2010.

Sierra Kathy, Berth Bates and Bryan Basham (2013), “Head First Servlets and JSP”, O’Relly media,ISBN 9780-596.

Smetters D.K and Grinnter R.E (2002), “Moving from the design of usable security technologies to the design of useful secure application” Palo Alto, USA, P.1

Solmes, R. V, Carroll J.M et al. (1993), “A process approach to information security management”. IFIP/Sec ’93, Deerhurst, Ontario Canada.

Solms, R., “Information security management: why information security is so important”. Information Management and Computer Security 6(4):1998, pp.174-177.

Sohail, S.and Shanmugham, B., “E-banking and customer preferences in Malaysia: An empirical investigation”. Information Sciences, vol. *150*, 2003, pp.207-217.

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

Stephen Northcutt, Donald McLachlan, and Judy Novak (2000), “Network Intrusion Detection: An Analyst’s Handbook”, 2nd Edition, New Riders Publishing; ISBN: 0735710082.

Sundram A, and Trina McNicholas (2010), Application of Agents and Intelligent Information Technologies, IGI Publishing

Suh and Han (2002) Information Systems Security. Englewood Cliffs, Printice -Hall

Steinmuller Sammy (1993), Don’t let Technology Pass you by, ABA Banking Journal, Vol 73

Tan, M., and Teo, T.S (2000), “Factors influencing the adoption of Internet banking”, Journal of the Association for Information Systems, vol.1, 2000. pp. 1-42.

Thawte, “The value of Authentication”, http://www.thawte.com, 18 July 2009.

The New Lexicon Webster's Encyclopedic Dictionary of the English Language. Wikipedia, New York: Lexicon.

Tiwari, Rajnish and Buse, Stephan (2007), The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector, Hamburg University Press.

Tiwari, Rajnish, Buse, Stephan and Herstatt Cornelius (2007), “Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage”. Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management, New Delhi, pp. 886–894.

Tiwari, Rajnish; Buse, Stephan and Herstatt Cornelius (2006), “Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises, Proceedings of The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, 2006 pp. 522–529.

Tognazzini Ruifeng (2005), Decision Support Systems and Intelligent Intelligent Systems

Vaidya “Emerging Trends on Functional Utilization of Mobile Banking in Developed Markets in Next 3-4 Years” 2011.

Vlek, C and. Stallen J (1981), “Judging risks and benefits in the small and in the large”. Organizational Behaviour and Human Performance 28, Pp. 235-271.

Weeks Stephen (2001), “Understanding Trust Management Systems”. IEEE Symposium on Security and Privacy.

Whyte, G., A. Bytheway, et al. (1997). “Understanding user perceptions of information systems success”. Journal of Strategic Information Systems 6: 35-68.

Willian Stallings (2006), “Cryptography and Network Security Principles and Practices,” Fourth Edition, pp. 483- 562

Winfield I (1986), “Human Resources and Computing”. London, William Heinemann Ltd,.

Willemssen J.C. (2000), "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives.

www.worldinternetstats.com, Nov. 2012.

www.javvin.com/networksecurity/CommunicationSecurity .html, 18, September 2009

Yahalom R., Klein B. and Beth T. (1993), “Trust Relationships in Secure Systems-A Distributed Authentication Perspective”, IEEE Symposium on Security and Privacy. Washington, DC, IEEE Computer Society, May 24-26.

Yan, J., Salah A. (2008), “Usability of CAPTCHAs or usability issues in CAPTCHA design”, Proceedings of the 4th symposium on Usable privacy and security. New York, NY, USA: ACM. p. 44--52.

Young, K. (1999), “Online Security Threatens Banks”. *The Banker.* September 1999, pp.21-23.

Zikmund, W. (1993), *“*Business Research Methods”, NY, I.E. Dryden.

APPENDIX 1

BANK INTERNET BANKING APPLICATION FORM

Account Details

Account Info

Account Title: ----------

Branch: ----------

Account No (NUBAN). :

Address ----------

****Phone** _----------,

****Email** _----------

Account Signatories/User

Signatory 1(A)

Name: ----------

Sign

****Phone (GSM)** _____

****Email** _____ ☐ **Send Log-In details**

Signatory 2(B)

Name _____

Sign

****Phone (GSM)** _____

****Email** _____ ☐ **Send Log-In details**

Signatory 3(C)

Name _____

Sign

****Phone (GSM)** _____

****Email** _____ ☐ **Send Log-In details**

For Official Use

CSO _____ _____ _____

Signature(s) verified by: Name & Signature of Officer | Staff ID | Stamp/Date

OPS MGR _____ _____

Processed by: Name & Signature of Officer | Staff ID | Stamp/Date

Approval _____ _____

Approved by: Name & Signature of Officer | Staff ID | Stamp/Date

NOTE: valid E-Mail Address is MANDATORY

Customer 'Log-On' details shall be sent to e-mail address provided above

It is your responsibility to keep your Internet Banking details safe and under your control. Do not reveal your 'Log On' password; it is your signature. Alpha Bank will not accept any liability for any fraud that may be committed on your account as a result of your failure to protect your password.

Your account will be debited with:

- **=N= 50.00 Monthly Fee**

I hereby agree to the terms and conditions here above stated: Sign …… Date:……

****Mandatory fields; must be completed by Customer**