OPEN ACCESS
Computer Science & IT Research Journal
P-ISSN: 2709-0043, E-ISSN: 2709-0051
Volume 3, Issue 2, P.52-65, July 2022
DOI: 10.51594/csitrj.v3i2.355
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

# FRAUD PREVENTION AND DETECTION SYSTEM IN NIGERIA BANKING INDUSTRIES

Kamalu Aliyu Babando[1]

[1]School of Basic and Applied Sciences, Taraba State Polytechnics, Suntai. Jalingo Campus, Nigeria

*Corresponding Author: Kamalu Aliyu Babando
Corresponding Author Email: kab_babando@tarabapoly.edu.ng
**Article Received:** 10-06-22 **Accepted:** 01-07-22 **Published:** 17-07-22



## ABSTRACT

Fraud is on the rise as a result of the advent of modern technology and the global superhighways of banking transactions, resulting in billions of dollars in losses worldwide each year. Although fraud prevention technologies are the most effective method of combating fraud, fraudsters are flexible and will usually find a way around them over time. We need fraud detection approaches if we are to catch fraudsters after fraud prevention has failed. Statistics and machine learning are effective fraud detection technologies that have been used to detect money laundering, e-commerce credit card fraud, telecommunications fraud, and computer intrusion, to name a few. The program is simple to use, and anyone with permission can use it. The importance of computer technology has expanded as it has advanced in all areas of human endeavor.

**Keywords**: Fraud Detection, Fraud Prevention, Banking Industries, Telecommunications.

## INTRODUCTION

Fraud is on the rise as a result of the advent of modern technology and the global superhighways of banking transactions, resulting in billions of dollars in losses worldwide each year. Although fraud prevention technologies are the most effective method of combating fraud, fraudsters are flexible and will usually find a way around them over time. We need fraud detection approaches if we are to catch fraudsters after fraud prevention has failed. Statistics and machine learning are effective fraud detection technologies that have been used to detect money laundering, e-commerce credit card fraud, telecommunications fraud, and computer intrusion, to name a few. The statistical fraud detection instruments are presented, as well as the fields where fraud detection technologies are most typically used. Fraud develops significantly each year, leading in the loss of vast amounts of data all across the world. Banking fraud is defined as any action taken to gain a service without the intention of paying for it. Using this concept, fraud can only be identified after it has occurred. As a result, it's critical to distinguish between fraud prevention and fraud detection. Fraud prevention encompasses all steps that can be taken to prevent fraud from occurring in the first place. Customers' identification cards, as well as any other Personal Identification Number (PIN), such as those used in Private Branch Exchanges, are examples of these in banking systems (PBX). There is no perfect preventative strategy, and most are a trade-off between effectiveness and usability. On the other side, fraud detection is the process of discovering fraud as soon as possible after it has occurred. The problem is that fraud strategies are constantly evolving, and once a detection method is discovered, fraudsters will change their minds and try something different. Ref establishes the legal principles that apply in many areas of law that are affected by the use of fraud detection technology in banking. This study underlines the significance of secrecy and personal data security. The development of fraud detection systems and the exchange of ideas in this field are limited by the fact that discussing the procedures in full would be worthless because it would reveal too much information. They claim that (Jealous, et al.,2014).

Fraudsters want information in order to avoid detection. Another challenge is that fraud detection requires enormous, constantly changing data sets. Banking system fraud is classified into four types by Reference: contractual fraud, hacker fraud, technological fraud, and procedural fraud. In Ref., there are twelve different types of fraud identified. This essay's authors have witnessed a combination of the aforementioned misleading acts. The fraudster obtained the ability to place overseas orders as a firm employee by acquiring a legitimate PIN to use in the banking system, but he had no intention of paying for these services (contractual fraud). Furthermore, he shared the PIN with others who accessed the service without paying (hacking fraud). In another case, an employee with advanced technological knowledge was able to fool the system and obtain a PIN that belonged to someone else. He then began using the PIN while pretending to be the legitimate user, resulting in a charge on the legitimate user's account (superimposed fraud).

In the first situation, fraud is only detectable after it has occurred, and the only method to avoid it is to cancel the service subscription. The second scenario is more difficult. After posing as someone else, the fraudster can carefully place only a few calls. Unless his account balance

reaches a specific level or he carefully reviews an itemized account, the honest user may never notice the scam. According to (Kotonis – Chair, 2013).

**Fraud**

In the literature, fraud has been defined in numerous ways. Most developing countries throughout the world consider fraud to be a criminal offense. It is also a felony in Nigeria, which prompted the publication of a decree on fraud and other fraud-related matters/structures, specifically "the failed banks and recovery of public debts decree 18 of (2011), banks and other financial institution decree (BOFID) 2010, Money laundering Act No 3 of 2012. Federal Intelligence Investigation Bureau (FIIB), Independence Corrupt Practices Commission (ICPC), and Economic and Financial Crime Commission (EFCC). According to the Oxford Advanced Learners Dictionary of Current English, "fraud" is defined as a criminal act/deception. Fraud, according to Udo (2012), is concerned with the acts of individuals who aim to redirect the results of others' hard work into their own pockets. According to Adeniyi (2014), fraud is defined as a purposeful conduct by one or more individuals, among management personnel or third parties, that results in a falsification of financial statements;

1. Manipulation, falsification or alteration of records of documents.
2. Misappropriation of Assets.
3. Suppression or omission of the effect of transactions from records or documents.
4. Recording of transaction without substance.
5. Misapplication of accounting policies

Adekanye says (2012), Fraud is defined as the falsification or alteration of a written document with the intent of causing harm to another person. He went on to clarify that any alteration to a writing document with the aim to defraud is therefore forgery.

According to Wikipedia, fraud is any cunning, sneaky crime that destroys persons and families and causes businesses to fail. Fraud, according to Eze (2014), is defined as irregularities involving the use of criminal deception to acquire an unjust or illegal advantage. Another definition of fraud is "an act by which one person intends to obtain an unfair advantage over another."

**Bank Fraud**

Bank fraud is not a recent occurrence. They are older than the industry. Bank fraud is defined as a deliberate or intentional attempt to get unlawful financial gain at the expense of another individual who is the rightful owner of the funds (Orjih, 2015). Bank fraud should be generally defined as acts involving the loss of assets by banks through deceitful and dishonest means. The fraudster's goal is to defraud the bank, bank employees, bank clients, or any other member of the public by defrauding them through financial operations. Bank customers, bank personnel, or a combination of staff and customers or non-customers can all commit fraud. Furthermore, like a canker worm, bank fraud has entered our social fabric, and reducing its prevalence will need a joint effort from citizens, governments, bank staff, and relevant authorities. Unfortunately, bank officials are typically hesitant to discuss specifics about possible frauds at their banks for fear of ruining their company's reputation (Eze, 2014).

**Nature and Types of Bank Frauds**

The nature, style, and methods of operation of bank frauds vary greatly. In general, fraud can be committed in a variety of ways. Bank fraud can be divided into three categories based on the perpetrators (Shogotola, 1994).

(a) Internal fraud

(b) External Fraud

(c) Mixed Fraud.

**(a) Internal Perpetrators of Fraud:** Insiders include accountants, executive assistants, supervisors, clerks (cashiers), typists/stenographers, technicians, drivers, and cleaners, among others.

**(b) External Fraud:** These sorts of fraud are those conducted by individuals unrelated to the bank. An example might be an armed robbery attack during banking hours or during a special movement of cash in transit. Furthermore, some external fraud may occur as a result of some customers' carelessness, recklessness, or negligence. It frequently comes through corporate accounts, where a dishonest employee may have access to the company's check book.

**(c) Mixed Fraud**: These are instances of fraud conducted by coordination between insider employees and external clients. It is widely assumed that no effective fraud can be carried out without the assistance of insider personnel. For example, in one of the most egregious armed robberies in 2010 against Union Bank Plc, Nnewi, the employee dispositions chart seized from the bad debt was allegedly produced by a number of staff members (insider). That is why Shongotala warns that the banking industry has become a genuine minefield on which some banks and their top management employees are in secret league with the enemy, rather than a battleground with a clear-cut firing line between banks and fraudsters.

**Fraud Detection Techniques**

***Expert Systems***

The expert system is a feature of computing systems that can provide and argue in some deep areas of knowledge while analyzing and solving problems (Majumdar, 2006). Knowledge is encoded in the form of law by expert system detectors. That is, the law specifies whether and when events must occur, as well as in which state they must occur. The NIDES system, for example, uses online monitoring of user behaviour to identify assaults. Statistical analysis components and rule analysis tools were included in the NIDES system to detect abnormalities and misuse.

***Neural Network***: A neural network is a collection of nodes that are linked together to imitate the operation of the human brain. Each node in the adjacent layer communicates with a large number of other nodes using weighted communications. The data structure in neural networks is known as a node, and software that can act as neurons to these data structures is also known as a node. The networks are then trained by linking these nodes together and applying a learning algorithm to them. This memory or neural network's nodes have two active modes (on or 1) and two inactive modes (off or 0), and each synapse (connection between nodes) has a weight. Synapses with a positive weight stimulate or enable the next inactive node, whereas synapses with a negative weight disable or inhibit the next connected node (if be active). According to Sharma (2011), an

artificial neuron is a system with many inputs but just one output. There are two categories of neuron cases: education and performance. The neuron learns that it is excited against specific input patterns and is thus fired in the case of education, but the emerging process of financial frauds is generally diagnosed through the analysis and extraction of information (data analysis) from the information bank of financial institutions transactions that will be marked, and this issue aids in the development of policies and security protocols, as well as the attainment of new identity pattern enter. If the input is not a component of the listed inputs, the fire rules decide on its arousal and insufficiency. Braves and Langsdorf pioneered the use of a combination of role-based continuous systems and neural system approaches. The Falcon Fraud Management system, which is a powerful tool for avoiding fraudulent activity in the usage of debit and credit cards, employs neural network algorithms. By comparing the current transaction to the cardholder's historical behaviour, this system forecasts the possibility of account fraud (Liu, 2014). If this system detects a card fraud transaction, a call will be placed with the card as soon as possible to prevent the fraud, and the card will be disabled. If the Falcon system detects fraud but there is no way to prevent fraud with the card, the card is temporarily blocked, and the card holder should pursue the situation by phone with the bank's call center, and the card will be blocked until the card holder does not register contact with the call center. This system can use neural networks to train a cardholder's spending behavior and detect any irregularities in the technique and how to pay the money, which is considered fraud. The Falcon prediction system was designed and developed using contributed approaches and machine learning technologies such as adaptive pattern recognition, neural networks, and statistical models. Another example of a network application is the MLP Neural Algorithm. This algorithm just works with transaction data and does not require to access the cardholder's previously recorded information history on the information bank. Another example of neural network application is the grain parallel neural networks method, which employs both fuzzy neural networks and a role-based approach. The NNID system, which is an anomaly detection system constructed by the corporate neural network and operates on the UNIX operating system, is one of the neural network-based attack detection systems (Ghosh and Reilly 2014).

This system's performance is reviewed in such a way that it influences the users' behavior throughout the day. This system is incredibly convenient and economical to use because it stores daily log data and can be used offline. Both anomaly detection and abuse detection employ artificial neural networks to predict previously unanticipated future user behaviour. These methods rely on the neural networks corporation. (Ghosh and colleagues, 2014)

***Model-Based Reasoning*:** Model-based reasoning is an anti-abuse strategy that looks for obvious behaviors that can be determined using an attack signature to detect attacks. A single information bank representing the attack scenario is necessary for this, and it must include the signature or sequence of attack behavior. This technology recognizes assaults based on their signatures and the information bank that holds them, similar to how antivirus software recognizes viruses based on their signatures on files. The system that is based on this accumulates evidence of the attack and does it repeatedly until it meets the threshold. At the moment, one attack has been identified and will be reported as soon as possible. The pattern-matching technique provided by komarand

Spaford is used to detect abuse assaults based on colored Petri nets. In a Linux context, this pattern is utilized as an audit trail for input. (Nejad, 2015).

a) **Internal Perpetrators of Fraud:** This relate to members of staff (insiders);Accountant, Executives Assistance, clerk(cashier), Typist/Stenographers, Technicians, Drivers, clearners e.t.c.

b) **Eternal Fraud:** These types of fraud are fraud related to those committed by persons not connected to the bank. A typical example was that of fraud armed robbery attack either during the banking hours or during special movement of cash in transit. More so some external fraud could result through carelessness.

## METHODOLOGY

Structured System Analysis and Design methodology (SSADM) is utilized to complete these tasks. It enabled us to create a software design and database design, which was the primary goal of the research.

### Analysis of the Existing System

We would have to break down the existing system into numerous autonomous components in order to adequately analyze the function of each component and how they interact with one another. System analysis is an essential component in the life cycle of a system. In order for an ideal system to be constructed to meet its primary goal, it must be systematically studied. This includes system analysis as one of the problem-solving strategies. The following are existing system transactions:

i. Transactions Text Message Alert
ii. Dispense Error
iii. Online Money Transfer
iv. User Query Alert

### Analysis of the Propose System

The primary goal of studying the proposed system is to develop a system capable of meeting managerial requirements, that is, a system capable of replacing every single procedure in the existing transaction. As a result, the system Design process is an important and critical stage in a system's life cycle. However, when examining the proposed system, the following implementation must be taken into account:

i. Update the system for instance account number generation
ii. Use image verification during transaction
iii. Check for fraudulent activities.
iv. User authentication

### Database Design

The most significant steps in information processing are the input and output processes, with storage in between. Data can be saved to be processed later, and the output of operations can be saved for later use. At this point, it is almost always required to construct multiple files that will be utilized by programs for data storage. A database is a collection of connected entities that may be retrieved and explored later. Figure 1 depicts the database structure.

**Table 1: Table File**

| S/no | Name | Type | Length | Key | Extra |
|---|---|---|---|---|---|
| 1 | Id | Alphanumeric | 11 | PRIMARY | AUTO_INCREMENT |
| 2 | File_name | Alphanumeric | 50 | - | - |
| 3 | File_number | Alphanumeric | 50 | | |

**Table 2: Users Bio Data**

| S/no | Name | Type | Length | Key | Extra |
|---|---|---|---|---|---|
| 1 | user_id | INTEGER | 11 | PRIMARY | AUTO_INCREMENT |
| 2 | f_name | TEXT | 50 | - | - |
| 3 | s_name | TEXT | 50 | - | - |
| 4 | Username | ALPHANUMERIC | 50 | - | - |
| 5 | Password | ALPHANUMERIC | 50 | - | - |

**Table 3**

| S/no | Name | Type | Length | Key | Extra |
|---|---|---|---|---|---|
| 1 | ID | INTEGER | 11 | PRIMARY | AUTO_INCREMENT |
| 2 | Attempted_username | Alphanumeric | 50 | - | - |
| 3 | Attempted_password | Alphanumeric | 50 | - | - |
| 4 | Attempted_date | Alphanumeric | 50 | - | - |
| 5 | Attempted_file | Alphanumeric | 50 | - | - |

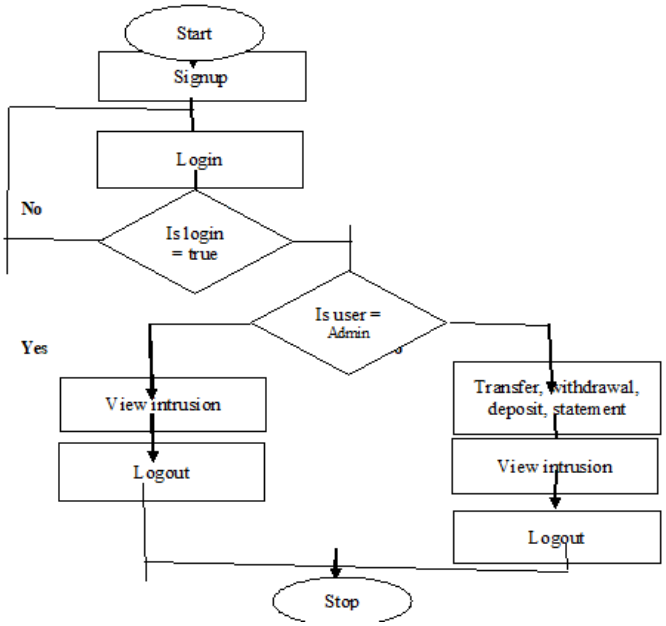


Figure 1: System Flow Chart

## USE CASE DIAGRAM

### Admin User

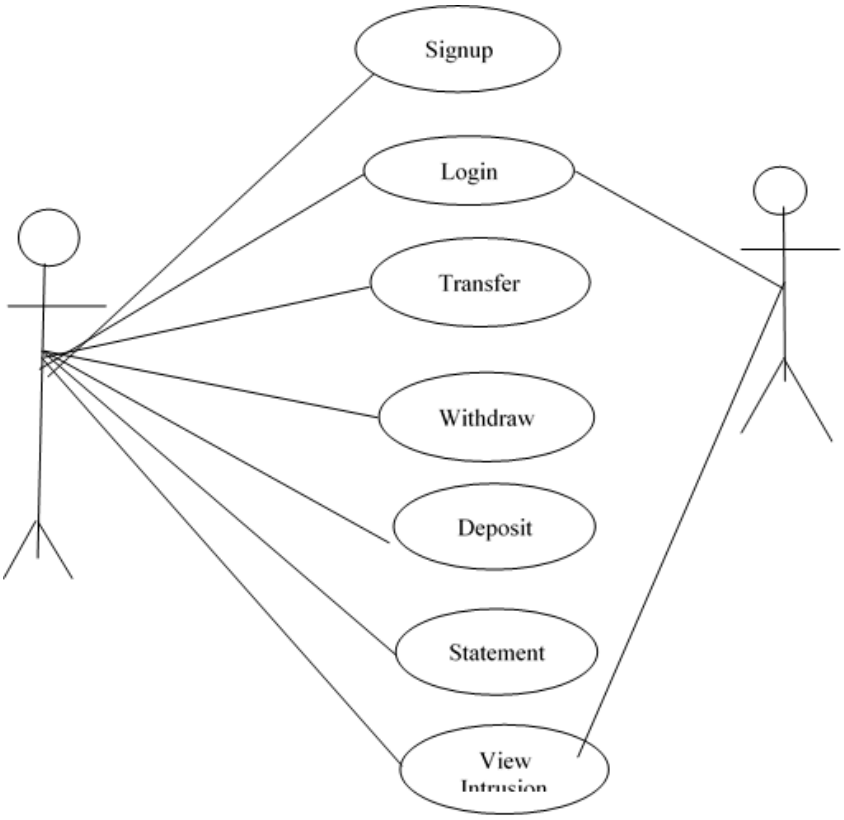


Figure 2: Admin User

## ENTITY RELATIONSHIP DIAGRAM

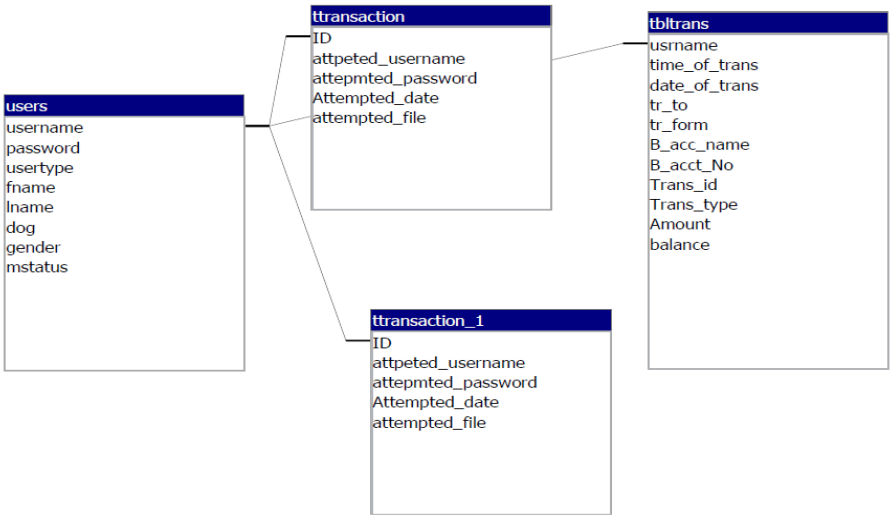


Figure 3:Entity Relationship Diagram

## SYSTEM DEVELOPMENT METHODOLOGY

The system employed waterfall model to design, implement and deploy the application

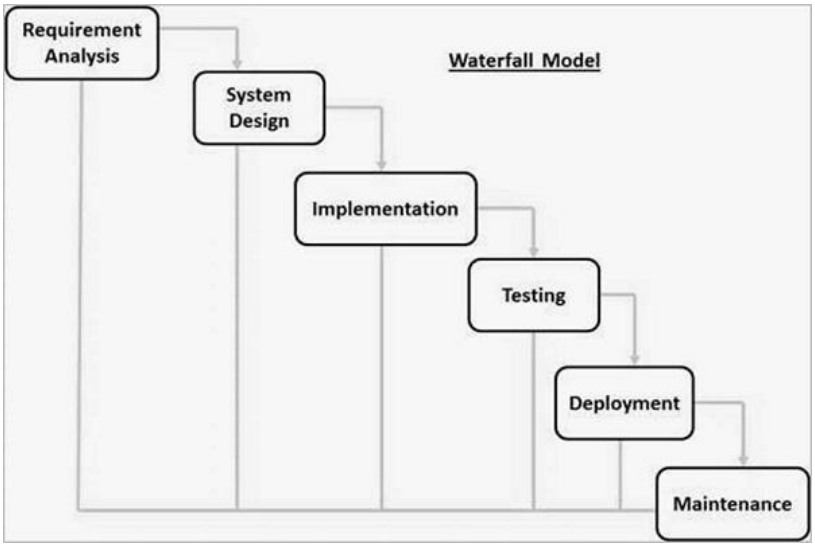


Figure 4:System Development

### System Requirement

For the software to run correctly and efficiently it will require a computer with,

i. Windows 2000/XP/7
ii. CD-ROM Drive
iii. Hard disk of at least: 1GB
iv. RAM of at least: 256MB
v. Processor: Pentium IV
vi. Printer (optional)

### Software Requirement

i. Windows operating system
ii. Web browser
iii. Server base application example: XAMPP, WAMP of higher version

## IMPLEMENTATION AND RESULT

### Programming Paradigm

This is concerned with the programming language used in the system's implementation. Microsoft Visual Basic was used to develop the GUI (Graphical User Interface) and write source code for each event in the system in this research project. To complete the testing stage, the system was compiled using the IDE (Integrated Design Environment), and an executable file was prepared for deployment and distribution on other systems.

### Choice of Programming Language

Because this proposed system is a "Fraud Detection and Prevention System," the above-mentioned language is a good choice for compatibility with the Windows PCs on which it will be installed, as

well as to save time during the design stage. Visual Studio, on the other hand, has the following characteristics:

1. It's a non-procedural language
2. It's an event-driven language
3. It's an Object-Oriented Programming (OOP) language.

## PROGRAM MODULES

This system is made up of numerous modules that work together to form a single unit. Modularity is a desirable feature in a program because it makes it easier to maintain, update, and change the program.

**Home Page**


Figure 5:Home Page

This is where the user is expected to either signup or login for his/her desired services.

**Login Form**

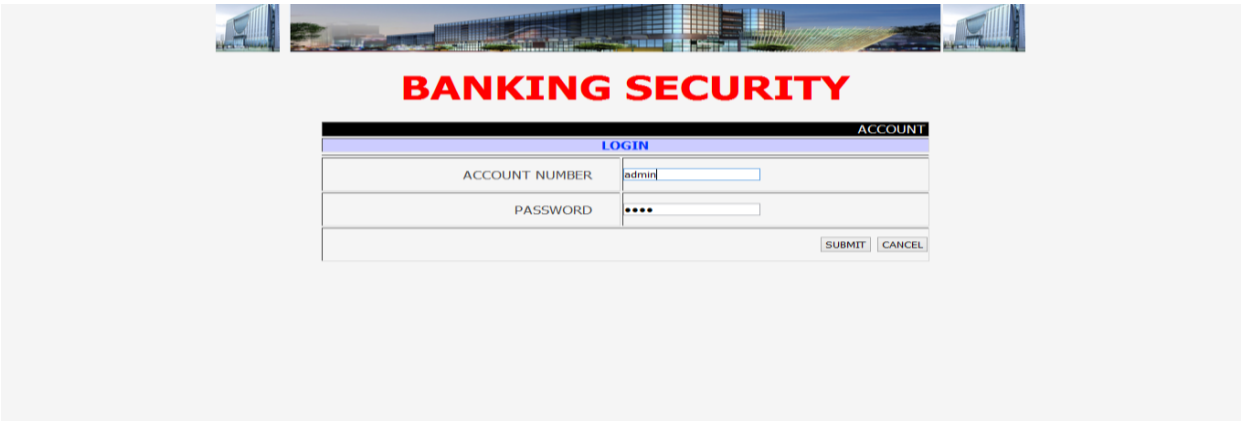


Figure 6: Login Form

Login form provide the user the right to have access to his account and have a desired service

**Main Menu of Bank Operation**


Figure 7: Main Menu of Bank Operation

This provide customers with various banking operation such as Transfer, withdrawal, Deposit, view of bank statement and view malicious activities in their account

**Transfer Form**

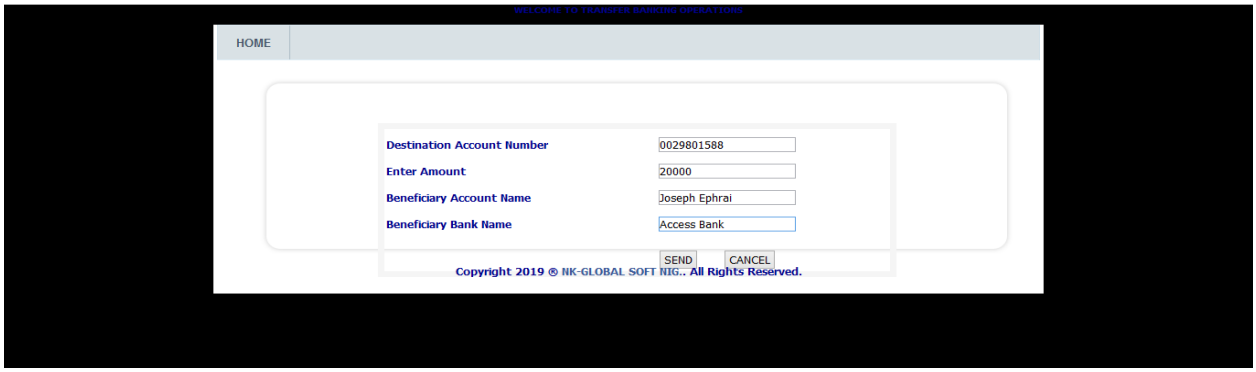


Figure 8: Transfer Form

This enables a user to carryout transfer operation using the software in banking system

**Account Statement Form**

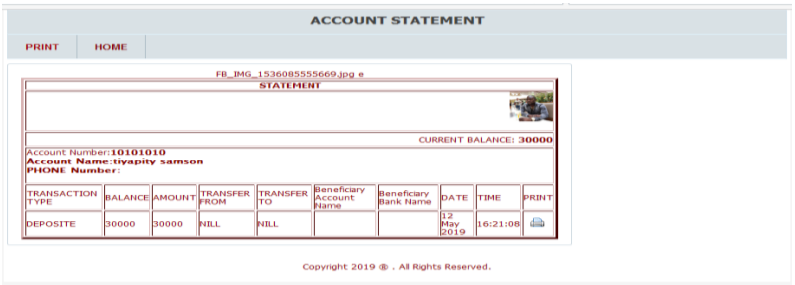


Figure 9: Account Transfer Form

This is the details of banking operation or transaction carried by a customer in a particular given time

**Intrusion View Form**

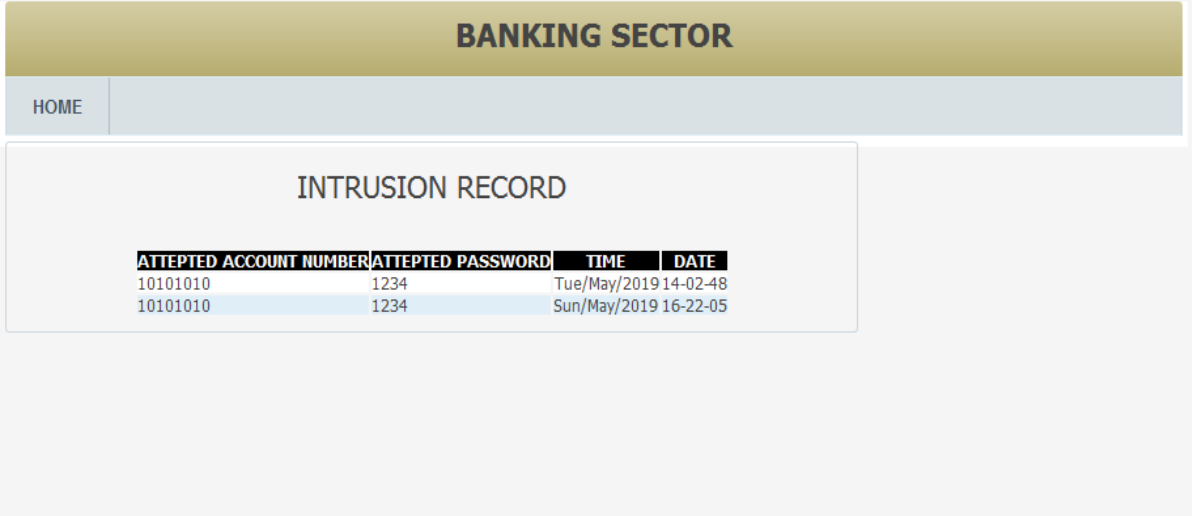


Figure 10: Intrusion View Form

This is the result of unauthorized access to a user account by Intruders, to gain access to the users' information and resources.

**Authentication and Authorization**

The software is incorporated making most of the pages secured or protected which demands only approved users gaining access to such pages. The secured pages comprises of the user login details. The software utilized and validate user credentials which help manage user authentication. Authentication is the process of inputting a user name and password to gain access to a specified secured form. The software also utilizes the role of management to manage authorization allowing the ability to specify the resources users are allowed to access. It enables the treatment of group of users as a unit by assigning users to specific roles and creating access rules for them. When a user requests for a protected resource, take for instance, the user page, will redirect the user to logon page where he has to enter the required credentials, usually a token. The membership validate user‖ method in the code-behind file checks the name entered and compares it will all the names in the membership store, when it finds a match, it compare the token entered with the token of the match found in the store. If they are both the same, it attaches an authentication ticket to the response that represents the use credentials (the token not included) and if not, returns the user to the log on page with an access denied message. If the user is authenticated, the user in role method further checks if that name entered has authority to access the resource requested. It does this by checking the access rule if the user's role can access the resource requested for. If it comes out with booking true, then the user is given access and the page or resource requested for open and if it comes out with booking―false‖, the user is returned to the logon page with an access denied message. This procedure helps to ensure that a user does not log in as an administrator and vice-versa thereby viewing resources that are not meant to. It is also important to note that the authentication ticket issued to an authenticated user remains active until the user logs out or the session expires.

## TESTING

### Unit Test

Creating a strong and logical test plan is critical to creating a bug-free software system. The following is the unit test plan created for testing this application:

### System Design

Some of the tools that can be used to design a system are as follows:

i. **Algorithm:** This is a procedure for solving a specific problem(s) that is/are not ambiguous. Deterministic and guarantee to terminate on a complete execution.

ii. **Flow Chart:** This is graphical or diagrammatical presentation of sequential steps, required to solve a programming or systematic problem(s).

iii. **Pseudo Code:** A code used to clearly outline the logic plan of a program.

iv. **Structure Chart:** These employ square shapes to identify a program's processing steps. This is particularly beneficial when the program(s) are divided into modules. Among the techniques mentioned above, the latter was utilized to identify the processing steps of this system utilizing a top design approach structure chart. The diagram starts with a module that provides full security to any authorized users by requiring a user name and password before granting access to the system for any input or output activities.

## CONCLUSION

A comprehensive Fraud Detection and Prevention System is a computer software that may be distinguished from the human approach of identifying any illicit banking activity. The primary goal of this research is to determine the impact of information technology (IT) on the efficient and successful functioning of businesses. When the disadvantages of the manual technique are considered, it is clear how the usage of an information system can readily improve on the implementation of the aforementioned software.

The system's operation is researched; fact-finding techniques are employed to analyze the current system of operation in order to identify the problem. Macromedia Dreamweaver was utilized in the design of the new system, and PHP was used in the construction of the software that makes up the various procedures. The system was evaluated and proven to be more efficient and dependable in dealing with any banking unlawful transaction issue.

Looking at this research, the system's improvement, efficiency, and quick service have outweighed the human way of detecting banking criminal activities. The application is simple to use and may be used by any authorized individual. With the advancement of computer technology, its significance can be observed in all aspects of human activity.

### Recommendation

Based on the findings and discussion, the following recommendations are made for improvement in maintaining the standard of this software.

i. Bank should adopt and use the developed package

ii. Awareness should be created on the benefits that can be derived from the use of this application.

iii. There should be time – to – time orientation on the use this application in standard micro-finance bank to facilitate its operation.

The imperfection of this software design should be dully observed and considered by future researchers for further study.

**References**

Becket, B. (2017). *Introduction to fraud prevention System.* Blackwell Scientific Publication. London.

Behrouz, A., & Forouzan, P. (2015). *Fraud control system in banking sectors*. Nashville, TN: Vanderbilt University Press. New York.

Burnett, S., & Paine, S. (2013). *RSA security official guide to fraud control.* Berkeley, CA: Osborne/McGraw-Hill Press.

Burton, S., Kaliski, J., Matthew, B., & Robshaw, J. (2016). *How to control fraud.* MIT Press. London

El Gamal, T. (2015). *Ways of fraud occurance in various sections*. Macmillan Publishing Company. New York

Gamed, R., Knudsen, J., & Erik, M. (2014). *Fraud control in telecommunication*: Prentice Hall Inc. Press.

Liddell, D., & Scolt, L. (2016). Ways of detecting and preventing *fraud.* Oxford University Press. London

Menezes, A., Van, O., & Vanstone, A. (2014). *Guide to control fraud in banking*. Berkeley, CA: Osborne/McGraw-Hill.

Moris K., Irfan, G., Hussain, M. (2010). Fraud detection in banking sector. *International Journal of Advanced Science and Technology*, *34*.

Parag, K., Shelke, S.S., & Gavande A.D. (2012). Issues of Intruders in bank. *International Journal of Scientific and Technology Research*, *1(*4).

Prema, J., & Kumar, A. (2014). *Ensuring bank security* Mangalore Institute of Technology & Engineering, Moodbidri, Karnataka1.

Pascal, J. (2015). *On the complexities of fraud control attack.* McCraw –Hill Book. New York

Rivest, R.L., Shamir, A., & Ad leman, L. (2015). On a method for obtaining digital signatures and public key on detecting and prevention fraud.