CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Frauds have plagued telecommunication industries, financial institutions and other organizations for a long time (Jia and Jongwoo, 2005). The type of fraud addressed in this dissertation is called credit card transaction fraud. This fraud costs financial institutions millions of dollars per year. As a result, fraud detection has become an important and urgent need for these businesses.

Currently, data mining is a popular way to combat frauds because of its effectiveness. Data mining is a well-defined procedure that takes data as input and produces output in the form of patterns (Hand *et al.*, 2002). In other words, the task of data mining is to analyze a massive amount of data and to extract some usable information that one can interact with for future uses. Once one has the right model for the data, the model can be used to predict future events by classifying the data. In terms of data mining, fraud detection can be understood as the classification of the data. Input data is analyzed with the appropriate model that determines whether it implies any fraudulent activity or not.

A well-defined classification model is developed by recognizing the patterns of former fraudulent behaviors. Then, the model is used to predict any suspicious transaction implied in a new data set. Data mining and model construction require a lot of time, which prohibits it to detect frauds in real time. This is a serious setback since, in many occasions such as online credit card transactions, one need to detect fraudulent activities in a very short period of time, typically while the fraudster is still at the banking hall. Otherwise, the loss could be huge.

Multi-agents are computer programs that can act on behalf of a person to do various jobs. Multi-agents can automate a large portion of fraud detection process and require little human intervention. Additionally, multi-agents do not stick to one model or rule. They can construct new models and rules for fraud detection with their machine capabilities. It will be harder to deceive multi- agents than other computer programs for fraud detection. Besides, in a multi-agents system, many multi-agents can work in parallel and cooperate with each other. This not only accelerates the detection process but also increases the detection accuracy. Moreover, multi-agents can be deployed online for real-time detection. This is an extremely desirable feature for online credit card fraud detection and network intrusion detection.

Fraud in organization and industries of late has taken on a new dimension. This is due to the advances that have been made in information technology. Its increasing waves have resulted in a whole lot of havoc in various organizations. For businesses and organizations alike, fraud alongside financial crime is not an acceptable way of carrying out day to day operations. Fraud schemes are ever on the increase, its cost is on the increase, same as customers' expectations. Fraud has resulted in financial losses; it costs much to investigate and to pursue attendant litigation. Fraud eats away impinges on customer/consumers' confidence and ruins brand image. It is indeed the number one enemy of the business world. In recent times, surveys conducted by leading internal consulting firms indicate that fraud in the financial sector is rapidly increasing as information technology in this sector advances and most of the reported cases involve data manipulation with assistance of bank staff working hand in hand with external fraudsters (Lee *et al.,* 2005).

One such aspect of banking where there is high rate of abuse of office and some level of collaboration in perpetrating fraud is in the case of credit card. Timely information on fraudulent activities is strategic to the banking industry. Banks have many and huge databases. Valuable business information can be extracted from these data stores. Credit card fraud detection is the process of classifying those transactions into two classes of legitimate (genuine) and fraudulent transactions (Singh *et al.,* 2014). Credit card frauds can be broadly classified into three categories, viz: traditional card related frauds (application, stolen, account takeover, fake and counterfeit), merchant related frauds (merchant collusion and triangulation), and Internet frauds (site cloning, credit card generators and false merchant sites). Data mining is a process that uses a variety of data analysis tools to discover patterns and relationships in data that may be used to make a valid prediction (Singh *et al.,* 2014). In everyday life, credit cards are used for purchasing goods and services using online transaction or physical card for offline transaction.

In credit or debit card based purchase, the cardholder presents card to a merchant for making payment. To commit fraud in this kind of acquisition, the fraudster has to steal the credit card. If the legitimate user does not understand the loss of card, it can lead to important financial loss to the credit card company and also to the user. In online payment mode, attackers need only little information for false transaction, for example, secure code, expiration date, card number and many other factors. In this purchase method, many transactions will be done through Internet or telephone. To obligate fraud in these types of purchases, an impostor simply needs

to know the card details. Most of the time, the honest cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any irregularity with respect to the "usual" spending patterns. The examination of existing purchase data of cardholder is a likely way to reduce the rate of positive credit card frauds. Since humans tend to display specific behaviorist profiles, every cardholder can be characterized by a set of patterns comprising information about the distinctive purchase category, the time since the last buying, the amount of money spent, and other things. Nonconformity from such patterns is reflected as fraud.

Credit card frauds are increasing day by day as the use of credit card is increasing (Patel, 2014). Occurrence of credit card fraud has increased dramatically both online and offline. Credit card based purchase can be done in two ways: (i) physical card (ii) virtual card. In physical card purchase, the cardholder presents his card physically to the merchant for making payment. For this type of fraud the attacker has to steal the credit card. In virtual card purchase only the information about the card is stolen or gathered like card number, secure code etc. Such purchases are done over the Internet. For this type of fraud the attacker needs only the card details so the only way to detect this type of fraud is to analyze the spending pattern of the card holder. When one's credit card or credit card information is stolen and used to make unauthorized purchases on e-commerce systems on the Internet, one becomes a victim of internet credit card fraud or no card present fraud. This is nothing new and there is nothing unusual about this because identity theft and credit-card fraud are present-day happenings that affect many people and involve substantial monetary losses. Fraud is a million dollar business and increasing every year.

Credit card is refers to a method of selling goods or services without the buyer having cash in hand (Delamaire *et al.,* 2009). A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer's bank – also known as issuing bank – which provides the credit services to the consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to the consumer by charging consumer's credit card. This charge is achieved through merchant's bank – the forth entity – which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card's limit before

authorizing that transaction. If the transaction is valid, the issuing bank will block the requested amount from consumer's credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant's bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods. The blocked amount on consumer's credit card account will be transferred into merchant's bank account.

1.2 Statement of the Problem

Information Technology (IT) has contributed to a great extent in mitigating fraud for banks that have embraced and implemented it. Credit card transaction frauds cost financial institutions millions of dollars per year. As a result, fraud detection has become an important and urgent task for this business. The incidents of loss of hard earned money to fraudsters have raised a lot of concern and portend serious danger to economic growth. Ordinarily, thieves invade homes and offices to steal physical cash from their victims. The rapid development in information and communication technology has introduced a cashless society where people can pay for goods and services using credit cards. This appears more secured as people no longer keep huge physical cash at home; leading to less incidents of theft. The recent development shows that hackers have device electronic means of stealing money from people's account by stealing their credit card details and using same to transfer money to other accounts. This is heart breaking and requires an enhanced security system on communication channels to avert such financial loss. Another challenge for contemporary financial institutions is the ability to understand and deal with the high volume of data and information, and using knowledge from them to improve and make informed decisions. Credit card fraud detection is a pattern recognition problem. Every cardholder has a shopping behavior which establishes a profile for the cardholder. Currently, fraud detection system (FDS) identifies many legitimate accounts as fraudulent resulting in a large number of false positives (FPs). As every cardholder has a huge number of possibilities for developing new patterns of behavior, the types of transactions are widely variable. Hence, it is almost impossible to identify consistent and stable patterns for al1 the transactions. In fact, there are so many variations of behavior for each individual that are exponential in combination and the complexities of enumerating all combinations of cases are enormous. This ever changing pattern of behavior with the combination of legitimate and fraudulent cases has left the Financial Institutions (FIs) with a large number of FPs (approximately 90% of flagged accounts) for investigation. The above challenges can be addressed through the use of a multi-agents system that is based on artificial

intelligence since it will provide managers with added value information reduce the uncertainty of the decision outcome and thereby enhance banking service quality. No doubt, the application of new technologies can give bank a competitive lead to a high performance and eliminate fraud associated with credit cards. Credit card frauds (CCF) have been a long –time headache for credit card companies. With the growth of online business in Nigeria, the number of credit card frauds has also increased drastically.

1.3 Aim and Objectives of the Study

The aim of this dissertation is to design and develop an enhanced model for credit card fraud detection in Nigerian banks.

The specific objectives are:

1. To characterize the information source and identify the security problems inherent in the communication channels for credit card transactions
2. To provide a means of detecting and preventing credit card fraud in a real –time transaction on the Internet.
3. To model a security system that will promote trust in communication channels by implementing hybrid technology that will combine both adaptive data mining and multi-agents to authenticate the credit card transaction.
4. To develop a system using PHP-MySQL and java script to implement the credit card fraud detection model which can authenticate credit card transactions.
5. To evaluate the performance of this model in detecting credit card fraud.

1.4 Scope of the Study

This work focuses on predictive model using data mining that scores each transaction with high or low risk of fraud and those with high risk generate alerts. Predictive data mining performs inference on the current data in order to make predictions. The check those alerts and provide a feedback for each alert i.e. true positive (genuine) or false positive (fraud). Furthermore, in view of the broad nature of financial fraud, the study is particularly about credit card fraud using data strictly stored on the core banking database and card issuer's database. The study will narrow down to particular type of financial institutions which are the banks. Since most of the existing credit card frauds are done using a customer's banking information and card information, the study will focus on banking industry and card issuer institutions. This work will cover detection, monitoring and response of fraudulent activities in e-commerce business.

It will also cover the area of real-time alerting system to enable financial companies stop or deactivate any financial transaction suspected to be fraud.

1.5 Significance of the Study

The process of searching for fraud is lengthy due to the amount of data involved. In most cases, auditors unknowingly get the information they need from the involved employees who deliberately mislead them and waste their time. With a multi-agents fraud detection system in place to check unusual transactions, the work load is distributed among the agents, thus a search is faster and block any transaction suspected to be fraudulent. Since different agents communicate and carry out the verifications otherwise done manually, they detect a fraud on the fly, before a transaction fraud is concluded. Without an effective system to check against internal attacks, management of these financial institutions rely on auditors, both internal and external to investigate the fraud, if they suspect that one has taken place. The problem is that some fraud can go undetected or by the time they figure out that fraud has occurred it is either too late and the fraudsters have disappeared or they have had enough time to cover their tracks and the trail goes cold.

1.6 Limitation of the Study

Unfortunately most banks prefer not to go public and report the incidences as they fear losing business if the fraud cases are known to the public. Owing to this fact, it is difficult to get direct reports from the financial institutions, so it is difficult to come up with a clear indication of how rampant the problem is. However, reports from Central Bank of Nigeria (CBN), newspaper articles and a few publications on the issue show that the problem exists and is actually growing steadily.

1.7 Definition of Terms

Agent: Computer software that is capable of autonomous action in some environment in order to meet the designed objectives.

ATM: is an abbreviation for Automated Teller Machine. It is a cash point that can be used to withdraw cash, do transfers. A debit card or credit card is used at the machine to withdraw cash. The personal identification number (PIN) has to be entered along with credit or debit card to access cash.

Bank Account: It is record of financial transaction between a bank and the customer which is maintained by the bank. A bank account also shows the resultant financial position of the customer with the bank.

Bank Fraud: The use of potentially illegal means to obtain money, assets or other property owned or held by a financial institution or obtaining money from depositors by fraudulently posing at a bank or other financial institution.

Card Association: Is a network of issuing banks and acquiring banks that process payment cards of a specific brand.

Cardholder: Is a person who owns the credit card issued by appropriate credit card company or financial institution.

Commercial Banks: Financial institutions that provide services such as accepting deposits, giving business loans and auto loans, mortgage lending and basic investment products like savings accounts and certificates of deposits (Koru, 2014). The traditional commercial bank is a brick and mortar institution with tellers, safe deposit boxes, vaults and ATMS. However, some commercial banks do not have any physical branches and require customers to complete all transactions by phone or internet.

Credit card fraud detection: This is a process of classifying credit card transactions into two classes of legitimate (genuine) and fraudulent transactions.

Data Mining: This is a well-defined procedure that takes data as input and produces output in the forms of models or patterns.

Financial Institution: This is an institution that provides financial services for its clients or members (Wikipedia, 2016). Probably the most important financial service provided by financial institutions is acting as financial intermediaries.

Financial Sector: This is a category of stocks containing firms that provide financial services to commercial and retail customers. It includes banks, investment funds (Koru, 2014).

Fraudulent Card Transaction: is one in which the rules and regulations are not properly followed. Generally, such transactions are unauthorized by credit card holders and involve a lost stolen, fabricated, counterfeit and fraudulent processing of a credit card.

Multi-agents: Is a system that is capable of flexible autonomous actions in order to meet its design objectives. It is flexible in terms of its reactivity, proactiveness and social ability.

Knowledge: This can be defined as the body of facts and principles accumulated by human kind or the act, fact or state of knowing.

Machine Learning are computer programs that can learn from experience with respect to some class of tasks and performance measure.

CHAPTER TWO
LITERATURE REVIEW

2.1 Definition of Fraud

It is worthy of note that not much work has been written on credit card frauds detection using multi-agents. Fraud is an increasing phenomenon as shown in many surveys carried out by leading international consulting companies (NIBSS, 2018). Despite the evolution of electronic payments and hacking techniques there is still a strong human component in fraud schemes. Conflict of interest in particular is the main contributing factor to the success of internal fraud. In such cases, anomaly detection tools are not always the best instruments, since the fraud schemes are based on faking documents in a context dominated by lack of controls, and the perpetrators are those ones who should control possible irregularities. In the banking sector, audit team experts can count only on their experience, whistle blowing and the reports sent by their inspectors. Fraud is generally defined in law as an intentional misrepresentation of an existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage (US Legal, 2016). Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading.

Fraud is a crime of deceiving somebody in order to get money or goods illegally. Egu (2008) described fraud as a conscious premeditated action of a person or group of persons with the intention of altering the truth or facts for selfish personal monetary gain. Egu (2008) said that this involves the use of deceit and trick and sometimes, high intelligent cunning and know-how. This action usually takes the form of forgery, falsification of document and authorizing an outstanding theft.

Ojigbede (2000) agreed that fraud is an action which involves the use of deceit and trick to alter the truth so as to deprive a person of something. The International Auditing Guidelines refer to frauds as irregularities involving the use of deceits to obtain an illegal or unjust advantage. A person, who pretends to be something that the person is not, is a fraud, a snare, a deceptive, trick, cheat and a swindler (Jenta, 2002). By extension fraud will include embezzlement, theft or any attempt to steal or unlawfully obtain, misuse or harm the assets of a bank (Bank Administration Institute 1989). Other definitions of fraud between organizations and jurisdictions include: Willful perversion of the truth made with the intent to deceive and resulting in actual or potential prejudice to another inducing a course of action by deceit or

other dishonest conduct, involving acts or omissions or the making of false statements, orally or in writing, with the object of obtaining money or other benefit from, or of evading a liability to the Commonwealth. Fraud is the crime of falsification and with fraudulent intent of making or altering writing documents or other instruments.

Fraud is a deliberate misrepresentation which causes another person to suffer damages, usually monetary losses. Most people consider the act of lying to be fraudulent, but in a legal sense, lying is only small element of fraud. From the forgoing, it is evident that fraud has to do with the employment of distorted facts to gain access to what belongs to another. Fraud perpetrated by members of bank staff with or without the assistance of persons not employed by the bank is referred to as internal fraud. Fraud perpetrated by non-employees, with or without the assistance of bank staff is called external fraud. In internal fraud, a fraudulent person therefore is someone who uses tricks or deceit to acquire property or secure benefits to the detriment of his employer (the bank). Many bank employees who engage in fraud find any means possible to conceal their acts by either destroying the relevant documents or ensuring that they remain in the same position for several years.

2.1.1 Forms of Fraud

There are several types of bank frauds, as there are several different sizes of banks. Frauds in banks vary widely in nature, character and method of perpetration. The list of fraud is in exhaustive as new methods are devised over time. However, most types of bank fraud include the following (Ojo, 2008).

a. **Mail Fraud:** this is a process whereby the content of a duly authorized mail originated in a bank is converted to the benefit of illegitimate recipient.
b. **Forgery**: this is the act of forging a customer's signature to draw money fraudulently from the customer's account; forgoing other employees' signatures for fraudulent transfer of funds from one account to another or for fraudulent withdrawal of funds from a customer's account. The forgery can be cheques, certificate of investments, will of a dead person and other payment instruments. Experience has shown that most forgeries are caused by inside staff or by outsiders in collusion with the inside staff who have access to the specimen signature being forged.
c. **Defalcation**: This type of bank fraud takes time before it is discovered, because it is neatly perpetrated. It is uncovered by customers during account or cash reconciliation.

d. **Teeming and lading**: this is the suppression of cash or cheque lodgments or withdrawals of customers by the cashier, teller or an officer of a bank. A type of suppression could be hiding third party's cheques drawn on a customer's account when the customer has no sufficient funds to accommodate such drawings. The rectification is done with subsequent lodgment either from the same customer or from another customer. Another type of suppression is a customer's surplus deposit which the receiving cashier deliberately refuses to declare. The objective of the fraudster is to convert the funds which belong to a customer or lodger to his own use.

e. **Cheque kitting and cross firm**. Cheque kitting is the use of illegal or dud cheque to obtain money. It could be the use of dud cheque drawn on one branch of a bank and lodged in another branch of the same bank to obtain unauthorized credit. Due to the immediate credit usually accorded such in house cheques, a quick withdrawal could be made before the funds are credited. Another one is a situation where bank customer issued a cheque from his account with a bank to another bank where he has an account but without sufficient funds in the account with the drawer bank to carry the cheque but hopes to utilize the time required for a cheque to clear to obtain unauthorized credit interest charge time from the bank were people deposited the cheque. Then, the bank manager gives people funds based on the understanding that funds will soon be made available into people account from the drawer bank. The role of the kitter may be to use these uncollected funds for personal use. Cross firing on the other hand is a method used by customers to create fictitious or inflated turnover. It is a process whereby a cheque is drawn on one branch of bank and lodged in another branch of the same bank, just to beef-up turnover. Cheque fielding is also the use of stolen cheque to obtain cash or goods from supplier.

f. **Advanced fee fraud (419):** this may involve an agent approaching a bank or staff of a bank with an offer to access large funds at a very favorable term. The purported or actual source of such funds is not specifically disclosed or identified but mention will be made of oil-rich sheikhs, funds based on South Africa Gold or other influential names. The only way to have access to these funds is through the agent who must receive a fee or commission in advance. As soon as the agent collects the fee, people disappear into thin air and the money is never made available. Any bank, especially the distressed banks and banks that need huge funds to bid for foreign exchange can easily fall victim of this type of fraud.

g. **Payment against unclear effects:** this is the act of giving direct credit to bank customers against an instrument that is yet to crystallize into cash. This type of fraud is common with branch managers and other credit officers. When such instruments which have already been

paid against by the presenting bank at the clearing house are eventually dishonored by the paying bank, and returned unpaid, the customer's account will be debited with the sum already paid and the debt will crystallize.

h. Unauthorized lending: any lending that does not agree with laid down rules and regulations of the bank or does not receive prior approval of line superior is fraudulent, whether the lending is only for a few hours or for a longer period. This type of fraud is common among branch managers and credit officers. In essence, granting of bank facilities without security and verifiable accounting information is also unauthorized lending and its audient.

i. Presentation of Cloned Cheques: Lodgment of falsified cheques for purpose of obtaining value.

j. Abuse of Suspense Accounts: Posting of fraudulent entries into suspense accounts with the aim of concealing information.

k. Dry Posting: Entries not supported by approved vouchers or documents.

l. Impersonation: impersonation by third party to fraudulently obtain cheque book that he/she utilizes in making illegal withdrawals forms another type of fraud.

m. Success in this method largely depends on the ease of obtaining the stolen cheques and the carelessness of the banks in detecting forged documents.

n. Foreign Exchange Operations Fraud: this has been noticed to be a fertile ground for sharp practices. Such practices have been observed to take the following forms: Banks may sell forex at a premium, which is usually more than the percentage markup stipulated by the central bank.

o. Illegal transfer of forex by banks, which is personally utilized by the members of the board and or management team; Bank's funds from forex market (FEM) are usually used by some bank directors for private purposes that are not allowed officially; Sale of repatriated forex in the black market and diversion of exports proceeds etc.

2.1.2 Causes of Fraud

Causes of fraud include the following amongst others (Olaoye et al., 2014):

a. General Lust for Affluence: it is a matter of fact that the Nigerian society in the last twenty years or there-about has become one where most people want to be rich overnight by whatever means and this has been responsible for the increase in the number of bank fraud and other forms of frauds.

b. Recognition Being Accorded Wealthy People Regardless of the Source(s) of their Wealth: the manner in which people recognize wealthy people in our various communities, churches and mosques without considering the source(s) of their wealth has even made the matter worse .Young and talented men and women engage in drug trafficking and in committing frauds because our society does not only condone these social vices but also encourages them by singing songs of praise in their honor, making them chairmen at functions, naming halls in universities, streets and highways after them, and even floating nongovernmental organizations in their names.
c. Our national awards like Commander of the Order of the Niger (CON), Member of the Federal Republic (MFR), Grand Commander of the Republic of the Niger (GCRN), and Member of the Oder of the Niger(MON), just to mention but a few are sometimes wrongly awarded to those who defrauded Nigerian banks.
d. General Belief That the Economy (banks and other financial institutions) Can Sustain Any Amount of Loss: the attack on the nation's treasury and banks by fraudsters is partly due to the belief by many Nigerians that the banking sector is the most profitable sector of the economy and that the nation's wealth is inexhaustible and sometimes they see it as part of the national cake. Anybody with a little knowledge of economics or finance should know that banks are trading on equity which means they are using other peoples' money to make money and depositors' monies are not theirs. They can only sustain themselves by making profit. After all, banking business is all about risk.

2.1.3 Methods of Fraud Perpetration

Fraud perpetrators could be grouped into three major classes (Adeyemo, 2012):

a. Internal fraud: perpetrated by staff
b. Mixed fraud: A collusion of staff and non-staff
c. Fraud perpetrators have been found to use different methods to facilitate their activities.

Some of the identified medium includes:

a. Enlisting support of insiders
b. Recruitment of impostors
c. Supervision or omission of the effects of transaction from records
d. Willful misrepresentation of accounting policies
e. Forgery of financial instruments e.g. Parallel cheques, forged drafts etc.
f. Forgery of signature (Bank officials and customers)

g. Identity theft i.e. Forgery of identification documents such as identity cards, and driver's license.
h. International Passports and other forms of identification
i. Use of Courier companies or dispatch clerks to intercept / substitute clearing cheques in transit.
j. Diversion of phone calls (customer/bank) —swapping of SIM cards.
k. Hacking into bank's information system.

2.1.4. Bank Fraud

Bank fraud is the use of illegal means to obtain money, assets or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. Fraud is a criminal offence (Siklos, 2001).

2.1.4.1 Types of Bank Fraud

As a customer you may be seen as a potential target for fraudulent activities. However, by arming yourself with information and tools you can protect yourself from becoming a victim of fraud.

a. **Cheque Fraud:** Cheques can be altered to an illegitimate payment recipient and higher transaction amount by adding a few digits or may be provided with or cheque can be completely forged. Suspicious properties of hand or machine written cheques can be recognized by special experts (Sonia and Arora, 2015).

b. **Loan Fraud:** Fraudulent loan applications which are the reasons of bank fraud may contain false information to hide financial problems. Also, an employee can knowingly approve loans to accomplices who declare bankruptcy.

c. **Money Laundering:** It is a special kind of bank fraud in which the main aim is to hide true information of origin of funds.

d. **Identity Theft:** In this fraud, the information of an individual is obtained and this information is used to apply for identity cards, accounts and credit in that person's name. The information can be obtained from mail scam, telephone. Identify theft fraud is common on internet.

e. **Payment Card Fraud:** Payment card can be stolen or may be reproduced with skimming. Cards can be intercepted in transit when it is being sent to the user. Cards can also be negotiated by merchant who undertakes duplicate transaction of card.

f. **Electronic Fraud:** Mainly fake websites and scam emails come under electronic fraud. Personal information of customer is taken by the fake email id and fake websites.

2.1.4.2 Causes of Bank Fraud

Causes of fraud can be categorized into two, viz: institutional factors and environmental factors (Nwaze, 2008).

1. **Institutional Factors:** The institutional factors are those that can be traced to internal environment of the organization (Nwaze, 2008). They are to a great extent factors within the control of the management of the bank. A major institutional cause of fraud is poor management. This comes in form of inadequate supervision. A junior staff with fraudulent tendencies that is not adequately supervised could get the impression that the environment is safe for the perpetration of fraud. Poor management would also manifest in ineffective policies and procedures, which a fraudulent minded operator in the system will capitalize on. Even where there are effective policies and procedures in place, fraud could still occur with sometimes deliberate skipping of these tested policies and procedures. Inexperienced operators are susceptible to committing unintentional fraud by falling for numerous tricks of fraudsters. An inexperienced operator is unlikely to notice any fraud attempts and take necessary precautionary measures to checkmate the fraudster or set the detection process in motion. Overstretching is another reflection of poor management. This can aid perpetration of fraud to a large extent. A staff that is overstretched is not likely to perform at optimum level of efficiency. Ordinarily, the longer a man stays on the job, the more proficient he is likely to be. An operator who has spent so long on a particular job may be encouraged to think that no one else can uncover his fraud. The existence of this kind of situation in a bank is clear evidence of poor management and such situations encourage fraudulent practices. Poor salaries and poor conditions of service can also cause and encourage fraud. Employees that are poorly paid are often tempted to fraudulently convert some of the employers' monies to their own use in order to meet their personal and social needs. This temptation is even stronger on bank employees who on daily basis have to deal with cash and near cash instruments. In our society, it is argued that greed rather than poor working conditions or poor salaries is what lures most people into fraudulent acts. This explains why fraud would still exist in the banking sector, which is reputed to be one of the highest paying sectors. Some people have an insatiable appetite to accumulate wealth and would therefore steal irrespective of how good their earnings are. Where a staff feels short-changed in terms of promotion and other financial rewards, he/she becomes

frustrated and such frustration could lead to fraud as such employee would attempt to compensate himself in any way. Among the internal causes of fraud, the Nigerian Deposit Insurance Corporation (NDIC, 2014), states that prevalence of fraud and forgeries are an indication of weakness in bank internal control system.

2. External Factors/Environmental Factor: Environmental factors are those that can be traced to the bank's immediate and remote environment. If the whole society of which the bank is a part is morally bankrupt, it will be difficult, if not impossible to expect the banks to be insulated from the effects of such moral bankruptcy (Nwaze, 2008). The banking industry is not immune from the goings on in its external environment. Little or no premium is put on things like honesty, integrity and good character. The society does not question the source of wealth. Any person who stumbles into wealth is instantly recognized and honored. It is a fact of our time that fraud has its root firmly entrenched in the social setting where wealth is honored without questions. Ours is a materialistic society which to a large extent encourages fraud. With reference to fraud, criminal motivation is said to be pathological when the state of mind of the criminal disposes and impels him/her to commit fraud even though he/she is not in dire need of the resources. Also, worth mentioning is lack of a call-over system in the banks, lack of regular and un-notified rotation of clerks, doing more than one job which is incompatible and so on as major causes of fraud. A call-over system is a system where all bank transactions are verified for accuracy, authorization and reliability. Directly or indirectly, some Nigeria youths especially those with little Information Communication Technology (ICT) knowledge with special reference to those that found them in the banking industry with criminal intent engage in one bank fraud or the other in order to eradicate poverty. Most of them have some of their family members that depend on them for what to eat and drink or even put in their pockets. All these make fraudsters to have the feeling that they are above the law and as such can get away with ill-gotten wealth unpunished.

Other predisposing Factors to Fraud:

a. Global economic recession
b. Nature/quality of workforce
c. Absence of fraud detection mechanism
d. Collusion 'between fraudsters and bank staff.
e. Ignorance of banking ethics by bankers.
f. Poor motivation and low staff morale.
g. Societal acquisitive instinct and insatiable lust for wealth.

h. Inadequate deterrent punishment for fraudsters.

i. External influence on bank staff.

2.1.5 Statistics of Fraud in Nigeria

Over the years, technology has played a vital role in Nigeria's financial sector. From initiating funds transfer right from the comfort of our rooms, to paying utility bills without having to visit the service providers and uniquely identifying bank customers with biometrics etc. Many cutting-edge products and services have been developed which in turn have changed the way we interact and transact. Even the days of long queues in banks are long gone. The ease, transparency and swiftness that technology brought to the financial ecosystem in Nigeria are noteworthy. “The Bad Guys” are constantly finding ways to perpetrate their illicit intentions and take advantage of the system. However, “The Industry” is always deliberating and implementing strategies and policies to counter the acts of these fraudsters. The directive by the Central Bank of Nigeria (CBN) for the establishment of industry fraud desks, sending of all electronic interbank transactions to the Central Anti-Fraud Solution (HEIMDALL), introduction of biometrics to the ecosystem, and most importantly, the general public collaboration, have contributed to reducing fraud menace in Nigeria's financial space. Fig.2.1 shows that 19,531 fraud cases were reported for Deposit Money Banks in 2016 as against 10,743 in the Year 2015. Although, there was 82% increase in reported fraud cases as compared to 2015, one also noticed marginal reduction in attempted fraud value and actual loss at **4,368,437,371.64** and **2,196,509,038.78** respectively. Also, there was a decrease of 2.65% in actual loss due to fraud in 2016 when compared with 2015. Table 2.1 shows the summary of fraud report, the fraud volume in 2016 recorded higher than 2015.

Table 2.1: Summary of Fraud Report (Neff, 2016)

Year	Fraud Volume	Attempted Fraud Value (₦)	Actual Loss value (₦)
2015	10,743	4,374,512,776.64	2,256,312,660.00
2016	19,531	4,368,437,371.64	2,196,509,038.78

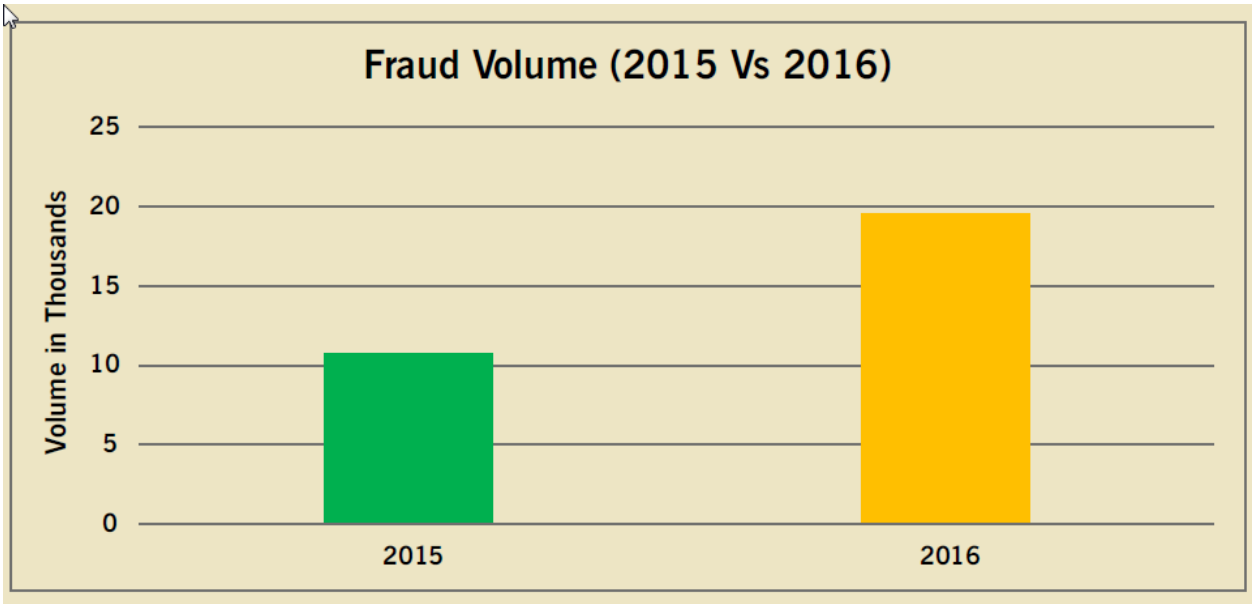


Fig.2.1: Comparing Fraud Volume for the years 2015 and 2016 (Neff, 2016)

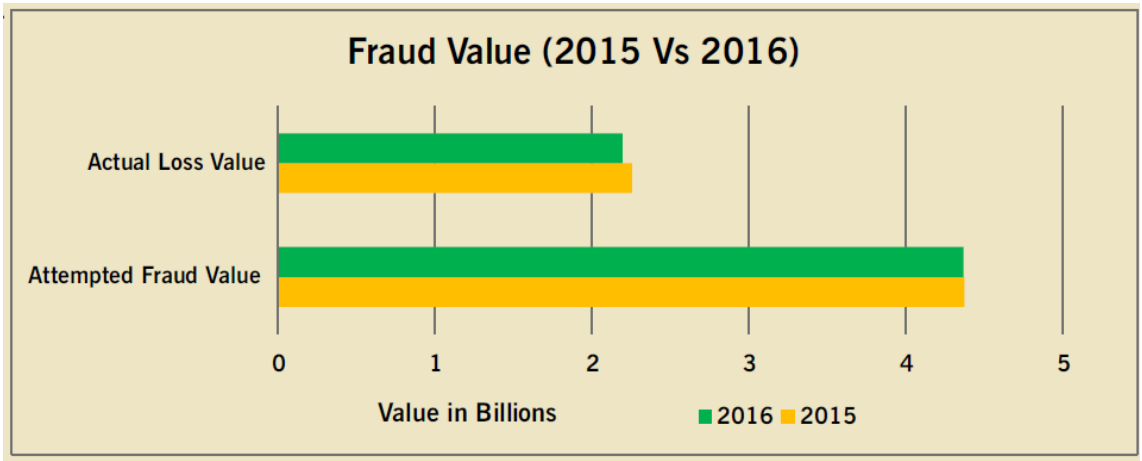


Fig.2.2: Comparing Fraud Value for the years 2015 and 2016 (Neff, 2016)

2.1.5.1 Fraud per Channel

Table 2.2 shows reported fraud events in the year 2016 and categorizing them according to channels, fraud perpetrated through the Automated Teller Machine (ATM) recorded the highest volume of fraud followed by Mobile. This is analogous to several emerging products and services riding on these channels which fraudsters are taking advantage of, especially mobile channel. The third most used channel to perpetrate fraud is Web.

Table 2.2: Fraud per Channels (Neff, 2016)

Channel	Fraud Volume	Actual Loss Value(₦)
Across Counter	325	511,072,861.29
ATM	9,522	464,514684.27
Check	12	4,558,897.75
eCommerce	520	132,252,118.32
Internet Banking	698	320,665,957.87
Kiosk	3	10,198,000.00
Mobile	3,832	235,170,720.40
POS	1,658	243,321,812.67
Web	2,677	83,776,994.11
Others	284	190,976,992.10

It is noteworthy to mention that ATM has been the most used channel for fraudulent transactions for the last two consecutive years. One has also seen the increase in mobile channel fraud hence, the need for the financial institution (banks) to re-evaluate current strategies and policies. Same with 2015, “across counter” channel recorded the highest actual loss value for the year 2016 with approximately ₦511M. Although, it is less than what one observed in 2015 in terms of volume and value. One advises that banks should review their internal processes to curb this, especially with the current status of our economy. ATM and Internet banking occupy the second and third positions respectively – same with 2015. Fig.2.3 depicts fraud according to channels in the year 2016, volume and value.

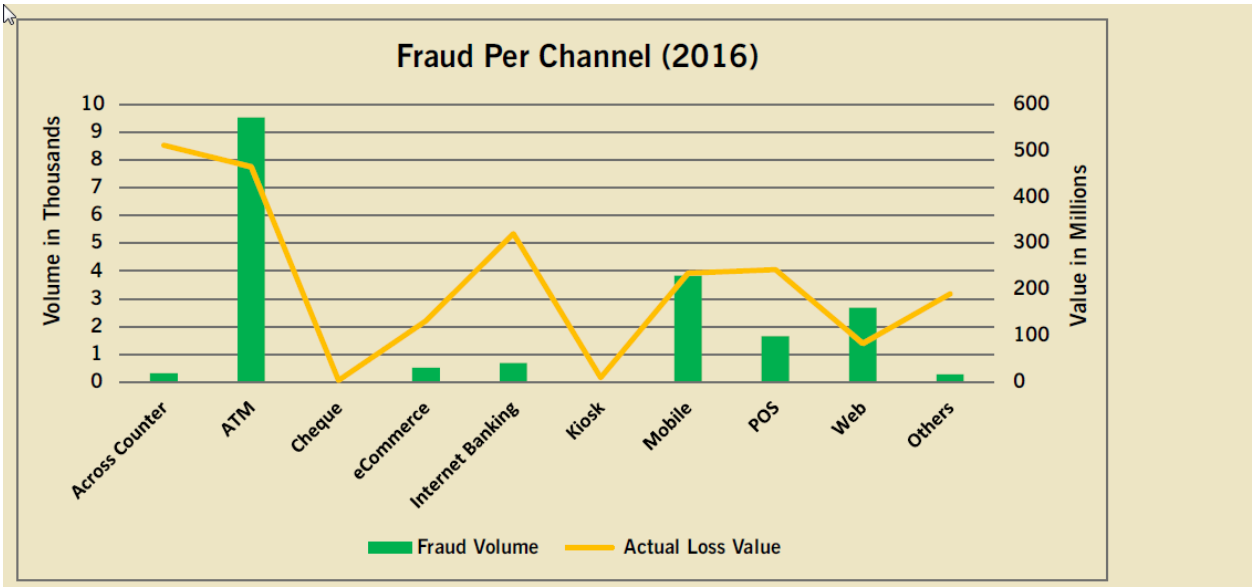


Fig.2.3: Fraud according to channels in the year 2016: volume and value (Neff, 2016)

2.1.5.2 Fraud by Platform

Nigeria Inter Bank Settlement System (NIBSS) categorized various channels stated above into electronic and non- electronic platforms. Tables 2.3 and 2.4 show all payment channels currently captured on the Industry Anti-fraud portal with their corresponding fraud volume and actual loss value for 2016 represented as either electronic or non-electronic platform. Examining the total fraud volume and value on both platforms, it is evident that fraudsters still leverage more on the electronic platform to carry out their illicit acts. Fig.2.4 depicts fraud by platform. Consequently, the Non-electronic platform which comprises of "Cheque and Across the Counter" channels represents about 23% of the total actual loss for the year. This shows a lower percentage when compared with 2015, with non-electronic platform representing 43% of the total actual loss for that year.

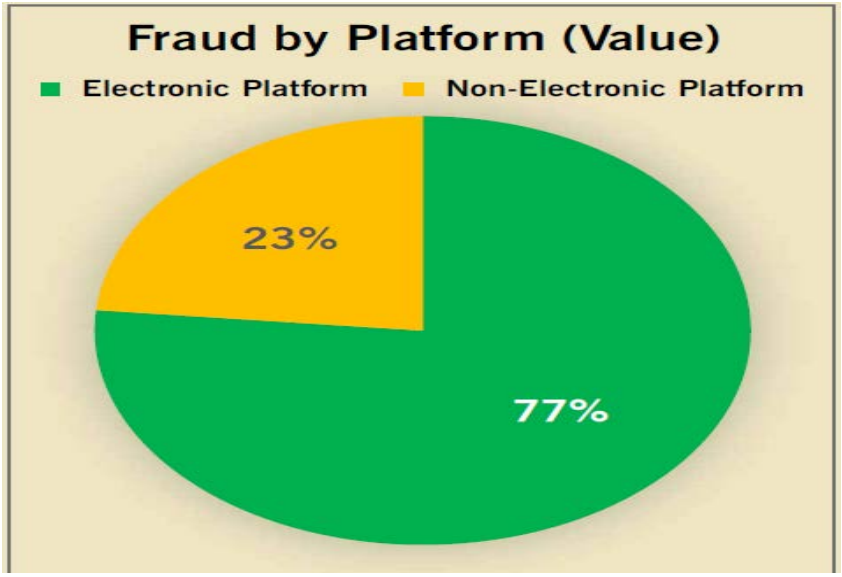


Fig.2.4: Fraud by Platform (Neff, 2016)

Table 2.3: Electronic Channel (Neff, 2016)

ELECTRONIC PLATFORM		
Channel	**Fraud Volume**	**Actual Loss Value(₦)**
ATM	9,522	464,514,684.27
Ecommerce	520	132,252,118.32
Internet Banking	698	320,665,957.87
Kiosk	3	10,198,000.00
Mobile	3,832	235,170,720.40
POS	1,658	243,321,812.67
Web	2,677	83,776,994.11
Others	284	190,976,992.10
TOTAL	**19,194**	**1,680,877,279.74**

Table 2.4: Non-Electronic Channels (Neff, 2016)

NON-ELECTRONIC PLATFORM		
Channel	**Fraud Volume**	**Actual Loss Value(₦)**
Across Counter	325	511,072,861.29
Cheque	12	4,558,897.75
TOTAL	**337**	**515,631,759.04**

2.1.5.3 Fraud per Month

Based on trend and human perception, it is believed that fraud rates increase towards the end of the year due to several festivities observed during this period and the need for people to get more money. But, the truth is, fraud can occur anytime, hence the need for us to always gear up our preventive and detective strategies. Table 2.5 shows the reported fraud cases in 2016, there was a twist when compared with the last two years. Although there was increase in the "ember" period, there was less impact in terms of actual loss value – this will be in detail under "fraud per quarter" segment. This increase is marginal when compared with last year. In 2016, the month of October recorded the highest fraud volume, followed by March and June respectively. The month of June recorded the highest actual loss value, while February and January took the second and third position respectively. Fig.2.5 shows the reported fraud per month both in fraud volume and actual loss value.

Table 2.5: Reported fraud per month (Neff, 2016)

Month	Fraud Volume	Actual Loss Value(₦)
Jan	1,373	227,538,777.49
Feb	961	247,384,495.54
Mar	2,070	188,483,660.93
Apr	1,558	86,164,641.79
May	1,918	104,982,112.35
Jun	1,991	428,160,136.23
Jul	1,448	202,828,418.01
Aug	1,213	157,102,022.47
Sep	1,587	116,094,659.61
Oct	2,128	153,091,198.51
Nov	1,424	138,862,567.58
Dec	1,860	145,816,348.27
TOTAL	**19,531**	**2,196,509,038.78**

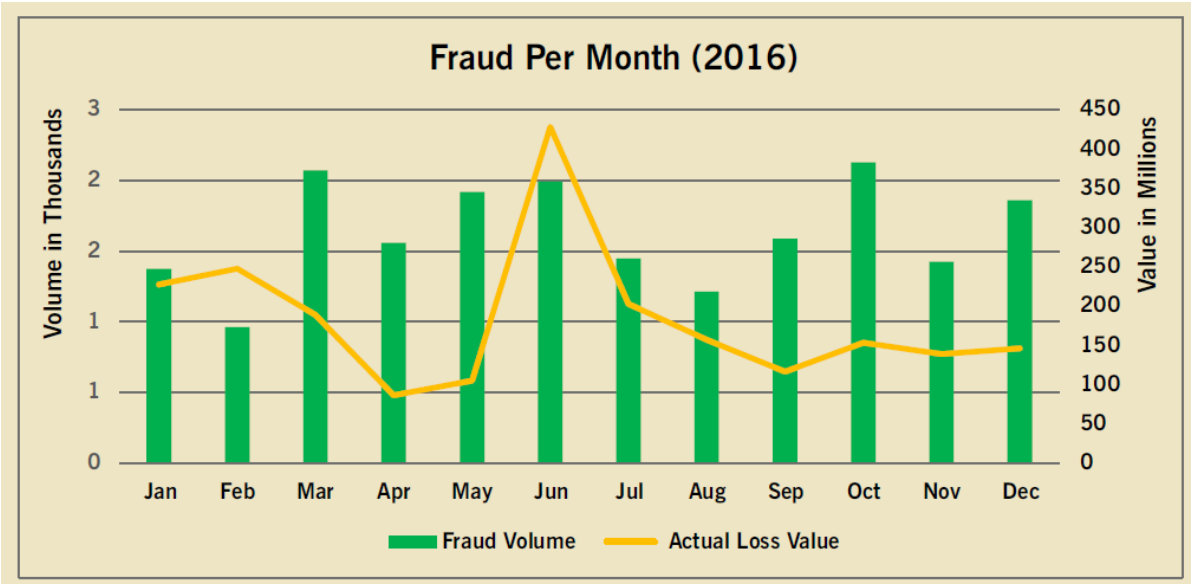


Fig.2.5: Reported fraud per month (Neff, 2016)

2.1.5.4 Fraud per Quarter

Segregating reported fraud cases in the year 2016 into quarters, one experienced constant decrease in the actual loss value. Indeed, this is notable and shows that our co-operation in the fight against fraud is paying off. For the first time in three years, the fourth quarter of 2016 recorded the lowest actual loss and attempted fraud value. In 2015, attempted fraud value consistently increased across each quarter. The same goes for actual loss value with just a marginal drop in the second quarter. Fig.2.6 shows the reported fraud per quarter and the attempted fraud value and actual loss value attached.

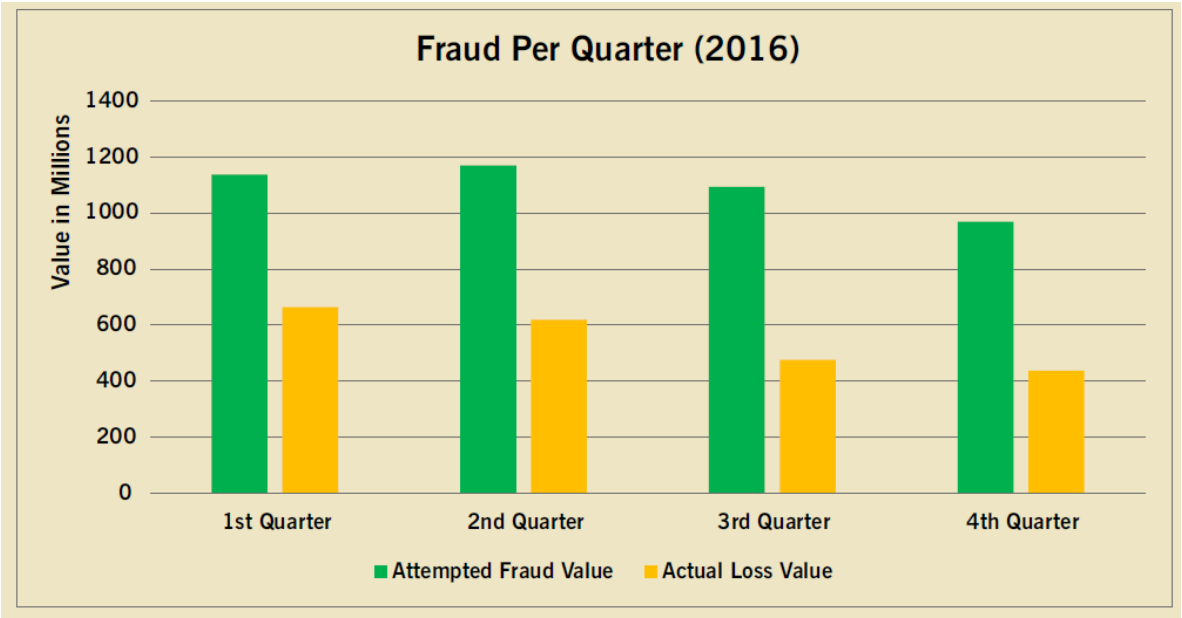


Fig.2.6: Reported Fraud per Quarter (Neff, 2016).

In 2014, fraudulent transactions consummated through ATM, Internet banking and Web Channels were the top three. In 2015, ATM, POS and Web were the top three most used channels to perpetrate fraudulent transactions. However, in 2016, ATM, Mobile and Web were the three most used. Apparently, ATM and Web channels have consistently appeared in top three channels used to perpetrate fraud for three years running. This is something one has to look at collectively as an Industry. Fig. 2.7 shows the fraud volume per channel in the last three years, it can be deduced that ATM channel has been the focal point for fraudsters in the last three years. The emergence of Mobile channel in this category cannot be extraneous to the various financial products and services we have these days, which ride on mobile platforms.

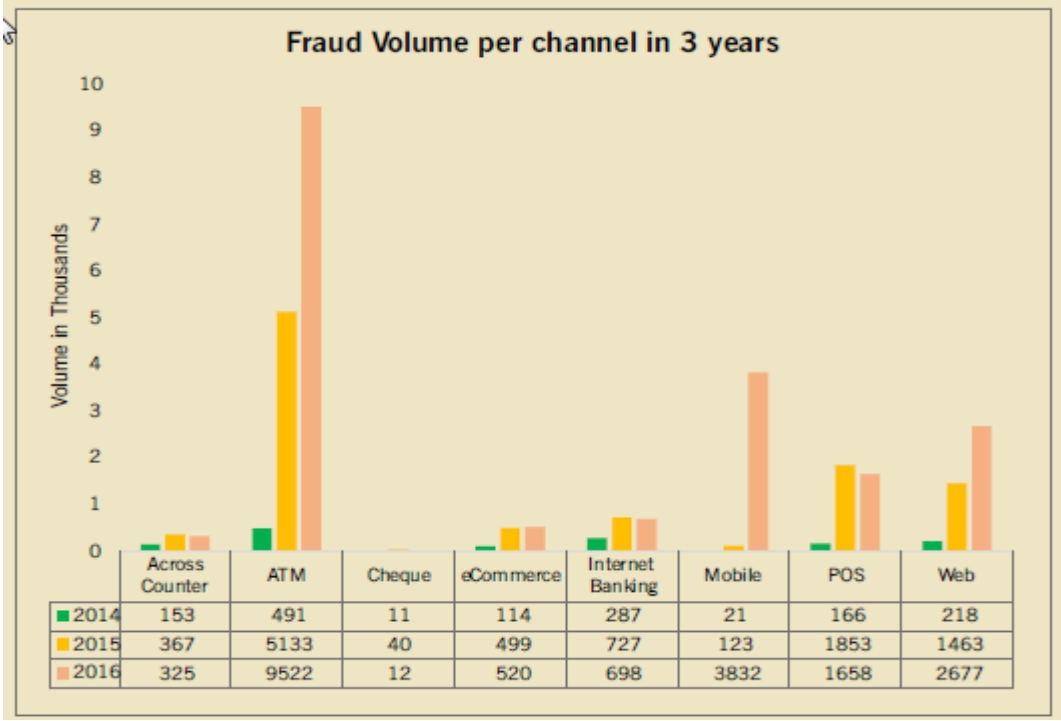


Fig.2.7: Fraud volume per channel in the last 3 years (Neff, 2016).

2.1.5.5 Fraud Rate

Although values of the year 2016 are almost same with those of 2015, the difference in its volume when compared to 2015 suggests more success in curbing fraud. Tables 2.6 and 2.7 show all fraud rate per value and volume in 2016. More attempts in volume can be seen over a period of three years, and the rate is expected to increase significantly if the current recession is not taken into consideration. The current economic recession has, and will always drive persons deeper into fraudulent activities. Also, with the growing adoption of electronic means of payment by individuals and migration to the use of smart phones coupled with the popularity of crypto-currencies in our nation, heightened fraud attempts in volume is almost inevitable. However, though fraud volume in 2016 increased with over 80%, the value in actual loss and attempted was lower than that of 2015. This lends credence to collaborative efforts between the various fraud desks and banks, as well as NIBSS aggregating responsibilities over the various financial institutions. Fig.2.8 shows trend in Nigeria over the last three years which recorded increase with over 80% in 2016.

Table 2.6: Fraud rate per value (Neff, 2016)

Year	Attempted Fraud Value(₦)	Actual Loss(₦)	% Difference
2015	4,374,512,776.64	2,256,312,660.00	**52**
2016	4,368,437,371.64	2,196,509,038.78	**50.2**

Table 2.7: Fraud rate per Volume (Neff, 2016)

Year	Transaction Volume(₦)	Fraud Volume	Fraud Rate (Vol.)	Transaction Value(₦)	Fraud Value(₦)	Fraud Rate (Val.)(₦)
2014	113,421,933	1461	**0.001%**	43,857,678,478,941	7,750,152,748.00	**0.017%**
2015	162,598,740	10,743	**0.006%**	48,932,506,699,512.20	4,374,512,776.64	**0.009%**
2016	278,744,529	19,532	**0.007%**	64,186,537,023,217.30	4,368,437,371.64	**0.007%**

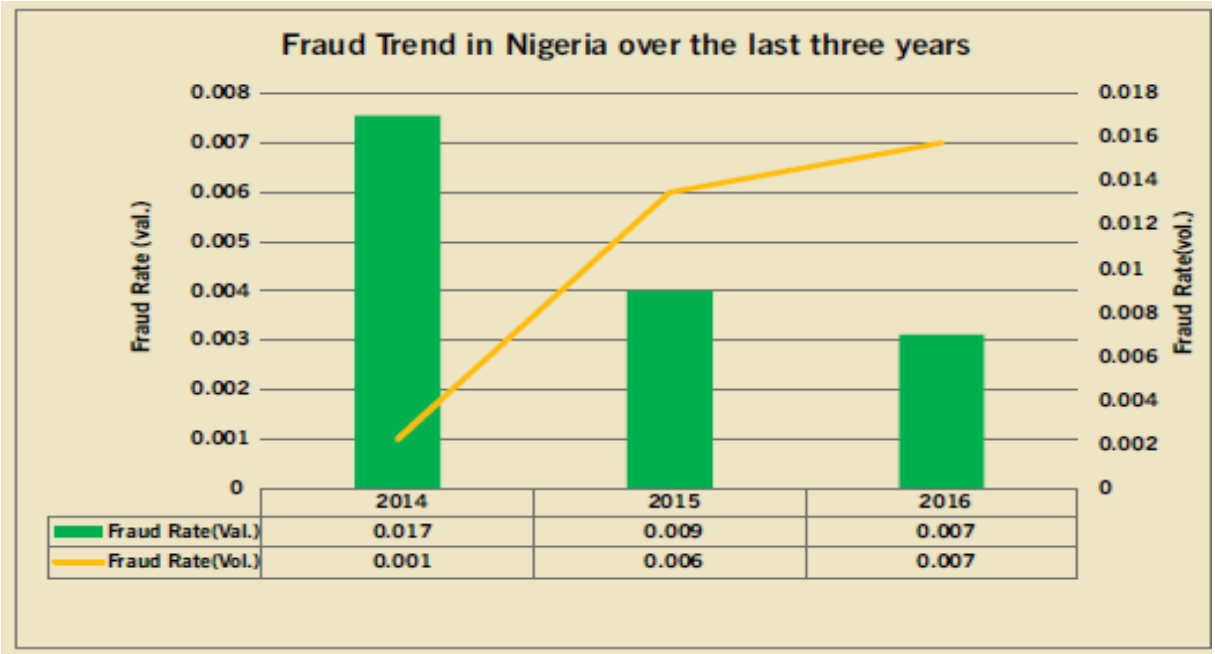


Fig.2.8: Fraud Trend in Nigeria over the last three years. (Neff, 2016)

2.1.5.6 Fraud Control Measures in Banks

Having realized the extent of damage fraud has done to the economy in general and the banks in particular, it is proper to proffer solutions as to how fraud can be controlled. To this effect, the following measures can be used to control fraud (*Olaoye et al., 2014*).

a. Recruitment of competent staff with the right experience and skill. Banks should institute measures that will encourage staff retention and continuous filling of vacancies.
b. Banks should be compelled to establish clear organizational structure and reporting lines. CBN should intervene and enforce changes in Banks with clumsy reporting lines. Furthermore, frequent changes in organizational structure should be discouraged.
c. CBN Examiners should intensify their review of bank systems to identify areas of job compromise with respect to segregation of duties (especially Back Office, Risk Management, Internal Control and Internal Audit functions). Furthermore, guidelines should be issued on the categories of banking positions that should not be held by the same person.
d. Management should either follow up on any significant matters that are brought to their attention, or ensure that instructions issued are carried out. Executive Management should articulate the bank's position on fraud in a formal anti- fraud policy which should be communicated to all staff.
e. Management should understand the business they manage including peculiar business, market and operational risks inherent in foreign jurisdictions and specialized products. Furthermore, training courses for front office staff should be extended to the operation and internal control audit staff.
f. Management should incorporate robust anti-fraud policy as part of their risk management framework. Such policies should include measures to identify both existing and future risk of fraud and implement relevant internal controls for every aspect of business activities.
g. Management should develop intelligence gathering techniques, both from internal and external sources, to alert management to the existence of possible fraud.
h. Policies must be put in place to encourage and protect "whistleblowers" to report any suspicious or irregular activity to an appropriate person within the bank.
i. Top Management, Executive Management and Board Audit committee should ensure that significant weaknesses or suspicions raised are acted upon and resolved quickly. Management should consider engaging independent internal or external specialists to carry out fraud investigation where necessary.

j. Management should ensure that key stakeholders (regulators, police, internal auditors etc.) in fraud investigation and management are informed whenever there is fraud occurrence. This will ensure that serious action is taken on fraudsters in order to deter future occurrence.
k. After a fraud investigation has been concluded, controls should be reviewed and revamped to ensure that internal processes and procedures prevent fraud from occurring. The following can be regarded as the general control policies which will ensure the detection, prevention and control of frauds in banks.

1. **Opening of new accounts:** A branch should make sure that all the banks policies in respect to opening of new accounts are complied with. If a customer is transferring his account from one bank to another, the customer should not be allowed to operate the account until proper report has been obtained from the bank by means of status inquiry particularly when the customer is new to the bank. The manager designates senior officer who should be interested in knowing why the customer has come to his bank from the other bank. Proper reference must be obtained before cheque books are issued to customers and all operating to new accounts should be carefully scrutinized while no withdrawals should be allowed without prior verification of the lodgment. Statement of account must be duly authenticated by a responsible officer. The address must not be ambiguous and their dispatch must be controlled. Details of stopped cheques must be entered in such a way that those who are likely to pay them are well informed. This can be achieved by circulating the "stop notice" to all officials concerned including cashiers, where appropriate. At quarterly intervals, all items in stopped cheques, register or display card must be reviewed against records and stale items detected. The use of counter cheques should be discouraged while banks should avoid honoring of cheques that are taken from the cheque books supplied to the customers. Payment to third party across the counter must be properly checked particularly when the third party is not well known in the bank. Banks should discourage customers from withdrawing large amount in cash where a draft or means of settlement can suffice. The use of photocopy camera to photograph a person drawing large amount should be encouraged. Cashier should be instructed never to pay cash to or receive cash from staff in respect of customers' transaction.
2. **Clearing cheques:** as part of control measures to curb incidence of fraud through the clearing house, the committee of chief inspectors had decided that banks, which accept spurious instrument into customers' accounts would henceforth be held responsible for any loss that may be sustained as a result of their action. It was also decided that when an

account witnesses an unusual large deposit of cheques, the collecting bank should alert the paying bank. Paragraph 10 of Lagos clearing rules of January 1990 clearly addresses this problem. It is therefore absolutely necessary that all clearing cheques should be scrutinized before dispatching with particular attention being paid to large or unusual cheques and indication of cross firing or kite flying. When an unusual item is noticed, the paying bank should be alerted immediately. These cheques must be under double custody at all times from the collecting bank or branch to the time they are handed over to the paying bank in the clearing house.

3. **Unbalanced position of accounts:** experience has shown that unbalanced accounts provide fertile grounds for frauds, hence, at times accounts are not balanced. The situation should therefore be made to balance the accounts regularly and promptly. Items in cut- off-balance account logged should be under the watchful eyes of the branch manager or head of operation entries in and out of the accounts must be duly authorized.
4. **Vouchers:** all processed vouchers must be cancelled and given adequate fire resisting or double custody. Special attention should be paid to suspense account vouchers, profit and loss vouchers, paid drafts and fixed deposit receipts. Microfilm should be used as applicable. Control of cost-purchase should be made within approved limits while prices being paid are reasonable.
5. **Control over computer:** access to the computer rooms must be restricted to authorized persons while movement must be maintained.

a. **All required reports must be produced as indicated on the daily report checklist.** The last report must be kept under surveillance by a senior officer.
b. **Recruitment and training of staff:** bank management must evolve a sound employment policy to ensure that the right caliber of staff and employee are into the banking industry. It is also necessary that very good references on staff be obtained from both their last school and other responsible citizens whose reputation are not in doubt. Staff must be properly trained on their various assigned duties to enable them appreciate their responsibility in detects and preventing frauds. Banks should avoid using new clerks as either cashier or reference clerks.

2.1.6 Fraud Detection Framework

The process of detecting fraudulent behavior covers the whole methodological cycle. The outputs of detection are reports containing the list of suspicious subjects and cases that need to be further investigated. Based on results of ongoing investigation, the optimization and prevention steps are designed. The decision-making process is then objective and systematic. Decision rules for fraud detection are implemented in fraud detection tools and in case these rules are not met, unusual behavior is detected and warning message is sent to the user. Basic prerequisite of optimization project is the performance management system that is able to point out weaknesses and propose prevention steps. The solution also contains predefined Key Performance Indicators (KPIs) that are used to measure overall performance of the process. It continuously increases efficiency of the whole process and monitors the implementation of prevention steps and also monitors the current amount of money spent on the process (Katerina, 2014).Fraud detection systems must not only contend with the creativity of fraudsters, but should also be acutely aware of when day-to-day processes have changed due to recent innovations or technological advancements in the domain (Leung and Waisze, 2010). Existing fraud detection methodologies may therefore need to be updated frequently in order to remain sufficiently informed of current developments. An agent-based fraud detection system can be developed where a number of multi-agents systems are each incorporated to add a particular aspect of the criminal justice process in investigating incidences of potential crime. By having agents emulate the various tasks that are involved in dealing with a crime, it is anticipated that the resulting fraud detection system will be able to achieve similar successes from applying the same procedure in order to successfully develop the fraud detection model. One method for detecting fraud is to check for suspicious changes in user behavior through automatic design of user profiling methods for the purpose of fraud detection, using a series of data mining techniques. Specifically, using a rule-learning program to uncover indicators of fraudulent behavior from a large database of customer transactions. Then the indicators are used to create a set of monitors, which prefer legitimate customer behavior and indicate anomalies. Finally, the outputs of the monitors are used as features in a system that learns to combine evidence to generate high-confidence alarms. Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities (Fawcett and Provost, 1997).

2.1.6.1 Impact of Fraud Detection

It is interesting to note that credit card fraud affects card owners the least because their liability is limited to the transactions made. The existing legislations and cardholder protection policies as well as insurance schemes in most countries protect the interests of the cardholders (Khyati and Bhawna, 2012). However, the most affected are the merchants, who, in most situations, do not have any evidence (e.g. digital signature) to dispute the cardholders' claim of misused card information. Merchants end up bearing all the losses due to chargeback, shipping cost of goods, card issuer fees and charges as well as their own administrative costs. Excessive fraudulent cases involving the same merchant can drive away customers, cause card issuer banks to withdraw service and also result in loss of reputation and goodwill. Card issuing banks have to bear the administrative cost of investigations into fraud cases as well as infrastructure costs of setting up the required software and hardware facilities to combat fraud. They also incur indirect costs through transaction delays. Studies show that the average time lag between the fraudulent transaction date and chargeback notification can be as high as 72 days, thereby giving fraudsters sufficient time to cause severe damage (Pozzolo, 2015).

2.1.6.2 Fraud Detection and Prevention

The negative impacts of fraud make it very clear and necessary to put in place an effective and economical fraud detection system. Recent technological advancements to combat fraud have contributed a number of solutions in this area. Fraud detection techniques involving sophisticated screening of transactions to tracking customer behavior and spending patterns are now being developed and employed by both merchants as well as card issuing banks. Some of the recently employed techniques include transaction screening through Address Verification Systems (AVS), Card Verification Method (CVM), Personal Identification Number (PIN) and Biometrics. AVS involves verification of address with zip code of the customer while CVM and PIN involve checking of numeric code that is keyed in by the customer. Biometrics might involve signature or fingerprint verification. Rule-based methods and maintaining of positive and negative lists of customers and geographical regions are also used in practice. Data mining and credit scoring methods focus on statistical analyses and deciphering of customer behavior and spending patterns to detect frauds (Huang *et al.,* 2007). Neural networks are capable of deriving patterns out of databases containing historical transactions of customers. These neural networks can be 'trained' and are 'adaptive' to the emerging new forms of frauds. Deployment of sophisticated techniques and screening of every transaction alone will not reduce losses. It is necessary to employ an effective and economical solution to combat fraud. Such a solution

should not only detect fraud cases efficiently but also turn out to be cost-effective. The idea is to strike a balance between the cost involved in transaction screening and review and the losses due to fraudulent cases. Analyses show that review of only 2.0% of transactions can result in reducing fraud losses accounting to 1.0% of total value of transactions. While a review of as high as 30% of transactions can reduce the fraud loses drastically to 0.06%, but that increases review costs exorbitantly.

The key to minimize total costs is to categorize transactions and review only the potentially fraudulent cases. This should involve deployment of a step-by-step screening, filtering and review mechanism. A typical deployment can involve initial authentication of transactions through PIN, expiry date on card, AVS and CVM. A second level of screening can involve comparing with positive and negative lists as well as rules based on customers, geographical regions, IP addresses and policies. Risk and credit scoring with pattern and behavior analyses can come next, followed by manual review. This classifies and filters out transactions as genuine or fraudulent in every step and as a result only a few transactions would require further manual review. Such a solution reduces the overall processing delay as well as total costs involved in manpower and administration.

2.1.7 Credit Fraud

Credit fraud is a term used to refer to the family of frauds which are perpetrated in credit industry. Credit card is a method of selling goods or services without the buyer having cash in hand (Delamaire *et al.,* 2009). A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer's bank – also known as issuing bank – which provides the credit services to the consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to the consumer by charging consumer's credit card. This charge is achieved through the merchant's bank – the forth entity – which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card's limit before authorizing that transaction. If the transaction is valid the issuing bank will block the requested amount from consumer's credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant's bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods. The

blocked amount on consumer's credit card account will be transferred into merchant's bank account in the following data. Fig.2.9 shows the front view of the credit card. The main components of the front view of the credit card are described:

Fig.2.9:Parts of a Credit Card (Front) (Delamaire *et al.*, 2009).

1. **Hologram**: This is a 3D image, usually in gold, that verifies a real card from a counterfeit.
2. **Issuing Bank**: This is the bank that sponsors the card. If there is no issuing bank, this part will have the card name or a blank spot.
3. **Card Number**: This is a 16-19 digit number that represents the line of credit on the card. Every card number is unique, and it acts as the ID for the credit card.
4. **Issue Date**: This is the date that the card was created. Not all credit cards have this.
5. **Expiration Date**: This is the date that the card will no longer be valid. You must get a new card before this day, or you will not access your account until a new card comes in.
6. **Card Brand:** This is similar to the issuing bank, but it represents the credit card company that manages the card. Examples include Visa, MasterCard, Discover, and American Express.
7. **Cardholder**: This is the full name of the person or business that owns the card. If the card is for a specific person in a business, it may include both the first and last name of the person and the business name.

Fig. 2.10 shows the back view of the credit card. The main components of back view of credit card are described:

Fig.2.10: Parts of a Credit card (Back) (Delamaire *et al.*, 2009)

1. **Help Line**: The customer service number for the card brand or the issuing bank, depending on the card.
2. **Magnetic Strip**: This is a strip of information that a card machine reads to identify one card from another.
3. **Signature Box:** This is the area you are supposed to sign so no one else can use your credit card.
4. **Verification:** This is a code that further identifies a credit card. It contains the last four digits of the card number, followed by three or four numbers. Those numbers make up the card verification value (CVV), which is also known as the CID for American Express, the CVV2 for Visa, and the CVC2 for MasterCard. You will probably only need this when you're making payments by phone or online.
5. **Card Number:** This is the reverse of the 16-19 digit number form the front of the card. Sometimes this is faded, but you will still be able to see the indentions for the numbers.
6. **Disclaimer**: This is a note from the issuing bank or credit card Company ensuring that you know the agreement associated with the card.
7. **Bank Address:** This is the address someone should release the card to in the event that you lose it. It also acts as an address you can send mail inquiries to. Some banks will add an email address or website to this line for further contact information.

2.1.7.1 How and Where Does Credit Card Fraud Begin

In order to understand the severity of credit card fraud, let one briefly look into the mechanisms adopted by fraudsters to commit fraud. Credit card fraud involves illegal use of card or card information without the knowledge of the owner and hence is an act of criminal deception. Fraudsters usually get hold of card information in a variety of ways: Intercepting of mails containing newly issued cards, copying and replicating of card information through skimmers or gathering sensitive information through phishing (cloned websites) or from unethical employees of credit card companies. Phishing involves the acquisition of sensitive information like card numbers and passwords by masquerading as a trustworthy person or business in an electronic communication such as e-mail. Fraudsters may also resort to generation of credit card numbers using Bank Identification Numbers (BIN) of banks (Pozzolo, 2015). A recent scheme of Triangulation takes fraud fighters many days to realize and investigate. In this method, the fraudster operates through an authentic-looking website, where one advertises and sells goods at highly discounted prices. The unaware buyer submits his card information and buys goods. The fraudster then places an order with a genuine merchant using the stolen card information. One then uses the stolen card to purchase other goods or route funds into intractable accounts. It's only after several days that the merchant and card owners realize about the fraud. This type of fraud causes initial confusion that provides camouflage for the fraudster to carry out their operations.

2.1.7.2 Credit Card Fraud

Although the use of credit cards as a payment method can be really convenient for our daily transactions; people must be aware of the risks that they impose on themselves while using their credit cards. More precisely, the incremental usage of credit cards gave the opportunity to fraudsters to exploit their vulnerabilities (Linda *et al.*, 2009). Credit card fraud refers to any illegal and unauthorized activity on the use of credit cards which is undertaken by a fraudster. According to Hand (2010), credit card fraud increased between 2005 and 2007. Moreover, Bolton *et al.* (2002) claim that in United Kingdom the total losses of credit card fraud for 2000 were £286 million (Quah and Sirganesh, 2008). In United States, the total losses for 2009 were as high as $3.56 billion; an increase of 10.2% comparing to the previous year. An interesting question arises as to who is responsible to pay for all those losses in case of a credit card fraud. Delamaire *et al.* (2009) claim that merchants are really vulnerable in case of a credit card fraud because they are required to pay for the losses due to the so-called charge-backs. Charge-backs

are requested by the consumer's bank as soon as the consumer reports a transaction as unauthorized.

Quah and Sirgnaesh (2008) concur with the above statement adding that merchants not only have to pay for the amount of the illegitimate transactions but also for any additional charges that are imposed by the credit card issuer. Yet banks are required to pay the costs of investigating whether a transaction, which is reported as illegitimate by the consumer, is indeed illegitimate as well as the costs of having the appropriate equipment's for detecting fraudulent transactions (Quah and Sirgnaesh, 2008). Although consumers are the least vulnerable in case of a credit card fraud there are states which enforce consumers to pay for the losses under particular circumstances. This happens in Nigeria in case the consumers do not realize that their credit cards have physically been stolen and fail to report the loss to their banks (Quah and Sirgnaesh, 2008). In particular, the consumers are not forced to pay the losses of an illegitimate credit card transaction if they report the physical loss of card in time or if the card is not physically lost at all. In the first case there shall be no illegitimate transaction at all since the credit card will be locked before the fraudster manages to use it. In the second case where only the details of the credit card are stolen and not the physical card itself; the illegitimate transaction can be undertaken in places where the physical card is not required to be present like phone or internet. With today's technological advances, that last type of fraud is very difficult to prevent and therefore the consumer is no longer responsible for any losses that may occur. Therefore those losses burden merchants and issuing banks. This is the most common fraud type that occurs in credit industry. A fraudster uses a legitimate card to undertake illegitimate transactions. The cardholder is not aware of the fact that their card is being used without their permission. The fraudster takes advantage of cardholder's ignorance by undertaking as much transactions as possible before the cardholder realizes and reports the fraud to their bank (Aleskerov *et al.*, 1997). A credit card fraud can be committed either offline or online (Laleh and Azgomi, 2009). These two ways are discussed below.

2.1.7.3 Offline Credit Card Fraud

Offline fraud occurs when a fraudster steals the physical card and uses it at the actual stores (Laleh and Azgomi, 2009). Although offline fraud is still popular nowadays; it is less common because there is a higher probability to fail. More precisely, the cardholders tend to realize the loss of the physical card and report that to their bank before the fraudster manages to undertake any illegitimate transactions with it. As soon as the stolen card is reported to the bank, the latter will lock the card so as it cannot be used anymore. It is particularly useful to note that if the

cardholder does not realize the loss of their card, a significant financial loss can occur. As mentioned in the introduction chapter, the policies of some banks enforce cardholders to pay for the losses which occur due to an unreported credit card theft. Remarkably, most of the UK banks tend to send the newly created cards via the post office. This is extremely dangerous because the cards may be stolen while they are on the way to cardholder's destination address.

2.1.7.4 Online Credit Card Fraud

During online fraud only the details of the card are stolen and not the card itself. This is also known as virtual card theft. The details of the card can be used in places where the card need not be physically present like internet or phone purchases (Laleh and Azgomi, 2009). This type of credit card fraud is very dangerous and more difficult to prevent because fraudsters can hold credit card's information for a long period of time before they use it (Aleskerov *et al.*, 1997). There is no way for the cardholder to know in advance that their credit card information is stolen. Therefore this type of fraud may only be detected after one or more illegitimate transactions have taken place. There are various ways that fraudsters adapt in order to steal the information of credit cards. Some of these ways are briefly discussed below:

Skimming

Skimming is a process where the actual data on a card's magnetic stripe is electronically copied onto another (Patidar and Sharma, 2011). Fraudsters use special-purpose devices – also known as skimmers – to capture the information of credit cards that are encapsulated inside their magnetic stripes (Xiong *et al.,* 2013). They can use the stolen card information to create counterfeit physical cards in order to use them at actual shops or simply supply the card information at online shops (Xiong *et al.*, 2013). Skimming can be committed by an unfaithful employee, who may swipe customer's card using the skimmer device while the customer is at the point of sale. In the past, skimmer devices have also been introduced on ATM cash machines. In addition to that, micro-cameras have been used to record the PIN code of a cardholder during ATM transactions.

Site Cloning

Fraudsters clone a legitimate website to deceive customers into placing an order with them. Since the fraudulent website seems identical to the legitimate one, the unsuspecting customers provide their credit card information to complete their order. Consequently, fraudsters who obtained the customer's credit card information can commit credit card fraud whenever they wish to (Patidar and Sharma, 2011).

False Merchant Sites

There are various websites that request credit card information in order to confirm customer's age. These websites will never charge the credit cards directly but they may sell their information to fraudsters who will commit credit card fraud (Patidar, 2011).

Credit Card Generators

These are automated programs which make use of banks' algorithms to generate credit card numbers (Patidar and Sharma, 2011). Fraudsters can generate an arbitrary sequence of candidate numbers and then use other techniques – like trial and error – to figure out which numbers correspond to real credit card accounts. These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. Fig.2.11 shows the international net-based for credit card generators. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. This makes the user to allow to illegally generating as many numbers as the user desires, in the form of any of the credit card formats (Bhatla, 2013).

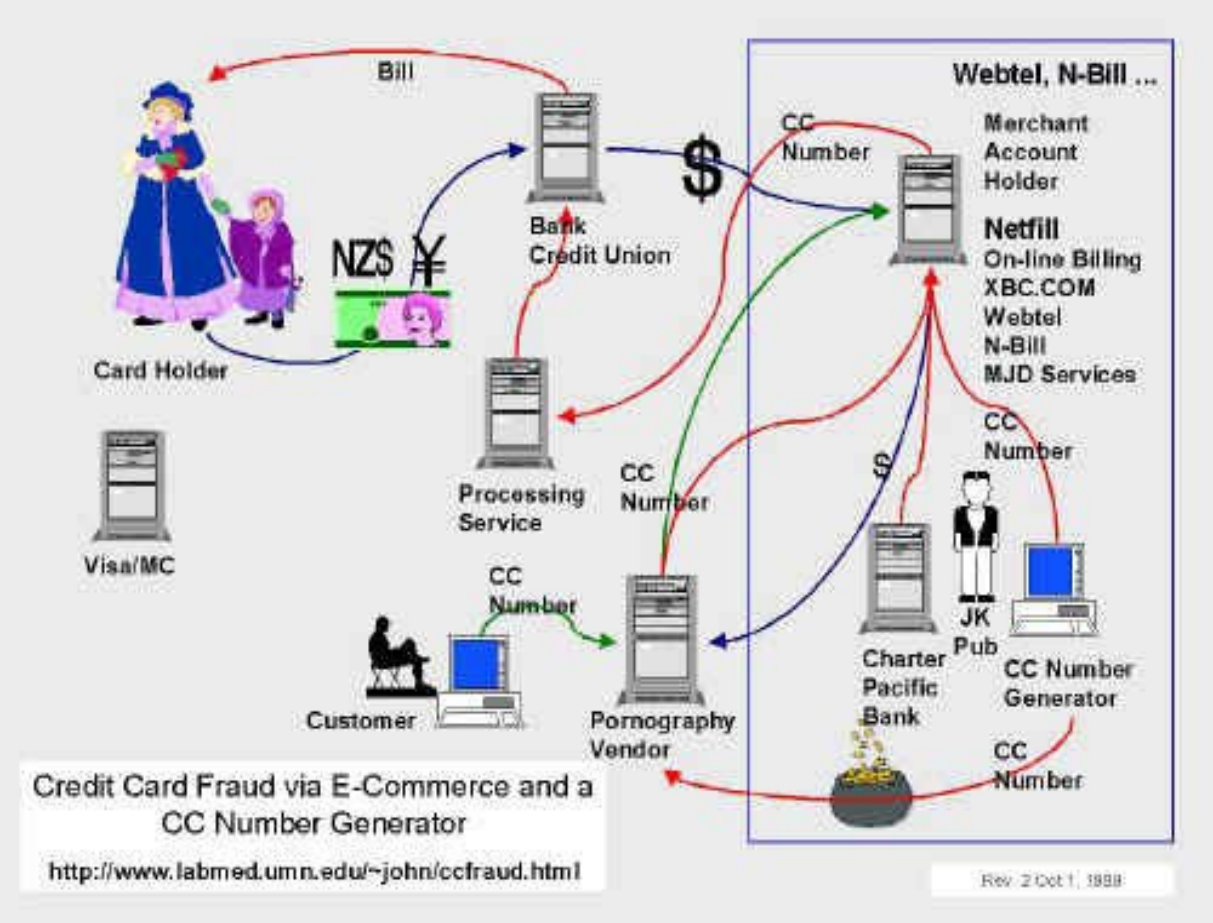


Fig.2.11: International Net-Based Credit Card (Faughman, 2014)

Authentication

There are three basic methods for determining whether a credit card will pay for what it is charging: (http://money.howstuffworks.com/credit-card4.htm)

a. Merchants with few transactions each month do voice authentication using a touch-tone phone.
b. Electronic data capture (EDC) magnetic stripe-card swipe terminals are becoming more common. Before checking out all should have to swipe their card in the terminal.
c. Virtual terminals on the Internet.

After the customer or the cashier swipes the credit card through a reader, the EDC software at the point-of-sale (POS) terminal dials a stored telephone number (using a modem) to call an acquirer. An acquirer is an organization that collects credit authentication requests from merchants and provides the merchants with a payment guarantee. When the acquirer company gets the credit-card authentication request, it checks the transaction for validity and the record on the magnetic stripe for:

a. Merchant ID
b. Valid card number
c. Expiration date
d. Credit-card limit
e. Card usage

In this system, the cardholder enters a personal identification number (PIN) using a keypad. The PIN is not on the card. That is encrypted in the cards database. (For example when one gets cash from an ATM, that machine encrypts the PIN and sends it to the database to see if there is a match.) The PIN can be either in the bank's computers in an encrypted form or encrypted on the card itself. This type of cryptography where the transformation is used is called one-way. This means that it's easy to compute a cipher given the bank's key and the customer's PIN, but not computationally feasible to obtain the plain-text PIN from the cipher, even if the key is known. This was designed to protect the cardholder from being impersonated by someone who has access to the bank's computer files.

Phishing

Refers to the spam emails that are sent by fraudsters in order to deceive their victims and obtain their personal information (Patidar and Sharma, 2011). Fraudsters can impersonate a service provider or institute that victims collaborate with. In their email, fraudsters can make use of a convincing excuse to ask for victim’s personal information including credit card details. The spam emails may also include links to fraudulent websites which again can deceive victims into revealing their personal information. Taking into account the enormous amount of spam emails that we receive at a daily basis, anyone can conclude that this type of fraud is still popular nowadays; although it has been out for many years.

2.1.8 Convenient Method of Payment

A credit card is a special product with the following characteristics (Soheila, 2013):

(1) It provides millions of people around the world with the opportunity to purchase goods and services with access to credit for up to 51 days, depending on the posted date of the purchase at no cost ,provided that the amount owing is paid back by the statement due date.

(2) Cardholders do not have to put up collateral against the amount they spend, therefore, it is unsecured.

In Nigeria, credit cards are widely used in purchasing goods and services.

The main reasons for this popularity are:

1. The existence of a widespread Point of Sale (POS) network.
2. Reducing the risk of carrying cash and the advantage of several weeks of free credit plus optional services and benefits such as Air Miles, free insurance plans, and a number of other rewards
3. Security of funds that is, in case of card loss or theft, the cardholder's liability at the most is 50 provided the cardholder reports a lost or stolen card in a timely manner.

The credit card system facilitates commercial transactions and provides profits for the Participating parties. The source of income for card issuers (CI) may come from: (1) merchant user fees, (2) cardholder user fees, and (3) interest charged on unpaid balances.

In purchasing goods and services the buyer pays for a purchase by using a line of credit from the credit card issuer (CI). The CI pays the seller for the purchase, and the buyer then pays the balance on the credit card back to the CI. Since the claim presented in payment is considered a liability of the credit card issuer, this type of transaction transfers much of the risk of insufficient funds in the transaction from the seller to the credit card issuer. In order to make up for these losses, CIs determine annual fees and interest rates based on the unrecoverable amount of money incurred by these losses. It is worthwhile to point out that most of the CIs are financial institutions (FIs) even though there are many which are not.

2.1.9 Credit Cards Transaction Process

The following information on the credit card transaction processes was collected through personal meetings with the staff of the financial institution and review of journals on this subject (Soheila, 2013).

2.1.9.1 Parties involved in a Transaction

Four parties are involved in processing a credit card transaction*:*

(1) the cardholder,

(2) the merchant,

(3) the Financial Institution (FI), and

(4) the VISA center.

1. The cardholder uses the card for a purchase and provided that the statement amount is paid back by the due date, interest charges will not occur.

2. The merchant by accepting the card for payment has the advantage of security of payment by the FIs.
3. The FIs issue the cards, settle other FI's cardholder and merchant transactions with VISA, process the incoming transactions and provide the cardholders with monthly statements.
4. VISA standardizes the transaction process and settles the interaction between cardholders, merchants, and the FIs. It also keeps track of transactions and markets the card.

Normally for every transaction, one or two FIs are involved: the cardholder's and the merchant's. The cardholders of one FI might go to the merchants of the same FI or another. Therefore, depending on the situation, the FI could assume two roles; being an agent for both the cardholder and the merchant or being an agent for either of them. Hence, the transaction processing system must be able to separate the incoming transactions of a particular FI from the other FIs and route each transaction to the appropriate place for authorization and record keeping.

2.1.9.2 Overview of Transaction Processing Flow

In purchasing goods or services through credit cards, in on-line processing systems, the authorization is the essential element of the transaction processing system. The authorization process is the first level of protection against fraudulent activities and it also maintains control over the cardholder's credit limit. It should be noted that the authorization is kept as a temporary file for up to five days and when the transaction is recorded in the cardholder file, the cardholder account balance is updated. In addition to on-line authorizations, there are merchants who have flow limits. If the amount of the transaction is below that limit, the authorization does not need to go through the FI's system and the merchant has the right to authorize the transaction locally. In fact, due to a widespread POS network in Nigeria many merchants have 'zero' flow limit and almost every transaction has to be authorized on-line by the related FI (Soheila, 2013).

The authorization process begins when a cardholder uses his/her card for a transaction. The POS machine reads the magnetic stripe embossed on the back of the card which encodes the card holder's name, account number, credit limit, and the expiry date. The authorization is completed when the transaction is approved and the cardholder signs the transaction slip. The next step is the submission of transaction slips to the FIs which either is done electronically or

manually. In electronic transfer, the POS machine keeps track of all the authorizations and sends them electronically to the FI (Patidar and Sharma, 2011). In this case the merchants do not need to submit the transaction slips. The manual option is when the merchant sends the actual slips to the FI and the FI's operators will enter the records manually into the system. In both cases after the submission of transactions, the FI credits the merchant's account by that amount.

To handle a large number of cardholder's monthly statements, FIs have set up several billing cycles during the month. A certain number of cardholders are associated with each of these cycles and the date for each billing cycle is different from the other cycles. At the end of each cycle a new statement is processed and mailed to the cardholder of that cycle along with a due date for payment. The statement contains information on the transactions such as the previous and the new balance, the minimum payment, and the available credit is also included. The cardholder is required to pay the total or part of the balance. If the balance is paid back in full, there are no interest charges. If the cardholder's payment is less than the minimum amount, the credit rating of the cardholder could be affected and the cardholder may be considered delinquent. Another type of transaction possible by credit cards is obtaining cash advances. In this type of transaction the interest is charged from the day when the money is withdrawn even though the balance is paid back in full on the statement's due date.
For handling a huge number of daily transactions, FIs and VISA have implemented a real-time, non-stop system of computer hardware and software. This system includes the communications network among the FIs and the VISA network as well as handles the data processing and the record keeping tasks. Fig. 2.12 depicts an overview of the VISA transaction processing system. The main components of the system are described below (Xiong *et al*., 2013).

The Card

A credit card is standard plastic card with a magnetic stripe on its back which is read by a POS machine at the point of purchase. The front side of the card has the cardholder's name, account number, the expiry date and a hologram. Currently, there are a variety of cards in the market. In general, the main categories of cards are: (1) classic, (2) gold, and (3) platinum. Classic cards do not normally have annual fees and are not associated with rewards programs. Very often, the credit limit on gold and platinum cards is much higher than the classic types but these cards have annual fees as well. Services and rewards such as insurance coverage for car rental are mostly associated with these types of cards.

The Swipe Machine

POS terminals or swipe machines are very common in Nigeria and are used for on-line authorization. After swiping the card through the machine and entering the amount of purchase on the keypad, the POS terminal reads the card's magnetic stripe information and places a call to the merchant FI's computer. This information, along with the merchant number, is transmitted via a modem, to the on-line authorization system. This service is typically processed by non-stop Tandem computers.

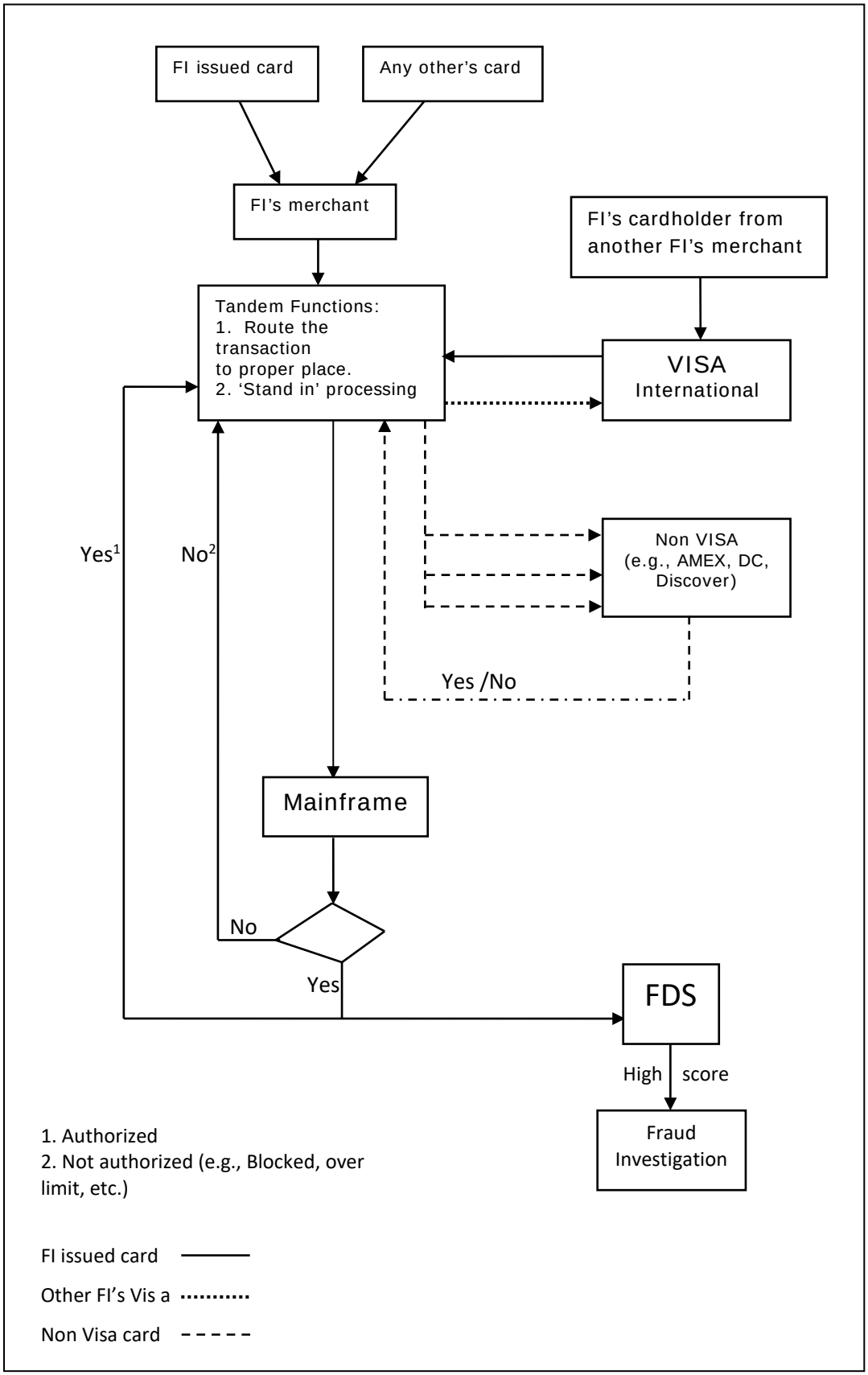


Fig. 2.12: Over-view of transaction processing flow (Soheila, 2013)

The Tandem

The Tandem is a non-stop computer used to process al1 the incoming electronic transactions regardless of the merchant's institution and country (Soheila, 2013). Every FI has its own Tandem which is connected to the VISA network. The functionality of the Tandem is summarized below.

1. Keeping a record of al1 incoming transactions for further referral in case of any system malfunction**.**

The incoming transactions are categorized as follows*:*

(a) A transaction by the merchant and the cardholder from the same FI.

(b) A transaction by the FI's merchant with a cardholder from another FIs**.** These transactions will be routed to VISA network and from there they will be sent to the cardholder FI's Tandem.

(c) A transaction by the FI's cardholder with another FI merchant. These transactions are sent to the VISA network and from there they are routed to the cardholder's FI Tandem for authorization.

2. There are occasions when the FI's mainframe is not able to do the authorization processing due to:

(a) A system breakdown,

(b) When the FI's computer system is down for different reasons (e.g., maintenance).

In these circumstances, the Tandem does 'stand-in' authorization processing, that is, it authorizes a transaction on behalf of the mainframe. This process is described below.

The Tandem authorizes the transactions based on a 'negative file' and an assigned floor limit. Negative file includes all the card numbers that have been considered fraudulent internationally. This list is provided by Visa international and is updated quite frequently with the occurrence of new fraud cases. Before any authorization, the Tandem checks that the card number is not on that list. The Tandem does not have cardholder's account information and, therefore, it cannot do any credit limit checking for the cardholder's account but there is a set credit limit for the incoming transactions that the Tandem will check and will not exceed. When the cardholder FI's mainframe becomes available again, the Tandem will send the approved authorized transactions to the mainframe either in real time or as a batch file, depending on the circumstances.

The Mainframe

The Tandem sorts the incoming transactions and transmits only those transactions which are from the FI's card holders or merchants to the FI's mainframe computer for authorization.

The mainframe, as the main component of the system, processes all the incoming authorization requests. For authorization, the mainframe performs a series of checks to ensure that the customer is eligible for making purchases. Some of these checks are listed here:

Card Expiry Date: If the card is expired the authorization is not allowed and the transaction is declined.

Excessive authorizations: Under the normal situations a client will not exceed a certain number of transactions in a 24 hour period. This check limits the number of authorizations that a customer can do during that period. If an account goes over the allowed number for the day, the authorization will either be declined (D) or referred (R) (i.e., referring the case to the FI staff).

Blocked: Block codes are used to put conditions on accounts. An account is checked for being fraudulent, delinquent or blocked. If any of these checks are positive, the authorization will either be declined or referred and the transaction is denied.

Credit Limit and Check: This check verifies that the cardholder has not exceeded his/her credit limit. If the sum of the current transaction amount and the current balance is under the credit limit, the authorization will be approved, otherwise it will be declined.

In the checking process, if one of the required checks for the transaction fails, the authorization is declined and this refusal will be sent to the Tandem and from there it will be sent back to the merchant. When the transaction passes al1 the required checks, the approved authorization goes back to the Tandem and from there, is sent back to the merchant. To make al1 these activities happen, FIs have implemented several sophisticated software packages. The databases required to track the aforementioned activities are as follows:

1. **Merchant file:** Information on the FI's merchant is included in this database.
2. **Cardholder File:** Information on the FI's cardholder account such as name, address, account number, current balance, credit limit, expiry date, and soon are contained in this file.
3. **Authorization Log:** All the authorized transactions done by the FI for its own cardholders are included in this file.
4. **Posted TX file:** This file keeps a record of all the transactions that have been received from the Tandem but have not yet been posted to the cardholders monthly.

5. **Statement File:** At the end of the cardholder's cycle, the accumulated transactions in the posted TX file will be sent to this file and the monthly statement for the cardholder is printed out.

When an authorization is approved, the account's available credit and amount/number of authorizations are updated and the mainframe sends this information to the authorization log database and the posted TX file. At the end of each cycle date, al1 the posted transactions of each account from the posted TX file will be sent to the statement file processor. This is used in printing out the monthly statements of the cardholder. When the cardholder pays the total or the minimum due amount, the cardholder's file is updated by this payment and the current balance is adjusted. To save computer disk space, the statement file keeps a record of the last three statements and by the production of a new statement the oldest statement is archived.

2.1.9.3 Fraud Schemes

Unauthorized use of credit cards for acquiring goods or services is fraud. Visa and Master Card constitute about 65 percent of al1 outstanding revolving credit worldwide and the substantial number of fraud occurrences is centered on one or both of these cards. Most credit card fraud schemes fall into the following categories:

1. Lost / Stolen
2. Never Received Issued (NRI) (Mail theft)
3. Counterfeit
4. Telemarketing and mail-order
5. Fraudulent applications

Lost and Stolen

Lost and stolen cards account for the majority of fraud cases. Fifty five percent of Visa and forty nine percent of MasterCard losses are based on lost/stolen cards. The average loss incurred by this kind of fraud is $700. When a card is lost or stolen the opportunity for fraud starts. Workplaces, glove compartments of cm, and sporting facilities are the main sources of stolen cards. Very often these losses are caused by a relative or friend's unauthorized use of the card without the cardholder's knowledge. Sometimes cardholders might sell their card to criminals, then report the card as lost or stolen or they might do shopping and then repudiate the event and report the card as lost or stolen (Xiong *et al*., 2013).

Never Received Issued (NRI)

An average of 439,000 new, renewal and replacement cards are mailed every day. Never received cards are card being stolen from the mail, either internally or externally, while in transit from the card issuer to the legitimate customer. The card may be used and then be sold on the black market. The average losses for this type of fraud are significant because the cardholder is not aware of the theft an by the time the fraud is detected a substantial amount of purchases has been made. Very often, only when the cardholder receives her/his monthly statement, does he/she realize that the card has been stolen in the mail.

Visa's never-received card losses leapt 68 percent in 1997. The average losses from never-received cards are about $1,500; double that of a lost or stolen card. One of the new ways to prevent this type of fraud is to send the card to the cardholder as a worthless piece of plastic (electronically blocked). On the receipt of the card, the customers have to call the bank to activate their card.

Counterfeit

The fastest growing type of bank card fraud is the illegal counterfeiting of credit cards, mainly Visa and MasterCard. By employing new technologies, criminals are able to produce exact replicas of existing cards. The average reported losses, due to this type of fraud, are higher than any other fraud category estimated at about $4.500.

Telemarketing and Mail-order Fraud

There are occasions when a fraudulent merchant or telemarketer calls to sell a non-existent product over the phone and by acquiring the cardholder's card number, processes a fraudulent charge against the account. It should be noted that this type of fraud, due to customer awareness, is on the decline.

Fraudulent Applications

In this kind of fraud, fraudsters provide FIs with false information and identities to acquire a credit card illegally. Unlike stolen cards, these cards are not signed and it takes longer time before the fraud is detected. This kind of fraud, due to the awareness of the FIs, is on the decline.

New Technologies and Card Counterfeiting

Card counterfeiting, in terms of frequency and severity, is on the rise. The basic principle underlying this kind of fraud is an account number which could be obtained from different sources such as legitimate records made in hotels, restaurants, retailers, discarded drafts or computer software.

In order to issue credit cards, financial institutions generate a series of numbers. From these numbers, a certain number (e.g., 500 of them) may be selected by a process known as skipping and king used for issuing credit cards. To defraud, fraudsters may use an account generating software such as Credit master and Credit Wizard to determine the skipping code and reveal the valid credit card account numbers. Fraudsters may also use another type of software called Sniffers to find credit card numbers that individuals are online. This software searches the networks for 16 digit numbers, records them and sends them to the fraudster.

One of the latest methods of counterfeiting credit cards is 'bit copying'. This is a process by which the magnetic stripe encoding from one card is copied to the stripe of another card. This method is one of the common methods of counterfeiting credit cards and is drastically on the rise in Nigeria. Public places such as particular restaurants and gas stations are major sources of these fraudulent activities.

The acquired number will then be embossed or encoded on a piece of plastic designed for this purpose. Whenever the number is embossed on an ordinary (blank) plastic card, it is called a 'white plastic' fraud. When the number is embossed and/or encoded on an expired or stolen credit card (from which the original data has been removed) the result is an 'altered' or 'falsified credit card. In the case of card alteration, magnetic stripes are altered or manufactured using equipment that can be purchased at electronic stores. When the number is affixed onto a totally counterfeit credit card, it is called a 'pure counterfeit' card. Fig.2.13 depicts the card counterfeiting process schematically.

The Counterfeiting Process

To understand the complexity and the nature of card counterfeiting, it is important to introduce the methodology used by counterfeiters in their operations. With improvements in technology, counterfeiting a credit card is often done by using desktop computer systems with peripherals, including embossers, laminators, and tipping foi1 in order to produce a more realistic looking card complete with a hologram and fully encoded magnetic stripe.

Often examination of the hologram is the key to the identification of a counterfeit card. On the legitimate cards, the hologram is embedded in the plastic at the time of manufacturing whereas counterfeit credit cards commonly contain a hologram affixed to the top of the card rather than embedded in the card. Thus, it can be seen or felt to rise slightly above the card face upon close examination.

The magnetic stripes and holograms used to counterfeit bank cards have a distinct submarket within the criminal communities.
The card counterfeiting in Nigeria is mainly an organized crime activity. This criminal activity started in Vancouver where fraudsters imported the technology of pure counterfeit credit cards.

FIs employ various technologies to detect and prevent credit card fraud. One of these is special security number embedded in the magnetic stripe. The Card Verification Value CVV), Card Verification Code (CVC), and Card Identification (CID) are the security numbers being used by VISA, MasterCard, and American Express, respectively. This number, done with the account number and expiration date, forms an algorithm during the authorization process. If any part of this algorithm is missing or incorrect, the authorization at the point of sale (POS) will be declined. For this reason, fraudsters not only need to have a valid account number but also need to know the mathematical formula used to mate the code and the method of its encryption to be able to produce a counterfeit card.
However, there are many situations where preventive techniques (e.g., holograms, validation codes such as CW) are not effective. For instance, in placing a telephone-order transaction or using the card over the Internet, these security features cannot be checked.

Smart Cards
To address the problem, credit card manufacturers plan to employ a series of security features, most of which are designed to enhance customer identification and authorization requirements. Due to the shortcomings of holograms as a fraud preventive, the next generation of credit cards, called smart cards, has computer chips instead of holograms.

Each card contains a microprocessor memory chip as well as data encoded on the magnetic stripe. For an authorization the cardholder is required to enter the personal identification number (PIN) encoded on the microchip. The industry foresees a time when bank customers will be able to use a single card to administer al1 their financial needs. Since the late 1980s, French banks with about 25 million smart cards in circulation, (about half of the world's total of smart cards), have already made use of this technology and based on reports, their fraud volume has been cut drastically.

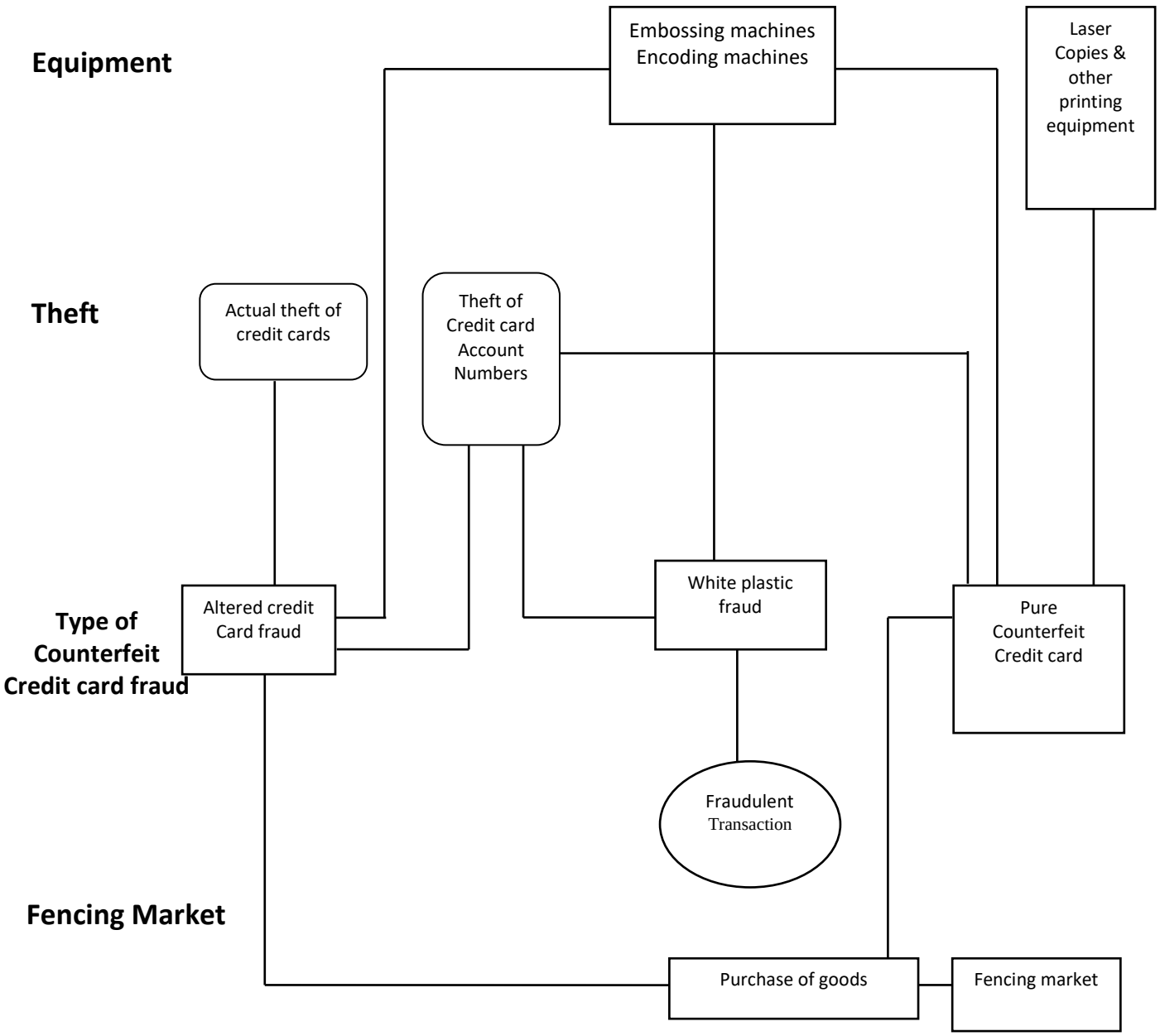


Fig.2.13: Counterfeiting Process (Soheila, 2013)

2.1.9.4 FDs and Credit Card Fraud

FIs make extensive use of NN based software to spot and flag transactions inconsistent with the cardholder's usual behavior. The focus of attention in this research is FDS, ANN base software being used by 40 of the top 50large credit card issuers worldwide including our collaborating FI. Historically, the first version of this software entered the market in 1992.

FDS is real customized software designed to determine the likelihood of card fraud. By using legitimate and fraudulent transactions, FDS has built an individual behavior profile for each

account. To the knowledge of the author, there is no documentation on the software due to the proprietary and business concerns of the software provider. Therefore, it is not clear how this profile is established but the conjecture is that the account profile file includes the type of merchant at which the cardholder typicality shops, the time of the day that the cardholder normally makes purchases, the geographic locations done with many more characteristics that only software developers are aware of. FDS inspects and evaluates the incoming transactions to set if they fit into the customer's established profile. Any deviation from the usual cardholder's behavior is monitored and scored by this system.

Based on the changes that FDS detects in the customer's pattern of behavior, it assigns scores between 1 and 1000 to each transaction. The higher the score, the higher the likelihood of fraud. Bank authorities set a threshold value and al1 transactions scored above this threshold are considered suspicious so that when these scores hit the set threshold, a case is created and is flagged for further investigation. Inherently, FDS makes no assumption about the suspicious transactions and transmit the flagged accounts, in real time, to the FI's fraud department for further follow up and investigation.

Fraud Investigation Process

To prevent more losses due to credit card fraud, FIs have set up groups or departments responsible for following up on the potentially suspicious transactions identified by the FDS.

The flagged accounts with their associated transactions are presented on the fraud analyst computer screen in real time. Fraud analysts examine the flagged transactions with the client's history and their experience determines the potential risk associated with these transactions. This judgment is based on different criteria such as the type of the merchandise (e.g., jewelry, high price electronic items), the unusual number of transactions or large amount of charges in a given day, the credit limit variations.

Based on bank policy, whether a transaction is considered to be legitimate or fraudulent, and the fraud analyst has to call the cardholder for transaction verification.

The cardholder can be reached

a. The cardholder confirms the transaction; referred to as 'false positive'. Approximately 90 percent of flagged cases by FDS are false positives.

b. The cardholder denies the transaction which results in two possibilities: (1) The card is lost, stolen or counterfeit, (2) the cardholder has made the Purchase but repudiates the event by reporting the card as lost or stolen. In both cases the fraud analyst will block the account.

The cardholder cannot be reached

a. The investigator will leave the customer a message to cal1 the bank back as soon as possible, he may block the account temporarily and makes a note on the system for further follow up.

b. The analyst is not able to find the cardholder due to wrong address or telephone number. This case has the high potential of fraud; therefore, the account will be blocked.

This procedure will be repeated for all flagged accounts.

2.1.10 Bankruptcy Fraud

Bankruptcy fraud occurs when consumers use their credit cards to spend more money than they can actually pay (Linda *et al.*, 2009). Credit cards can be seen as a way for consumers to borrow money from their banks. Normally, consumers will use their credit cards to carry out daily transactions. At a regular basis – for instance once every month – the bank will send a bill to their customers in order to request a payment for their credit card transactions. Customers, who plan to commit bankruptcy fraud, will overdraft their credit card accounts and then declare themselves as being in a position of a personal bankruptcy. In such a case the bank will have to pay for all the losses. Xiong *et al.* (2013) state that bankruptcy fraud increases expeditiously and can cause serious losses to issuing banks. In addition to that, they suggest the evaluation of credit card applications in order to verify the creditworthiness of applicants. Such an evaluation can usually reveal the possibility of a customer to go bankrupt in the future. Xiong *et al.* (2013) also state that the above-mentioned evaluation is not enough because customers with initial good creditworthiness can still be proved insolvent at a later stage. Therefore even if an applicant, who satisfies the desirable levels of creditworthiness, is provided with a credit card account, the latter should keep being inspected by the bank in order to predict any possibility of future insolvency. Whittaker *et al.* (2005) claim that a missed payment on a credit

card bill is an indication of an insolvent customer (Whittaker *et al*., 2005). Banks should take immediate measures to reduce the potential losses in case of a customer's bankruptcy. An example of those measures could be the reduction of allowed credit card limit. Of course, banks need to be very careful when taking restricting measures against their customers. The reason of this is that there is a danger to lose customers who did not intend to commit bankruptcy fraud but for some reason they were unable to pay their bills on time (Whittaker *et al*., 2005).

2.1.11 Credit Bureau

A way of evaluating the creditworthiness of a credit card applicant is by considering the reports of a credit bureau. Credit bureau are organizations which gather information about consumers from various different sources like financial institutions, banks, credit unions, courts and bankruptcy filings (Linda *et al*., 2009). Banks can request a report from a credit bureau by providing the details of a credit card applicant. Delamaire *et al*. (2009) state that a credit report can contain "personal particulars, details of non-compliance with contractual obligations, information from public directories and additional positive information such as repayment of loans according to contract at or before maturity". Information like current home address and occupation details may also be included in the credit report (Linda *et al*., 2009).

2.1.12 Credit Application Fraud

Credit application fraud occurs when a fraudster applies for a credit card using false information (Linda *et al.,* 2009). The credit application fraud is associated with another serious fraud, the identity fraud.

Identity Fraud

Identity fraud occurs when a fraudster uses a false identity with intention to commit another fraud (Phua *et al.,* 2009). Identity fraud can be perpetrated by inventing an identity which does not belong to a real person or by stealing the actual identity of a real person – also known as identity theft (Koops and Leenes, 2006). Inventing an identity is easy because there is no need for fraudsters to look for valid information of a real person. Nevertheless, this type of identity fraud is very difficult to succeed nowadays because financial institutions tend to check whether the applicant's information corresponds to a physical person or not. Identity theft, on the other hand, has a higher possibility to succeed; although it requires more effort to be committed due to the collection of a victim's personal information. Fraudsters gather all the necessary information to impersonate their victims. They can then apply for a credit card using victim's

information or commit other frauds. If the fraudster applies for a credit card and the fraudulent application succeeds then the fraudster will be able to use the issued credit card to carry out transactions on behalf of the victim. Bose (2006) states that identify theft grows rapidly year by year and that there were 9.9 million victims in America in 2005. There are several ways that fraudsters adopt to steal the personal information of their victims'. They can burgle victim's houses, steal their garbage or mails, bribe employees who have access to identity information or use malicious software like spywares to obtain unauthorized access to victims' computers and gather their confidential information (Bose, 2006).

The consequences of identity fraud in credit application can vary. If the fraudster invented an identity which did not belong to a real person and managed to receive a credit card, then the issuing bank would definitely lose their money because the fraudster would overdraft their credit card account and vanish without paying the bill. On the other hand, if the fraudster used a real identity then the real person would be liable to pay the bill unless he or she manages to prove the identity theft. In addition to that, the creditworthiness of real person might be damaged, making them unable to receive credit cards or loans in the future. It is worth mentioning that fraudsters who commit identity thefts can easily take over the bank accounts of real persons and use them to their advantage.

Chain of Trust

Abdelhalim *et al.* (2009), provide a broader definition of application fraud. They explain that "application fraud occurs when an individual or an organization applies for an identity certificate using someone else's identity". By identity certificate they mean any formal document which can prove the identity of a person like passport, credit card, driving license etc. They claim that application fraud is based on the way that identity certificates are used in the real world. More precisely they explain that there is a chain of trust between identity certificates which can easily be exploited by fraudsters. According to them, "the issuing of a credit card relies on the social security card, which in its turn relies on the passport, which again relies on the birth certificate". In other words, if a fraudster manages to steal the birth certificate of a victim, he will be able to apply for a new passport following by a new social security card and finally by a new credit card.

2.1.13 Credit Fraud Detection

It has already been mentioned that the losses of a credit card fraud can affect all consumers, merchants and issuing banks. Therefore, it is important to establish techniques for detecting and preventing credit card fraud. It contains a variety of techniques which can be used to build fraud detection systems. Understanding the characteristics of all those techniques can be a tedious task. A technique which promises a high predictive accuracy may be an appealing candidate to be used in the fraud detection system. However, there are various different parameters that need to be considered before deciding which technique best suits the needs of a particular situation. For instance, if the above mentioned technique which promises a high predictive accuracy cannot be applied into a large data set and if our data set is indeed large then that technique is obviously not appropriate for our situation.

2.1.14 Online Payment Using Credit Card

A credit card is a card that allows you to borrow money to pay for things. There will be a limit to how much you can spend called your credit limit. At the end of each month you can either pay off the whole of the amount you owe or make a minimum repayment (Edwards, 2013). With the rising interest in e-commerce, electronic payment techniques have increased more in number. The most popular way is payment-using credit card, probably because of its simplicity and comfort. The user just enters the relevant numbers, the merchant gets these validated and payment has been made. For extra security, the communication between user and merchant should be encrypted. Payment by credit card is the most popular and the easiest way to pay for goods and services online. A user simply enters his credit card number, his name and the expiry date of the card; the merchant validates this information and upon approval from the credit card company, ships the goods or provides access to the service. The only thing that needs to pass between the merchant and the buyer is the credit card number.

2.1.14a Evolution of Credit Card

A credit card is a great financial tool. It can be more convenient to use and carry than cash and it offers you valuable consumer protections under federal law. However, it is also a big responsibility. If not used carefully, you may end up owing more than you can repay, damaging your credit rating and creating credit problems for yourself that can be difficult to fix. Credit cards as we know today have been around for just over half of a century. One of the first credit cards appeared in 1951 when loan customers of Franklin National Bank of New York were screened for credit and those approved were given a card they could use to make retail

purchases. Participating merchants copied the customer information from the card onto a sales slip and the bank would credit the merchant account for the loan less a flat fee to cover the costs of providing the loan. In 1958, The American Express Company (a company built on the travelers' cheque business) began issuing a charge card for travel and entertainment charges, which was accepted at participating restaurant, hotel and airline merchants (creditcards.com, 2014). Cardholders enjoyed the convenience of plastic charge cards (especially when on the road for business) as well as the line of credit offered by the new bank credit cards. Merchants found that credit card customers usually spent more, than when they had to pay with cash (which is still true today – the average credit card purchase is 112% more than if cash is used). Accepting bank-issued cards was safer for the merchant than dealing with cash (more secure from internal and external theft and error) and less expensive than creating and maintaining a merchant-specific credit program (creditcards.com, 2014).

2.1.14b Credit Card Processing,

As the credit card processing became more complicated, the outer service companies started to sell processing services to Visa and MasterCard association members. This makes to reduce the cost of programs for banks to issue credit cards and settle accounts with cardholders and this makes for greater expansion for the payments industry (creditcards.com, 2014).The rules and standardized procedures of Visa and MasterCard are developed for handling the bankcard paper flow in order to reduce fraud and misuse of cards. The two associations also created international processing systems to handle the exchange of money and information and established an arbitration procedure to settle disputes between members.

2.1.14c Roles Involved In Credit Card Processing

Credit card processing is the process where it happens with many parties, it is also referred to as roles involved in the processing of a credit card transaction, namely, the issuer, the cardholder, the merchant, the acquirer, the card association, and the settlement bank (Keith Lamond, 2013). The card issuer is a licensed financial institution or its agent that issues the credit card to the cardholder and is responsible for the provision of responses to authorization requests. Those financial institutions can be a bank, also referred to as the issuing bank that is a member of a card association and adopts a payment card product promoted by the card association. The issuer here keeps the cardholder account's to which he charges the bills the issuer guarantees payment for authorized transactions, processing the payment card in accordance with the payment card product regulations and local legislation. The issuer supports

the clearing and settlement functions between the cardholder and the acquirer. The issuer host is the computing system that accesses the cardholder account's database and represents the issuer during the authorization, clearing, and settlement. The cardholder is a customer of the issuer that uses a payment card in a business to consumer (B2C) payment transaction. The card acceptor is the party that accepts a payment card at the point of service, formats the data of the transaction in a payment message, and forwards the payment message to the acquirer. Fig.2.14 shows the credit card transactions in real world and online.

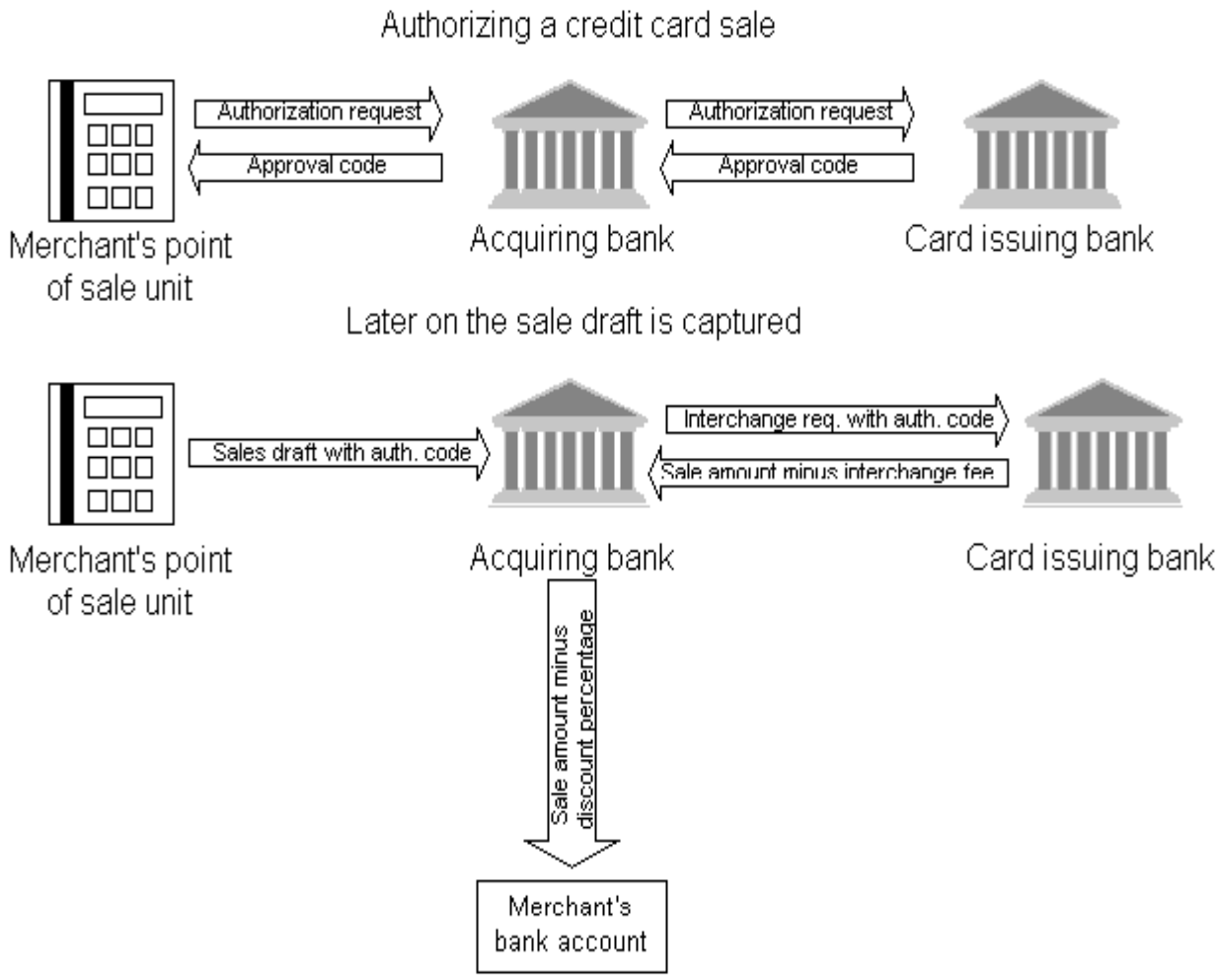


Fig.2.14: Credit Card Transactions: Real World and online (Lamond, 2013)

2.1.14d Credit Card Hacking

In 1980, the term hacking became a buzzword which was taken to be derogatory and by the misuse or overuse was attached to any form of socially non-acceptable computing activity outside of polite society. Credit card hacking is harder to do using traditional methods such as decrypting the magnetic stripes and recreating them. Hackers were assumed to be the fringe

society of the computing fraternity, who did not know any better and who had obtained access to a technology with which they terrorized the world of communications and computing. These connotations are in contrast to the use of the term in the 1950s and 1960s when hackers were at least to be tolerated for their potential, though not necessarily displayed in public. Scientists such as Edison (electric light bulb, phonograph, etc.), Fleming (penicillin), Barnes-Wallis (the bouncing bomb and swept wing aircraft), Watson-Watt (radar) and possibly even Babbage (the difference and analytical engines), may have been honored to be identified as hackers. Only in more recent times has there been confusion between the terms hacker, petty criminal (Lee *et al.*, 2011).

The concept of hacking as a methodology to achieve some particular goal has the allusion of working at something by experimentation or empirical means, learning about the process under review or development by ad hoc mechanisms. In hacking a computer, the enhancement of the system is an end in itself. Applications of that system don't count. In the same manner, there is not any particular way or any life cycle to do hacking and there is no specific end goal, an improvement is in itself an achievement, but not necessarily a reason for further activity. While hacking was generally counter-society it is not necessarily anti-society (Lee *et al.*, 2011).

2.1.15 Different Ways of Hacking

In an online credit card purchase, the payment data transfers between the customers PC and the vendor's shop over the internet. That raises concerns about credit card online security and identity theft. Most online shops are secured to prevent unauthorized people from seeing that information and you should see a secure site symbol displayed by the Web browser as proof. If one doesn't see evidence of a secure site, the transfer of personal information, including the credit card data, could be exposed and subject to theft. One should be careful and should think before entering the data, because it is difficult to intercept information transferred over a secured connection (FSPro-Labs, 2011).

2.1.15.1 Different Types of Fraudster

Fraudsters usually fall into one of three categories:

1. Pre-planned fraudsters who start out from the beginning intending to commit fraud. These can be short-term players, like many who use stolen credit cards or false social security numbers; or can be longer-term, like bankruptcy fraudsters and those who execute complex money laundering schemes.

2. Intermediate fraudsters who start off honest but turn to fraud when times get hard or when life events, such as irritation at being passed over for promotion or the need to pay for care for a family member, change the normal mode.
3. Slippery-slope fraudsters who simply carry on trading even when, objectively, they are not in a position to pay their debts. This can apply to ordinary traders or to major business people (Wells, 2016).

In 2007, Klynveld Peat Main Goerdeler (KPMG) carried out research on the Profile of a Fraudster (KPMG survey), using details of fraud cases in Europe, India, the Middle East and South Africa. The Association Certified Fraud Examiners (ACFE) carried out similar research on frauds committed in the US.

These surveys highlight the following facts in relations to fraudsters:

a. Perpetrators are typically college educated white male
b. Most fraudsters are aged between 36 and 55
c. The majority of frauds are committed by men
d. Median losses caused by men are twice as great as those caused by women
e. A high percentage of frauds are committed by senior management (including owners and executives)
f. Losses caused by managers are generally more than double those caused by employees
g. Average losses caused by owners and executives are nearly 12 times those of employees
h. Longer term employees tend to commit much larger frauds
i. Fraudsters most often work in the finance department, operations/sales or as the CEO.

The ACFE report also found that the type of person committing the offence depends on the nature of the fraud being perpetrated. Employees are most likely to be involved in asset misappropriation, whereas owners and executives are responsible for the majority of financial statement frauds. Of the employees, the highest percentage of schemes involved those in the accounting department. These employees are responsible for processing and recording the organization's financial transactions and so often have the greatest access to its financial assets and more opportunity to conceal the fraud.

2.1.16 Data Mining Techniques

This section describes the concept of data mining and the techniques which are found in the literature for detecting credit fraud. The main reason why these techniques are reviewed is that they form the basis of the credit fraud detection and they are reported as an implementation advice by the expert system.

2.1.16.1 Data Mining

Data mining refers to a family of machine learning techniques of extracting and analyzing non-trivial patterns from data (Chen *et al*., 2006). Data mining is also known as knowledge discovery because it can reveal previously unknown information which was hidden in the data of various databases. The mined information proves to be useful for the organizations who apply data mining. Based on the results, organizations may make important decisions which can help them survive in the competitive environment. For instance, an organization can analyze the sale records of its customers in order to send attractive offers on the most popular products. Hormozi and Giles *(*2004) stated that "data mining enables an organization to focus on the most important information in the database, which allows managers to make more knowledge-based decisions by predicting future trends and behaviors (Hormozi and Giles, 2004). Given that databases are rather large, it is very inconvenient and impractical to look manually for hidden patterns on the data. Therefore, data mining can be introduced to facilitate the discovery of useful knowledge. Forrester Research firm reported that 52%, of 1000 companies in total, decided to employ data mining techniques in 2001 to improve their marketing strategies; an increase of 34% comparing to 1999 (Hormozi and Giles, 2004).

Data mining can also be used to detect fraudulent credit card transactions, predict which customers are more likely to default their contractual obligations by going bankrupt and well as identify fraudulent credit applications. Srivastava *et al.* (2008) state that the only way to detect credit card fraud is by analyzing the spending behavior of customers using data mining techniques. Customers tend to follow a standard spending profile and therefore any transaction which deviates from that standard can be considered as suspicious. Suspicious transactions can be examined in detail by bank officers to determine whether they are indeed fraudulent or not. Like most of the machine learning algorithms, data mining techniques tend to learn models from data. Data mining is becoming a strategically important area for many business organizations including the banking sector. It is a process of analyzing the data from various perspectives and summarizing it into valuable information. Data mining assists the banks to

detect pattern in a group and unearth unknown relationship in the data. Data mining is a learning technique that has the capability to process data, analyze data and then extract gamut patterns, relationships and rules from the data.

Supervised Learning

This is the most common learning approach where the model is trained using pre-defined class labels (Bolton and Hand, 2002). In the context of credit card fraud detection the class labels may be the "legitimate" or "fraudulent" transactions. A supervisor provides a training data set whose transactions are classified. The training set can be used to build the predicting model. Any new transaction can be compared against the model to predict its class. If the new transaction follows a similar pattern to the illegitimate behavior – as this is described by the trained model – it will be classified as a fraudulent transaction. One limitation of supervised learning is that it requires confidentiality on the class of each training sample. If there is a fraudulent transaction X which is misclassified by the supervisor as legitimate then the constructed model will be problematic. The same happens for a legitimate transaction which is misclassified as a fraudulent. Moreover an unbalanced distribution – also known as skewed distribution – of the class labels in the training set can result in a model which does not have a very good predictive accuracy. Skewed distribution is the situation where there are much fewer training samples of class Athan class B. Maes *et al.* (2002) stated that fraudulent transactions are usually much fewer than legitimate ones. In addition to that, supervised learning models cannot detect new frauds. This is because the behavior of the new fraud is unknown to the trained model and therefore the latter cannot detect it. Further training is needed on the model to learn the existence of the new frauds. Finally a substantial effort is required from experienced people – also known as supervisors – to derive the labeled training samples which will be used to construct the model (Zhou, 2008).

Advantages:

1. It allows one to be very specific about the definition of the labels.
2. To determine the number of classes one wants to have.
3. The input data is very well known.
4. The results produced by the supervised method are more accurate and reliable in comparison to the results produced by the unsupervised techniques of machine learning.

Disadvantages:

1. Supervised learning can be a complex method in comparison with the unsupervised method.
2. It does not take place in real time while the unsupervised learning is about the real time.
3. It needs a lot of computation time.
4. If one has a dynamic big and growing data, one is not sure of the labels to predefine the rules.

Examples of supervised learning applications:

1. In banking and finance for credit card fraud detection.
2. Email spam detection.
3. In marketing area – a range of text mining algorithms are used for text sentiment analysis.
4. In medicine, for predicting patient risk (such as high-risk patient, low-risk patient) or for predicting the probability of congestive heart failure.

Unsupervised Learning

Unsupervised learning involves no class labels for model construction. Bolton and Hand (2002) explained that unsupervised learning techniques aim to discover those instances "whose behavior is unusual". A model which represents the "baseline distribution of normal behavior" is constructed without using class labels. That model is then used to detect instances which deviate from that normal behavior. It is particularly useful to notice that unsupervised learning techniques can detect both old and new fraud types since they are not bound to the fraud patterns which are encapsulated in the labeled training samples like supervised learning techniques do. Instead, unsupervised learning techniques aim to detect anything which does not comply with the normal behavior.

Advantages:

1. Less complexity in comparison with supervised learning.
2. Takes place in real time.
3. It is often easier to get unlabeled data.

Disadvantages:

1. One cannot be very specific about the definition of the data and the output.
2. Less accuracy of the results.
3. The results of the analysis cannot be easily ascertained.

Examples of unsupervised learning applications:

1. In marketing segmentation, when a company wants to segment its customers to better adjust products and offerings.
2. Social network and offerings.
3. Image segmentation.
4. Anomaly detection, etc.

Semi-supervised Learning

As mentioned above, supervised learning requires all the training samples to have their class labeled. In contrast unsupervised learning needs no labeled samples at all. Semi-supervised learning lies between supervised and unsupervised learning since it involves a small number of labeled samples and a large number of unlabeled samples (Zhou, 2008). In the context of credit card fraud detection, semi-supervised learning techniques may involve labels for some of the legitimate transactions only. This can reduce the effort needed by supervisors to classify training data.

2.1.16.2 Detection Techniques

This subsection provides a brief discussion on various data mining techniques which can be used to detect credit fraud. Classification is the most commonly applied data mining technique, which employs a set of pre-classified examples to develop a model that can classify the population of records at large (Bharati,2010).

They are as follows:

Logistic Regression: Logistic regression is a special case of linear regression analysis. Logistic Regression is used for predicting the outcome of a dependent variable based on one or more predictor variables. Here predictor variable can be either categorical or numerical.

Decision Tree: Decision trees are commonly used in credit card fraud detection. Decision tree is a flow based structure in which an internal node represents an outcome of the test on an attribute and a branch represents an outcome of the test and a leaf node represents classes. Root node is the top most node of the tree. Decision tree predicts the output of the target variable based on one or more input variables. Decision tree algorithms are ID3, C4.5, CART, and MARS. Fig.2.15 shows the decision tree.

Advantage: It can handle nonlinear and interactive effects of input variables.

Disadvantage: It has a complex algorithm. Even a small change in observed data might change the structure of a tree. Choosing splitting criteria is also difficult.

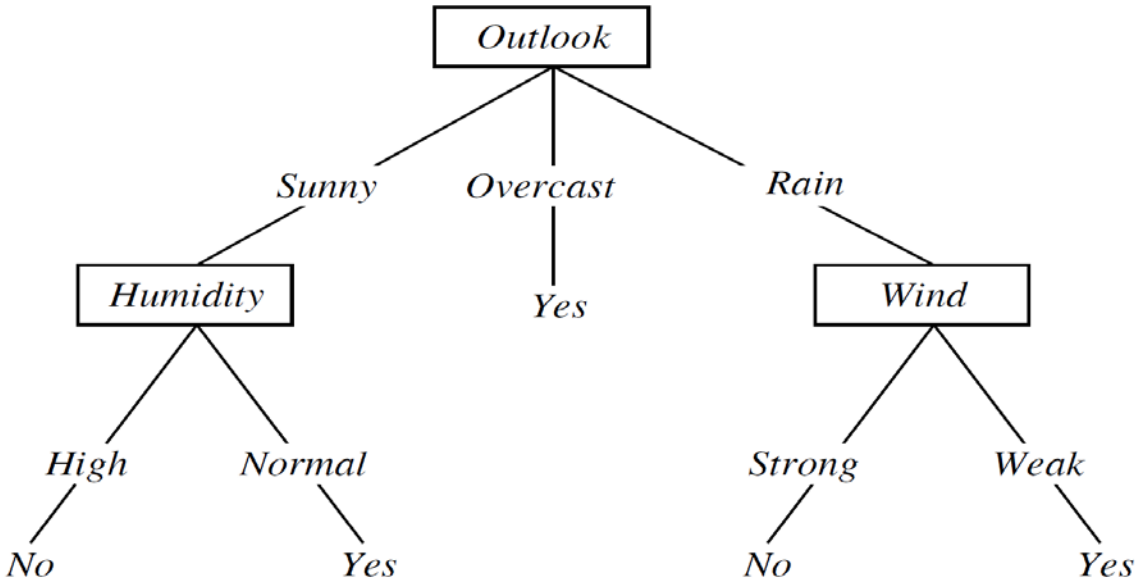


Fig. 2.15: Decision Tree (Mitchell and McGraw, 1997)

K-Nearest Neighbor (KNN) Algorithm

The concept of k-nearest neighbor can be used in many analogy detection techniques. Credit card fraud can be detected by using k-nearest neighbor algorithm. Using KNN, a new transaction is classifies based on the closeness of Euclidean distance function. In KNN, one classifies any new incoming transaction by calculating closeness or distance to other transactions. If they are close the transaction is illegal else the transaction is indicated as fraud. ***Advantage:*** It does not require establishing any predictive model before classification. ***Disadvantage:*** accuracy is highly dependent on the Euclidean distance.

Naïve Bayes Algorithm

Naïve Bayes classifier makes a conditional independence assumption that the effect of an attribute value of a given class is independent of other attributes. It is based on Bayes theorem. Advantage: It only provides a theoretical justification to the fact but does not use Bayes theorem.

Artificial Neural Network (ANN)

Although there are several fraud detection techniques based on knowledge detection, expert system, data mining etc. But they are problem to detect the fraud at the time when fraudulent transaction is in progress but with the help of techniques like Neural Network. When a customer uses a credit card there is a particular pattern of credit card use made by a customer. By using this previous data neural network is trained about a particular customer. As shown in

Fig.2.16neural network is trained based on his income, occupation, location, number of large purchases, location where large purchases are done etc. Based on these patterns the neural network classifies whether a particular transaction is fraudulent or genuine. The neural network produces output in real value between 0 to 1. If the neural network produces an output below 0.7 then the transaction is legal and if it produces an output above 0.7 then the chances of the transaction being illegal increases.

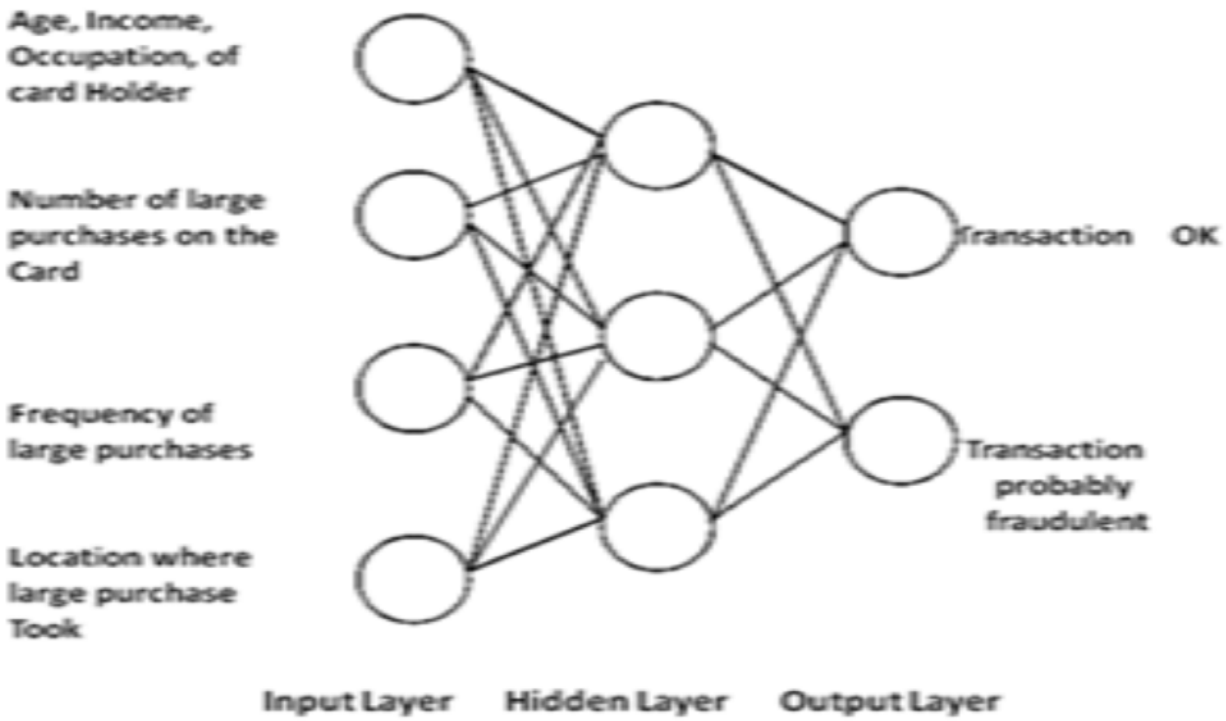


Fig.2.16: Layers of Neural Network (Sharma *et al.*, 2011)

Support Vector Machines (SVMs)

This means that an input sample can be classified into one out of two possible classes. It is suitable for credit card fraud detection because only two classes are needed; namely the "legitimate" and "fraudulent" class. SVM tries to calculate an optimal hyperplane which will separate the samples of the two classes (Gunn, 1998). There are various hyperplanes which can do that job but an optimal hyperplane will also maximize the margins between the samples of the two classes (Meyer, 2012). Fig. 2.17 which is taken from (Meyer, 2012) illustrates an example of two classes which are separated by an optimal hyper plane. Blue and black bullets correspond to the samples of the two distinct classes. Support vectors define the boundaries of each class by taking into account the sample which is closest to the hyperplane. Clearly the separating hyper plane lies in the middle of support vectors by maximizing the margin (the

distance between the hyperplane and the closest data points) between them. Hyperplane is a line that splits the input variable space. In SVM, a hyperplane is selected to best separate the points in the input variable space by their class, either class 0 or class 1. Support vectors are those points for which the Lagrange multiplier is not zero (there is more than just b in a support vector machine).

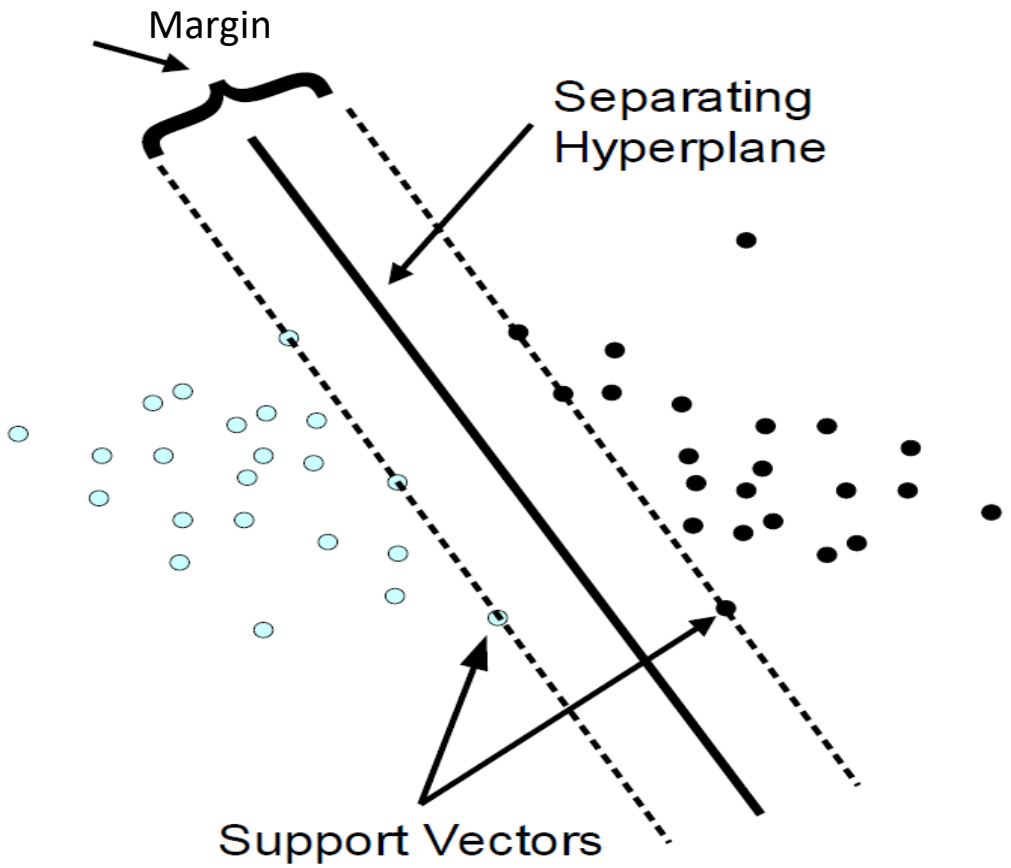


Fig.2.17: Support Vector Machine (Meyer, 2012).

2.1.16.3 Application Areas of Data Mining in Banking Sector

Banking information systems contain huge volumes of data both operational and historical. Data mining can assist critical decision making processes in a bank (Ionita and Ionita, 2011). Banks who apply data mining techniques in their decision making hugely benefit and hold an edge over. Some of these decisions are in the areas of marketing, risk management and default detection, fraud detection, customer relationship management and money laundering detection (Khac and Kechadi, 2010; Dheepa and Dhanapal, 2009). The banking industry across the world has undergone tremendous changes in the way business is conducted. With the recent implementation, greater acceptance and usage of 'electronic' banking, the capturing

of transactional data has become easier and simultaneously, the volume of such data has grown considerably. Data Mining can help by contributing in solving business problems by finding patterns, associations and correlations which are hidden in the business information stored in the data bases. By using data mining to analyze patterns and trends, bank executives can predict, with increased accuracy, how customers will react to adjustments in interest rates, which customers will be at a higher risk for defaulting on a loan, and how to make customers relationships more profitable. These applications are described below.

Risk Management and Default Detection: Every lending decision a bank takes involves a certain amount of risk. Quantifying this risk can make the risk management process easier and limit the risk of financial loss to the bank. Knowing customers' capability to repay can greatly enhance a credit manager's decisions. Data mining can also help to identify which customer is going to delay or default a loan repayment (Kazi and Ahmed, 2012). This advanced knowledge can help the bank to take corrective measures to prevent losses. For such forecasting, parameters to consider are turnover trends, balance sheet, limit utilization, behavioral patterns and cheque return patterns. Historical default patterns can also help in predicting future defaults when same patterns are discovered (Costa *et al.*, 2007). Data mining techniques are applied to enhance the accuracy of credit scores and predict default probabilities (Li and Liao, 2011). Credit score is a value representing a borrower's creditworthiness. Behavioral scores are obtained from probability models of customer behavior to forecast their future behaviors in various situations. Data mining can derive this score using the past behaviors of the borrower related to debt repayments by analyzing available credit history (He *et al.*, 2010).

2.1.17 Multi Agent Concepts

A multi-agents system is a computerized system composed of multiple interacting intelligent-agents within an environment. Multi-agents systems can be used to solve problems that are difficult or impossible for an individual agent or a monolithic system to solve. Intelligence may include some method, functional, procedural approach, algorithmic search or reinforcement learning.

The emergence of multi agent technology has resulted in a new paradigm, hence, transforming software development, design and implementation. The multi-agents based system for credit card fraud system is considered effective due to the multi agent capabilities. The desired optimal solution should be proactive and independent. Our desire is to demonstrate an alert notification to the key system (customer database and Credit card) on any suspicious transactions on the credit card process during run time.

2.2a Review of Anti-Fraud Systems

Fraud so far has been seen as serious economic threat. In the light of the above, several studies had been carried out to combat this menace. Alessandro (2010) proposed a multi-agents system called Forecaster's Intelligent Discussion Experiment System (FIDES).This system integrates the computational power of data mining tools and attack trees with experts' judgments negotiated through a Delphi-based system. Two scenarios are described: in the first one FIDES, supported by cause-effect diagrams, is used to classify alarms generated by the system to help the experts to focus on the dangerous ones; while in the second scenario FIDES is used in a proactive way in order to block or prevent human based frauds. The system combines Think-map, Delphi method and Attack trees and it has been built around audit team experts and their needs. The output of FIDES is an attack tree, a tree-based diagram to "systematically categorize the different ways in which a system can be attacked". Once the attack tree is successfully built, auditors are to choose the path they perceive as more suitable and can then make informed decision as to whether or not to start the investigation.

The layered system includes a core infrastructure and a configurable, domain-specific implementation. The detection layer employs one or more detection engines, which include; a rules-based threshes holding engine and a profiling engine. The detection layer may also be able to include an AI-based pattern recognition engine for analyzing data records, with the power of detecting new and interesting patterns and for updating the detection engines to ensure that the detection engines can detect the new patterns. In a concrete representation, the system is implemented as a telecommunications fraud detection system. When fraud is detected, the detection layer generates alarms which are sent to the analysis layer. The analysis layer filters and consolidates the alarms to generate fraud cases. The analysis layer preferably generates a probability of fraud for each fraud case. The expert systems layer receives fraud cases and automatically initiates actions for certain fraud cases. The presentation layer also receives fraud cases for presentation to human analysts, which in turn allows the presentation layer grant the human analyst's permission to initiate additional actions. These approaches to fraud detection are based primarily on setting preset thresholds and then monitoring service records to detect when a threshold has been exceeded. Threshold parameters for this system includes total number of calls in a day, number of calls less than one minute in duration, number of calls more than 1 hour in duration, calls to specific telephone numbers, calls to specific countries, calls originating from specific telephone numbers, etc. Depending on the nature certain of

customers or services, several parameters can be used to tailor a particular thresh holding for the system. Pattern recognition is a process whereby recorded events are analyzed to learn and to identify normal and potentially fraudulent patterns used in a system. If an interesting pattern is detected, pattern analysis processor determines whether it is a fraudulent or non-fraudulent pattern. In order to achieve this, pattern analysis processor relies on the strength of artificial intelligence technology to train itself in identifying fraudulent patterns.

The Analysis processor first determines normal patterns and then looks for deviations that can be identified as fraudulent. The Processor then detects emerging patterns of such deviations and identifies them as fraudulent patterns. There are various AI systems available for such a purpose. Examples include tree-based algorithms that obtain discrete outputs, neural networks, and statistical-based algorithms that use iterative numerical processing to estimate parameters. Such systems are widely used for pattern recognition. By utilizing an artificial intelligence system for pattern analysis, both normal and fraudulent patterns can be identified from the volumes of data stored in the history database. The processes of threshold detection, profiling and pattern recognition are described as being performed substantially in parallel primarily because time is of the essence. The processes can, however, be performed one after another or as some combination of parallel and non-parallel processing (John Gavan, 2003)

2.2b Review of Related Works on Credit Card Fraud Detection

The literature which is related to credit card fraud is reviewed. This is done by categorizing the work based on the detection techniques.

Case Study 1

Nabha *et al.* (2015) proposed a credit card fraud detection system using Hidden Markov model (HMM) and Adaptive communal detection. In this paper, the authors proposed a fraud detection system which detects the fraud before the transaction is completed. Hidden Markov model and communal detection have been used for increasing the accuracy of the system along with one time password (OTP). If any of the two methods detects the incoming transaction as fraud, OTP is sent to the registered cardholder.

Case Study 2

Singh and Rajan (2014) proposed fraud detection by monitoring user behavior and activities. In this paper, the authors proposed a unique and hybrid approach containing data mining

techniques, artificial intelligence and statistics in a single platform for fraud detection of online financial transaction, which combines evidences from current as well as past behavior. To determine the suspicion level of each incoming transaction based on the extent of its deviation from good pattern by using Bayesian Approach and Density Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm. The purpose of this method is to identify the customer behavior at the time of transaction to prevent fraudulent transaction.

Limitation

It is hard to track user's behaviors. All types of users (good users, business, and fraudsters) change their behavior frequently. Finding new or changing patterns is as recognizing old patterns.

Case Study 3

Sahil *et al.* (2015) proposed a credit card fraud detection using advanced combination Heuristic and Bayes' Theorem. The authors proposed the following steps; step one: Luhn's test is used to validate card numbers. Then, two rules i.e. address mismatch and degree of outlier are used to analyze the deviation of each incoming transaction from the normal profile of cardholder. These two steps compute initial beliefs. The initial belief values are combined to obtain an overall belief by applying advanced combination Heuristic in step four. Step five looks into spending history to extract characteristic information about genuine and fraud transactions.

Case Study 4

Hamid (2010) proposed a data mining framework for detecting subscription fraud in telecommunication. In this paper, the author proposed a framework to detect fraud using various techniques such as data cleaning, dimension reduction, clustering and classification.
The authors introduced 3 new features based on the clustering result in order to keep the learning from the clustering results.

Case Study 5

Yusuf and Bulkan (2013) proposed a cost-sensitive decision tree approach for fraud detection. In this paper, the authors discussed security mechanism such as CHIP and PIN that are developed for credit card system do not prevent fraudulent credit card usages over online credit card fraud, so the authors have developed and implemented a cost sensitive decision free

approach to detect fraudulent transaction and this approach is compared with the tradition classification models on a real world credit card data sit.

Case Study 6

Wiese *et al.* (2009) suggested an implementation of ANNs for detecting credit card fraud. Their implementation takes into account a sequence of transactions that have occurred at some time in the past, in order to determine whether a new transaction is legitimate or fraudulent. They believe that "looking at individual transactions" only is misleading since it cannot face any periodical changes in spending behavior of a customer. They call their approach "Long Short-term Memory Recurrent Neural Network (LSTM)''

Guo *et al.* (2008) suggested a different implementation of ANNs by converting the training samples into confidence values using a specific mathematical formula and then supplying these values to train the ANN — instead of the original training samples. They call their approach "confidence-based neural network" and they claim that it can achieve promising results in detecting credit card fraud.

Another implementation of ANNs is suggested by Patidar *et al.* (2011). They used the genetic algorithm in order to derive the optimal parameters of ANN. Like many other data mining techniques, ANNs make use of a number of parameters which need to be specified by software developers. Although the values of theses parameters can seriously affect the predicting accuracy of ANN models; a standard practice for specifying these parameters has never been established. The use of genetic algorithm which is suggested by Patidar *et al.* (2011) can help in deciding these optimal parameters. They call their approach "Genetic Algorithm Neural Network (GANN)".

Case Study 7

Chen *et al.* (2006) suggested an implementation of SVM which they call "Binary Support Vector System (BSVS)". The approach of Chen *et al.* (2006) is insensitive to skewed distribution of training samples.

An innovative implementation of SVMs for detecting credit card fraud is also suggested by Chen *et al.* (2004). They suggested for the issuing banks to ask their new customers to fill some questionnaires that can help them understand the spending habits of the customers .This is particularly useful since there is no prior history on the spending behavior of new customers

and therefore the detection techniques cannot spot fraudulent transactions at the initial stage. Therefore the answers to the questionnaires can be used in a similar manner to the historical information of each customer. They call their approach “Questionnaire-Responded Transaction Model” (QRT Model).

Limitation

One of the main problems of data mining techniques arises in situations where the training samples have an unbalanced distribution — also known as skewed distribution. In such a case the misclassification rate is increased whereas the predicting accuracy of the classifier is reduced.

Case Study 8

Sahin *et al.* (2011) provided three different implementations of decision trees for detecting credit card fraud. These implementations are called C5.0, C&RT and CHAID. Their differences lie in the way they construct the tree as well as the pruning algorithm which they use to remove erroneous branches and nodes. According to the experiments made by Sahin *et al.* (2011), the best predicting accuracy was achieved by C5.0 with an average of 92.80%, followed by CHAID with 92:22% and finally by C&RT with 91.34%. In their experiments, the three DT implementations out-performed the SVM implementation which achieved an average accuracy of 88.38%.

Case Study 9

YU *et al.* (2009) suggested an implementation of outlier detection technique. The similarity metric that they used to detect outliers is called distance sum. This is mathematically explained. Yamanishi *et al.* (2004) suggested another implementation of outlier detection for detecting credit card fraud. They call their approach “Smart Sifter” and claim that it can be applied in real time. This means that a new transaction is checked as soon as it arrives before being authorized. This is not the case for most fraud detection systems because real time detection is time consuming. Most of them will check the newly authorized transactions at some time in the future — for example once a day — in batch processing mode.

Limitation

The main disadvantage of this approach is that a fraud is just detected but not prevented. If, for instance, a fraud was committed in a physical shop then the fraudster would take the products

and run away before the bank discovers this fraud. Therefore, somebody — either the legitimate cardholder or merchant or bank — would need to pay the losses of this fraud.

Case Study 10

Brabazon *et al.* (2010) proposed an implementation of AIs for detecting credit card fraud which is committed online only. Although their approach can identify 90% of legitimate transactions, 96% of fraudulent transactions are classified as legitimate and therefore their approach is at least unrealistic

Another proposal of AIs for credit card fraud has been made by Gadi *et al.* (2008). They used the genetic algorithm as well to derive the optimal parameters of their model.

Case Study 11

Farvaresh *et al.* (2010) proposed a data mining framework for detecting subscription fraud in telecommunication. In this paper, the authors proposed a framework to detect fraud telecommunication subscribers by using various techniques such as data cleaning, dimension reduction, clustering and classification and also introduced three (3) new features based on the clustering result in order to keep the learning from the clustering results.

Limitation

The main problem is that the framework needs the historic to classify the customer in the commercial and residential class.

Case Study 12

Quah and Sriganesh (2008) proposed a real-time credit card fraud detection using computational intelligence. In this paper, Neural Network technique is used to detect fraud transactions and a new and innovative approach called Self Organizing Map (SOM) that is a neural network based on the unsupervised learning to detect spending pattern of the customer in a credit card database and SOM is classified as a multilayer approach consisting of: The initial authentication and screening layers, The risk scoring and behavior analysis layer (core layer), a layer of further review and decision-making and the purpose of SOM is to classify and cluster input data, to detect and derive hidden patterns in input data and to act as a filtering mechanism for further layers.

Limitation

The detection system performance was not evaluated.

Case Study 13

Srivastava *et al.* (2008) proposed a Credit Card Fraud Detection Using Hidden Markov Model. In this paper, clustering technique is used to detect credit card fraud based on the behavioral fraud like card holder not present, mail theft, counterfeit fraud and a model called Hidden Markov Model is proposed that performs a sequence of operations in two phases: In training phase these operations are performed such as to create cluster, identify spending profile of customer. If transaction contains anomalies then it gives the alarm that the transaction is fraudulent and HMM is scalable for handling large number of transaction at a time.

Limitation

It does not propose any approach to detect other fraudster behavior such as address mismatch, Internet Protocol (IP) address.

Case Study 14

Kovach and Ruggiero (2011) stated that fraud prevention describes the security measures to avoid unauthorized individuals from initiating transactions on an account for which they are not authorized. In spite of many advanced mechanisms available for fraud prevention for online banking applications, it can fail. Fraud detection consists in identifying such unauthorized activity once the fraud prevention has failed. In practice, fraud detection must be used continuously, since the system is unaware that fraud prevention has failed (Bolton, and Hand, 2010). Among the approaches used by fraudsters, phishing is one of the most common forms for stealing account details for authentication from the customers. Social engineering is the most common method used in phishing. Social engineering usually comes in the form of e-mails trying to convince users to open attachments or by directing them to some fraudulent site, and most of the time it is so well designed that many customers are led to informing their account details. This paper presents a framework and the corresponding system, for online banking fraud detection in real time. It uses two complementary approaches for fraud detection. In the differential analysis approach, the account usage patterns are monitored and compared with the history of its usage, which represent the user's normal behavior. Any significant deviation from the normal behavior indicates a potential fraud (Murad and Pinkas, 2009).

Kovach and Ruggiero (2011) presented a fraud detection system proposed for online banking that is based on local and global observations of users' behavior. Differential analysis was used to obtain local evidence of fraud where a significant deviation from normal behavior indicates a potential fraud. This evidence is strengthened or weakened by the user's global behavior. In

this case, the evidence of fraud is based on the number of accesses performed by the user and by a probability value that varies over time. The Dempster's rule of combination is applied to these evidences for final suspicion score of fraud. To achieve their main, they proposed a system with the general system architecture as shown in Figure 2.18.

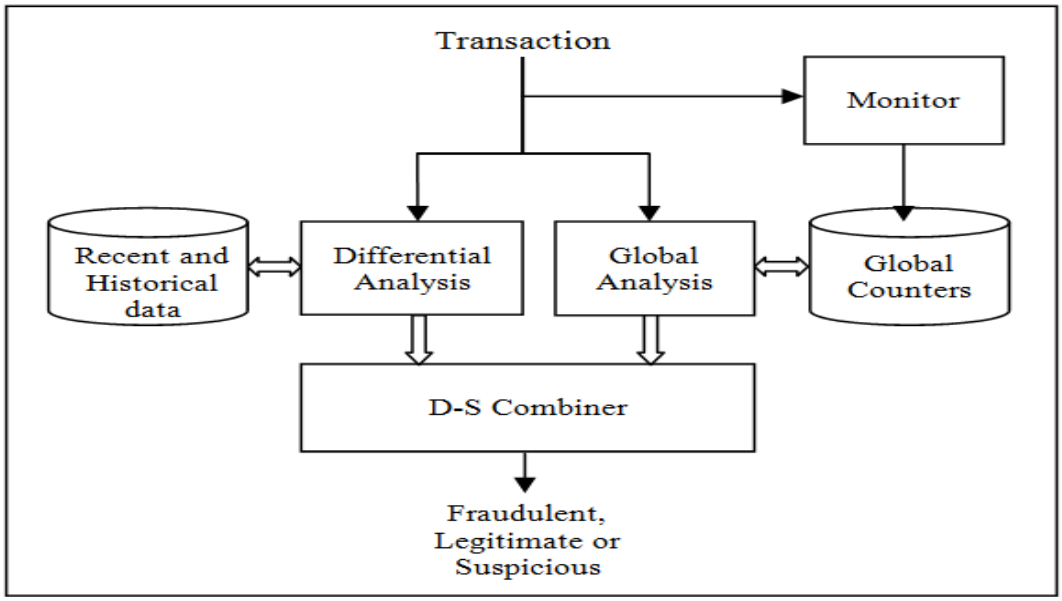


Figure 2.18: The General Architecture of Online Banking Fraud Detection (Kovach and Ruggiero, 2011)

In this architecture, each access device from which transactions are performed is supposed to have an identity. These identities are used along with a set of counters to monitor the number of different accounts accessed by each device. The system uses two independent approaches for detecting frauds: a differential analysis approach that detects significant changes in transaction patterns in individual accounts, and a global analysis approach that uses the set of counters to detect unusual number of accounts accessed by a single device. The fraud evidences determined by the two approaches are then combined in order to determine an overall score that may trigger an alarm depending on a prefixed threshold. Meanwhile, their main contribution is a fraud detection method based on effective identification of devices used to access the accounts and assessing the likelihood of being a fraud by tracking the number of different accounts accessed by each device.

Case Study 15

Kappelin and Rudvall (2015) stated that today it is easy to do banking transaction digitally, both on a computer or by using a mobile phone. As the banking-services increase and get implemented to multi-platforms, it makes it easier for a fraudster to commit financial fraud. In

their research, they discovered the need to focus on investigating log-files from a mobile money system that makes it possible to do banking transactions with a mobile phone. They developed a system whose main objective is to evaluate if it is possible to combine two statistical methods, Benford's law together with statistical quantiles, to find a statistical way to find fraudsters within a Mobile Money system. To achieve this, rules were extracted from a case study with focus on a Mobile Money system and limits were calculated by using quantiles. A fraud detector was implemented that uses these rules together with limits and Benford's law in order to detect fraud. The fraud detector used the methods both independently and combined.

Finally, the results obtained showed that it is possible to use the Benford's law and statistical quantiles within the studied Mobile Money system. It is also shown that there is only a very small difference when the two methods are combined or not both in detection rate and accuracy/ precision. Meanwhile, Kappelin and Rudvall (2015) concluded that by combining the chosen methods it is possible to get a medium-high true positive rates and very low false positive rates. The most effective method to find fraudsters is by only using quantiles.

Case Study 16

Khan *et al*. (2013) proposed credit card fraud detection model using Hidden Markov Model. Hidden Markov Models (HMMs) which is a statistical tool and extremely powerful method used for modeling generative sequences characterized by a set of observable sequences. Hidden Markov Model is probably the simplest and easiest model which can be used to model sequential data, i.e. data samples which are dependent on each other. An HMM is a double embedded random process with two different levels, one is hidden and other is open to all. The Hidden Markov Model is a finite set of states, each of which is associated with a probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities. In a particular state, an outcome or observation can be generated according to the associated probability distribution. It is only the outcome, not the state visible to an external observer and therefore states are "hidden" to the outside; hence, the name Hidden Markov Model (Ghosh and Reilly, 2014). HMM has been successfully applied to many applications such as speech recognition, robotics, bio- informatics, data mining etc.

Khan *et al.* (2013) achieved their aim by storing all the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) in the credit card database. If details entered by User into the database are correct then it will ask for Personal Identity number (PIN). After matching of Personal Identity

number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions is developed, then fraud detection system will start to work. Observation probabilistic in an HMM Based system is initially studied, spending profile of the cardholder and followed by checking an incoming transaction against spending behavior of the cardholder one can show clustering model is used to classify the legal and fraudulent transaction using data conglomeration of regions of parameter, HMM based credit card fraud detection during credit card transaction. Khan, *et al.* (2013) presented experimental result to show the effectiveness of our approach.

2.2c Review of Credit Card Authentication Techniques

Authentication is the process of determining whether someone is really who the person is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic (Margaret, 2014).Authentication is an act of confirming the truth of an attribute of a single piece of data or entity. In summary, user authentication is a means of identifying the user and verifying that the user is allowed to access some restricted services; for example, a user must be identified as a particular customer with an assigned property in the form of an account number in order to have access to their credit card information.

One-Factor Authentication

The existing credit card system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawals and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The credit card system compares the PIN entered against the stored authorization PIN for every credit card user (Adepoju, 2010). If there is a match, the system authenticates the user and grants access to all the services available via the credit card transactions. If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked. An instance of cash withdrawal on the existing credit card system is depicted in the transition diagram inFig.2.19. Entry of a correct PIN is adequate to authenticate a user to

the bank system and thereafter he is granted access to the system for withdrawal as depicted in Fig. 2.19.The existing system also blocks the credit cards after entry on an incorrect PIN thrice thereby eliminating further attempts to gain unauthorized access.

Weakness of One-Factor Authentication

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers) or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. Once an intruder acquires the user ID and the password, the intruder has total access to the user‘s resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner. For example, when a user ID and password is shared with a colleague there is no way for the system to know who the actual user is. A similar situation arises when a transaction involving a credit card number is conducted on the Web. Even though the data are sent over the Web using secure encryption methods, current systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card. In the modern distributed systems environment, the traditional authentication policy based on a simple combination of user ID and password has become inadequate.

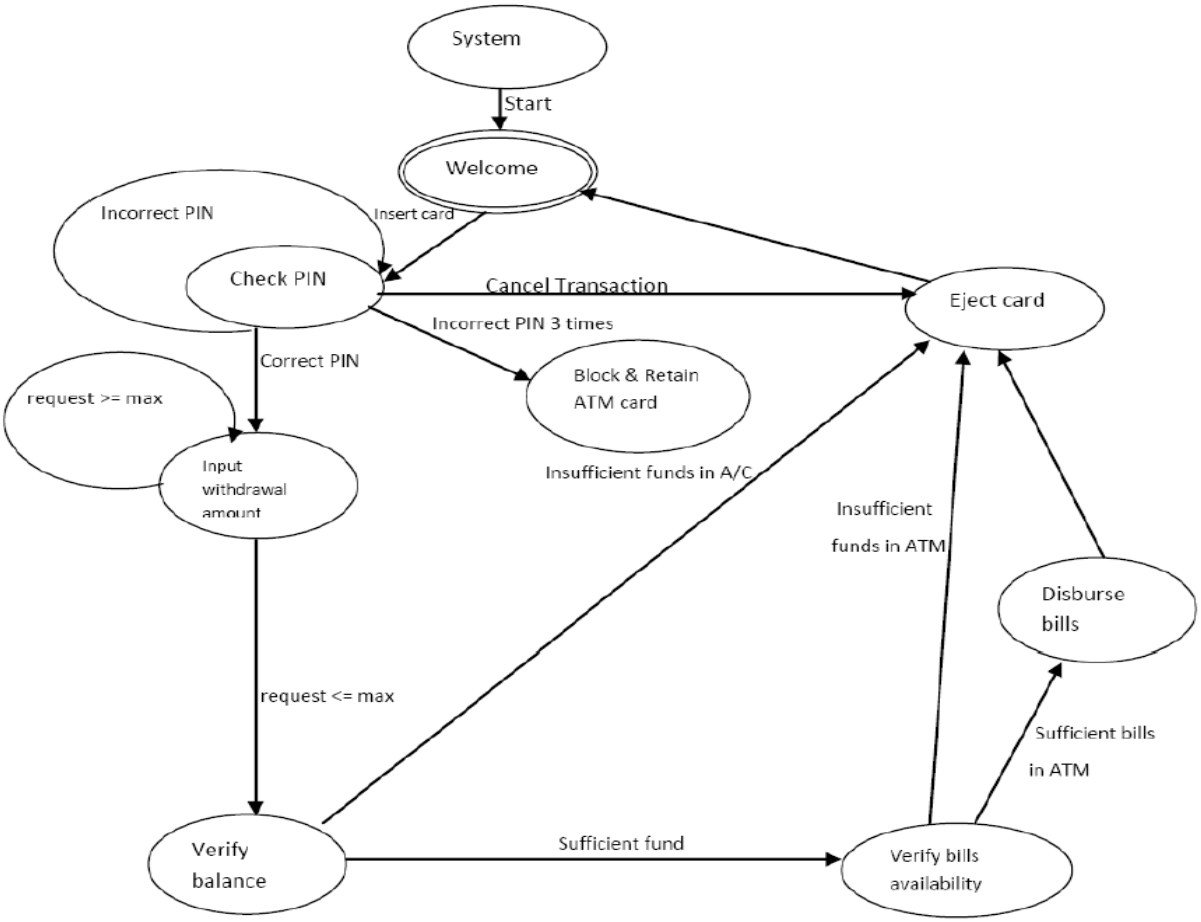


Fig.2.19: Transition diagram of the One-Factor Authentication (Adepoju, 2010)

Two-Factor Authentication

This is a security process in which the user provides two means of identification one of which is typically a physical token; such as a card and the other of which is typically something memorized, such as security code (Margaret, 2014). This is also called strong authentication. It may also be any two of the following;

a. Something known, like a password,
b. Something possessed, like your credit card, or
c. Something unique about your appearance or person, like a fingerprint.

When the confidentiality of information is particularly needful, the use of two-factor authentication may not guarantee enough protection. A stronger means of authentication, something that is more difficult to compromise is necessary. The system is in two different modes; the first will improve the security of the credit card by applying second level authentication on the existing credit card process for payment, after entry of a correct PIN, while the second will apply second level authentication in a scenario where a customer-

specified payment token. Fig. 2.20 depicts an instance of payment on the credit card for the two level authentication systems which is an enhancement of the existing system. The entry of a correct PIN is inadequate to authenticate to the bank system. This is because an additional level has been incorporated for the authentication process which requires the customer to enter a valid code which will be sent to the customer's pre-registered mobile device via SMS gateway.

If a correct code is supplied, the customer gets authenticated and is granted access for transactions. However, if an incorrect code is supplied even after the entry of a correct PIN, the authentication process fails and the customer is denied access for transactions. The second mode depicted in Fig. 2.20 is also an instance of payment on the credit card. This mode gives the customer the opportunity to choose the second level authentication process as an additional level of authentication for withdrawal in order to guarantee the security of the account owner. With this mode, a customer-specified withdrawal limit must be attained before the system prompts for entry of a valid code. If a valid code is supplied, the authentication process is complete and the customer is granted access for withdrawal. On the other hand, if an invalid code is supplied, the authentication process fails and the customer is denied access for withdrawal. It is imperative to note that if a customer-specified withdrawal limit is not in place, the entry of a valid PIN will be sufficient to authenticate the customer to the system and thereafter grant access for withdrawal. This implies that the second level authentication process would not be applied in such instances.

In addition, the entry of an incorrect PIN still guarantees maximum security in the proposed system because the bank card gets blocked in such instances. Two factor authentications also have setbacks similar to one factor authentication.

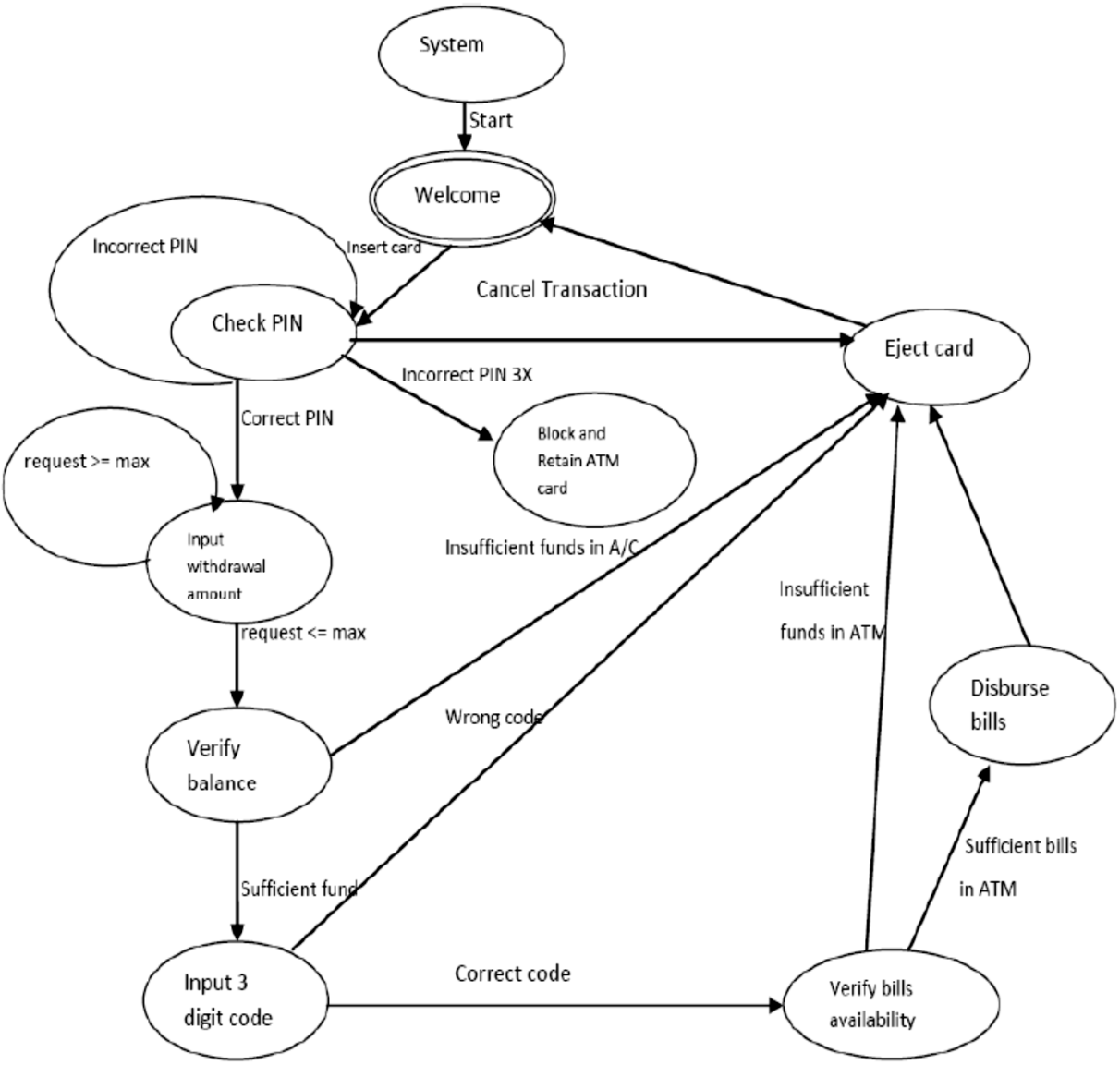


Fig. 2.20: Transition Diagram for Two-Factor Authentication (Margaret, 2014)

Biometric Authentication

Biometric authentication is one of the most exciting technical improvements of recent history and looks set to change the way in which the majority of individuals live. Biometric systems recognize individuals based on their anatomical traits (fingerprint, face, palm-print, iris, voice) or behavioral traits (signature, gait) (Anil, 2012). Kim (2003) had already proposed a two ID-based password authentication scheme where users are authenticated by smartcards, passwords and fingerprints. Biometric authentication is built on the fact that no two individuals can share the same morphological characteristics. Ratha (2014) presents integration of two technologies, namely biometrics and smartcard to meet some of the technical challenges posed in a network-

based authentication system. Biometrics provide the accuracy needed by these systems with smartcards providing security far beyond the magnetic stripe cards. By combining the two, the overall system requirements are better met than each of them individually.

In all, biometrics in general – fingerprint technology in particular, can provide a much more accurate, secure and reliable user authentication method especially for the proposed three-factor authentication system for credit card transactions.

Most biometric technology systems use the same basic principles of operation. First, a person must be registered, or enrolled, on the biometric system. Fig.2.21 shows the general biometric. The main components of general biometric are describe below:

a. **Enrollment**: The process by which a user's biometric data is initially acquired, accessed, processed, and stored in the form of a template for ongoing use in a biometric system is called enrollment. Subsequent verification and identification attempts are conducted against the template(s) generated during enrollment.

b. **Presentation**: Presentation is a process by which user provides biometric data to an acquisition device-the hardware used to collect biometric data. Depending on the biometric system, presentation may require looking in the direction of a camera, placing a finger on a platen, or reciting pass phrase.

c. **Biometric data**: The biometric data users provide in an unprocessed image or recording of a characteristic. The unprocessed data is also referred to as raw biometric data or as a biometric sample. Raw biometric data cannot be used to perform biometric matches. Instead, biometric data provided by the user during enrollment and verification is used to generate biometric templates, and in almost every system is discarded thereafter. Thus, Biometric systems do not store biometric data-systems use data for template creation. Enrollment requires the creation of an identifier such as a username or ID. This identifier is normally generated by the user or administrator during entry of personal data. When the user returns to verify, he or she enters the identifier and then provides biometric data. Once biometric data has been acquired, biometric templates can be created by a process of feature extraction.

d. **Feature extraction**: The automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process includes filtering and optimization of images and data in order to accurately locate features Since quality of feature extraction

directly affects a system's ability to generate templates, it is extremely important to the performance of a biometric system.

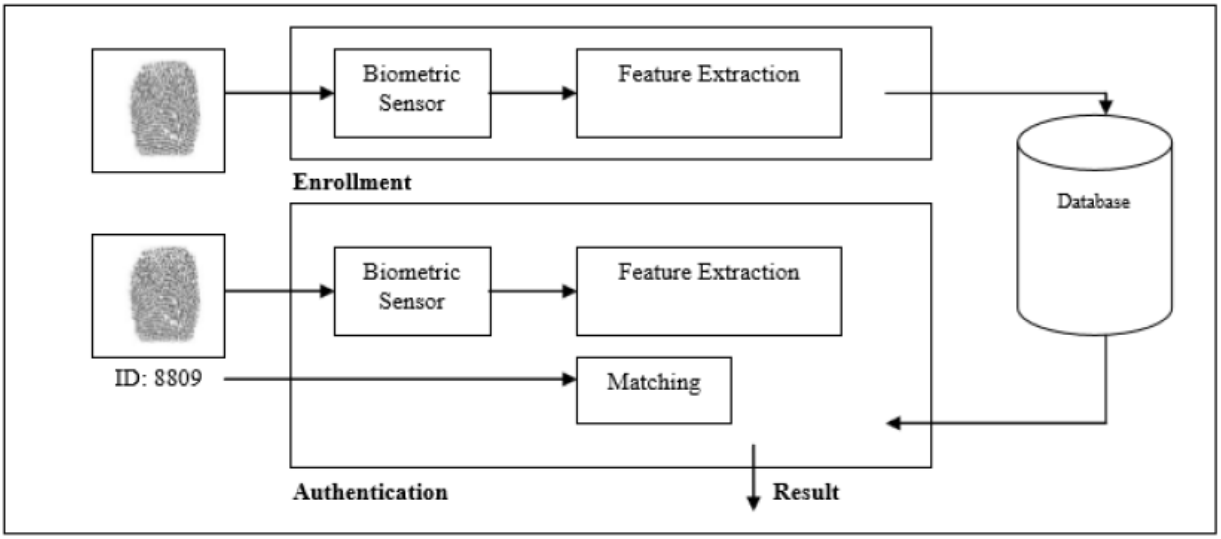


Fig. 2.21: General Biometrics System (Ratha, 2014)

Limitations of Biometric Authentication

Though biometrics as a third factor authentication for the credit card system add improved security to the system, it does has its own problems.

Anil (2012) named the two authentication errors that are mainly seen in biometric systems to include false non-match and false match. They further explained that false match occurs when two samples from the same individual have low similarity that the system cannot correctly match them, while false non-match occurs when two samples from different individuals have high similarity that the system incorrectly declares them as a match. The former case results in a denial of service to a legitimate user while the later results in intrusion into the system by an unauthorized user.

2.3 Summary of Literature Review and Knowledge Gap

Different works have been reviewed on fraud detection using different techniques. Khan *et al.* (2013) developed a credit card fraud detection model using Hidden Markov Model which is a statistical tool and extremely powerful method used for modeling generative sequences characterized by a set of observed sequences. Patidar *et al.* (2011) developed Artificial Neural Network which uses trained neurons that are assembled during initial transactions. The neurons are trained using the features and characteristics of earlier transactions. The Support Vector Machine is posed with problems of imbalanced distribution of training samples. However, all

the above mentioned works concentrating on fraud detection lack monitoring of detecting credit card fraud in real-time. Meanwhile, there is need for a distributed data mining system using multi agents. These agents are to be developed with data mining techniques to mitigate the flaws of single models. The new model is credit card fraud detection in Nigerian banks using adaptive data mining and multi- agents.

The existing systems adopted PIN or biometric or data encryption or HMM, and other fraud detection techniques. Most of these techniques have their setbacks. Attempt to use two level authentications yielded a better security system but still has some security challenges. Since the use of one factor or two factor authentications is still prone to security threats, this forms the major research gap.

CHAPTER THREE
METHODOLOGY AND SYSTEM ANALYSIS

3.1 Methodology Adopted

The multi- agent methodology, adaptive data mining technique and object oriented analysis and design methodology (OOADM) were adopted in this dissertation:

i. Multi- agent methodology (MAM) will provide an effective means for systematic monitoring of credit card fraud transactions in the banks so as to detect and report any abnormal financial transactions that may signify a high risk fraud and other financial inconsistencies. However, are well suited to dealing with the problem of monitoring vast volumes of dynamic information in a distributed fashion. In this way, they are to detect hidden financial problems, such as financial fraud, handle risks, and other inconsistencies. By utilizing a society of each charged with carrying out a different function autonomously, credit card monitoring systems will be able to analyze credit card qualitatively. There must be one consistent database of knowledge that enables the various agents to exchange knowledge regarding the entities involved.

ii. Data mining technique is used to extract and analyze non-trivial patterns from data sets on credit card frauds of various banks. It also helps to predict when the card is at default, and it uses the credit card to determining and analyzes the behavior and reliability of the customers. With data mining technique, banks can do a thorough profiling and ranking of their branches with respect to credit card fraud risk. To accomplish this, relevant information can be gathered from the credit risk information service databases. These files contain all the essential information pertaining to a credit card fraud. That includes characteristics such as identity of cardholders, location of the branch/bank where the credit card was issued and where the changes are made to the credit card.

iii. Object-oriented analysis and design methodology (OOADM) which is adopted in this dissertation is a set of standards for analysis and development of the credit card fraud detection system. It uses a formal methodical approach to the analysis and design of information system. Object-oriented design (OOD) elaborates the analysis models to produce implementation specifications. The main difference between object-oriented analysis and other forms of analysis is that by the object-oriented approach one organize requirements around objects, which integrate both behaviors (processes) and states (data) modeled after real world objects that the system interacts with. In other traditional analysis methodologies, the two aspects: processes and data are considered separately. For example, data may be modeled by ER diagrams, and behaviors by flow charts or structure charts. The primary tasks in object-oriented analysis (OOA) are:

a. Find the objects and organize them
b. Describe how the objects interact
c. Define the behavior of the objects
d. Define the internals of the objects

Common models used in OOA are use cases and object models. Use cases describe scenarios for standard domain functions that the system must accomplish. Object models describe the names, class relations (e.g. Circle is a subclass of Shape), operations, and properties of the main objects.

3.1.1 Sources of Data / Methods of Data Collection

In order to carry out a detailed analysis of the existing system, both primary and secondary data will be collected from different sources. Both secondary and primary data will be used to get facts on the subject where primary data will be collected from actual institutions and secondary data will be the data collected from literature review that include understanding and observing available credit card fraud detecting systems. Secondary data will also be gathered from a number of sources in order to carry out an insightful investigation into the existing systems, its working procedures, and its mode of operation. Secondary data include: internet sources, journals, books, newspapers and manual auditing of credit card fraud detection.

Data Collection Tools

Due to the sensitive nature of the study, the methods used for primary data collection were limited to the person(s) involved who were reluctant to have any written document from them, the result where the following methods:

Person/Telephone Interviews: This is done by interviewing bank key employees from their personal experience on areas on the credit card transaction that were prone to misuse by users or area already that had been misused by users. The key employees include branch managers, internal auditors and credit card officers.

Prototype System: This method proved to be very useful. Even though the bank employees were reluctant to give information on the subject, when provided with a prototype system and asked to contribute on checks that could be put in the system to detect possible credit card fraud they fully collaborated, thus most of the data collected is through this method.

3.1.2 Materials Required

Different web application languages and modeling tools will be used to come up with a comprehensive Credit Card Fraud Detection System (CCFDS). These include the following; Hypertext Markup Language (HTML), Hypertext Preprocessor (PHP), MySQL, Cascaded Style Sheet (CSS), Java Script, Dream weaver, Fireworks, SWiSHmax and Edraw.

Dream weaver is an HTML-based application that is used to generate graphical user interfaces. The visual editing feature enables the creation of a web page without having to type HTML code. Dreamweaver supports graphics created by Fireworks or any other application so that one can easily import those graphics onto the web page. It also provides a coding environment with coding tools for users to edit HTML codes or to include any other scripting language. The scripting language behind the development of the credit card fraud detection is PHP. Other Scripting languages used are CSS and JavaScript. JavaScript is used to add functionality beyond standard HTML to a web page. It adds interactivity to web site. Edraw application was used to draw the UML diagrams. The choice of PHP and MySQL for this dissertation is because of the following benefits they offer. MySQL is commonly used together with PHP in website development and is popular open source software. A PHP and MySQL database driven site completely separates content and designing part. This way one only needs to update the database and the rest is taken care of by the system.

3.2 System Analysis

3.2.1a Analysis of the Existing System

The overview of credit card has been shown in chapter two. However, the protocol for performing credit card transactions is composed of two query-response pairs. First, the Point-of-Sale solicits credit card number and expiration date, and the card responds with this information. In its response, the credit card also includes an iCVV, or integrated Card Verification Value: a dynamic security token intended to authenticate the message. Once this has been completed, the Point-of-Sale sends a charge request to the bank with the information received from the credit card, and then receives an authorization response to accept or reject the charge. Fig. 3.1 shows the current credit card (CC) protocol.

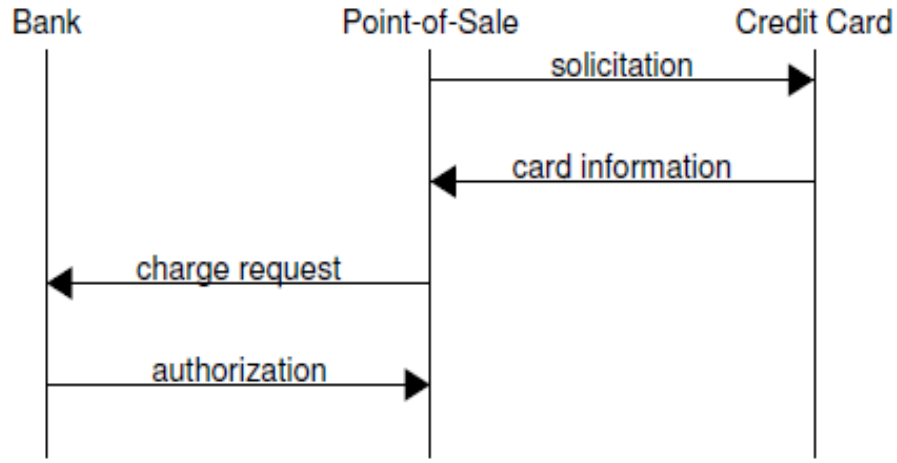


Fig. 3.1: The Current Credit Card Protocol

The exchange of messages in the CC Protocol is shown in Fig. 3.1. They are: solicitation, card information, charge request and authorization. Note that after the card responds to the Point-of-Sale, its involvement in the transaction is complete. The contents of these messages are as follows:

Solicitation: First, the Point-of-Sale solicits the credit card for its information. The solicitation is composed of a number of messages sent in both directions, identifying the Point-of-Sale type (e.g. 2PAY.SYS.DDF01) and the credit card type (e.g. VISA CREDIT). Since these messages are constant for a given Point-of-Sale and credit card, we abstract the solicitation messages as a single request from the Point-of-Sale to the credit card.

Card Information: The credit card responds to the solicitation by sending back the following card information:

1. The credit card number
2. The credit card's expiration date
3. The iCVV
4. The name of the bank that issued the card

The iCVV is an unpredictable 4-byte value freshly generated for every solicitation response, and is subsequently used by the bank to validate the transaction as described below.

Charge Request: The Point-of-Sale issues a charge request to the bank. This request is composed of:

1. The credit card number
2. The credit card's expiration date
3. The iCVV

4. The amount to be charged

Authorization: When the bank receives a charge request, it uses the credit card number to look up the account, verifies the expiration date, and then validates the iCVV to authorize the purchase. It will generally also perform some additional checks, such as verifying that the card was not reported lost or stolen, or matching this purchase's location against the known location of the card holder. Finally, it responds with its authorization decision.

When the credit card is manufactured, a secret seed value is shared between the credit card and the bank. This enables the credit card and the bank to both generate the same iCVV sequence, unpredictable to any party that does not have access to this seed. The iCVVs are simply sequential elements of this sequence: each time the credit card responds to a solicitation, it generates the next iCVV in the sequence and includes it with the card information response. In order to make an authorization decision, the bank searches through its account database which is indexed by the credit card number. Once the bank locates the account, it verifies that the received expiration date matches the expiration date on file. In addition, it recalls the iCVV from this credit card's previous charge request and generates the next element in the sequence, then compares the received iCVV to the value it generated.

It is possible that a card may generate an iCVV without communicating it to the bank. For example, a charge request may become corrupted in transit, or a Point-of-Sale may experience a network failure. As a result, a credit card's iCVV may have advanced further in the sequence than the bank expects. To handle this situation, the bank may generate several iCVVs in the sequence for comparison to the received value. If a match is found, the bank considers the iCVV to be valid. It updates its state into the pseudorandom sequence to reflect the received iCVV, and continues with any other checks to be performed before authorizing the charge. If no match is found, the bank considers the iCVV to be invalid and declines the charge.

3.2.1b Data Flow of the Present System

In Fig. 3.2, the data flow diagram of the existing system is depicted. The credit card holder supplies username and password, and then the system validate the user identity before proceeding to credit card verification. If the verification are through, the transaction will be completed otherwise access will be denied.

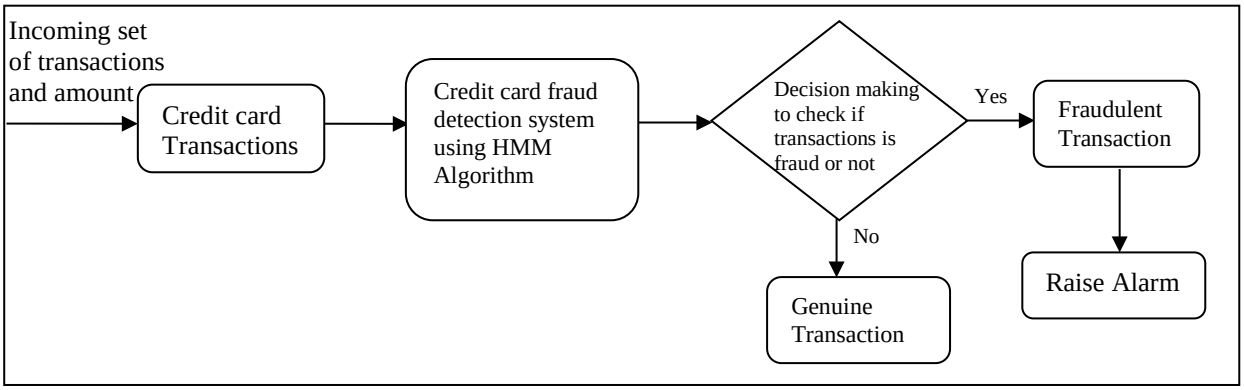


Fig. 3.2: Data flow diagram of the Existing System

1. The transactions that are supported out using any credit cards are accepted with the required details.
2. This transaction is further given to Credit Card Fraud Detection System
3. The score obtained from Credit Card Fraud Detection System is further used to identify or decide next action to be taken.
4. If the transaction is recognized as genuine transaction, then it is sent for further processing of clearance.
5. If the transaction is recognized as fraudulent transaction, then alert or alarm is raised to highlight for the same and is stopped from further processing of that transaction.

3.2.1.1 Advantages of the Present System

The present system is very useful to bank customers and bankers in the following ways.

1. Customers can make payment for purchases using credit card. This reduces the stress of queuing up in the bank to withdraw cash thereby wasting much time.
2. The existing system verifies the credit card details and users password before transactions can be carried out. This reduces the chances of fraudulent transactions using credit cards.
3. The workload on bankers is seriously reduced as transactions with credit card limit the number of customers they attend to on daily basis.

3.2.1.2 Disadvantages of the Present System

The current credit card protocol has several aspects which render it dangerous. Sensitive data is transmitted; it can be re-used by malicious parties. Proximity is used as an indicator of intent, requiring a card holder to maintain constant vigilance on the surroundings of their credit cards. These aspects invite a number of security attacks on the protocol.

1. **Eavesdropping fraud**: The goal of an eavesdropper is to gain the victim's credit card information such as the credit card number and expiration date. Eavesdropping is a passive attack, where the eavesdropper hears all communication between the Point-of-Sale and the credit card (Kortvedt, 2009). Communication between the bank and the Point-of-Sale is assumed to be secure. An outline of this attack is shown in Fig. 3.3.

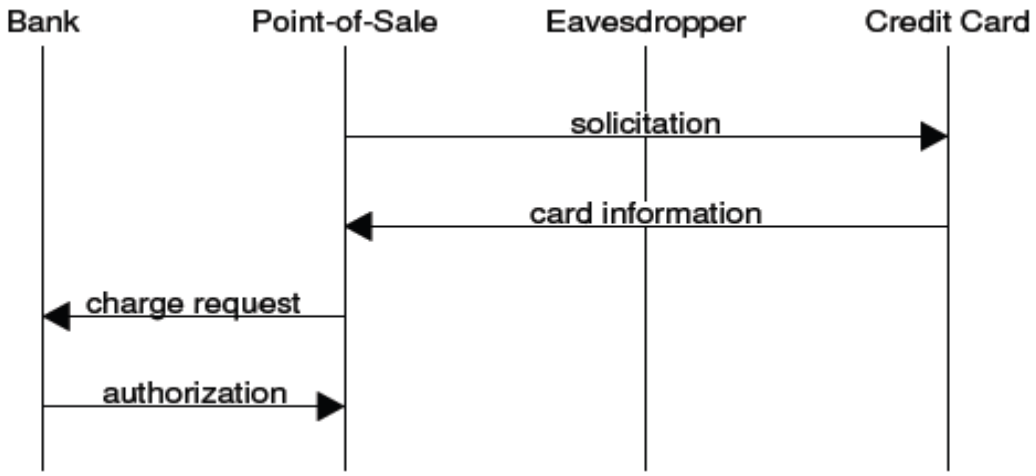


Fig. 3.3: Eavesdropping (Kortvedt, 2009)

One has demonstrated the feasibility of this attack by building a very low form-factor antenna capable of eaves-dropping on communications. In the current implementation of the CC Protocol, an eavesdropper acquires the credit card number, expiration date and the issuing bank name.

2. **Skimming fraud:** The goal of a skimmer is to perform a purchase on behalf of the victim, without the victim's knowledge or consent. First, the skimmer masquerades as a Point-of-Sale to the victim's credit card, acquiring the credit card number, expiration date, issuing bank name, and the iCVV. Subsequently, the skimmer masquerades as a credit card to a legitimate Point-of-Sale, making a purchase on behalf of the victim by replaying the skimmed credit card information and the iCVV. An outline of this attack is shown in Fig. 3.4.

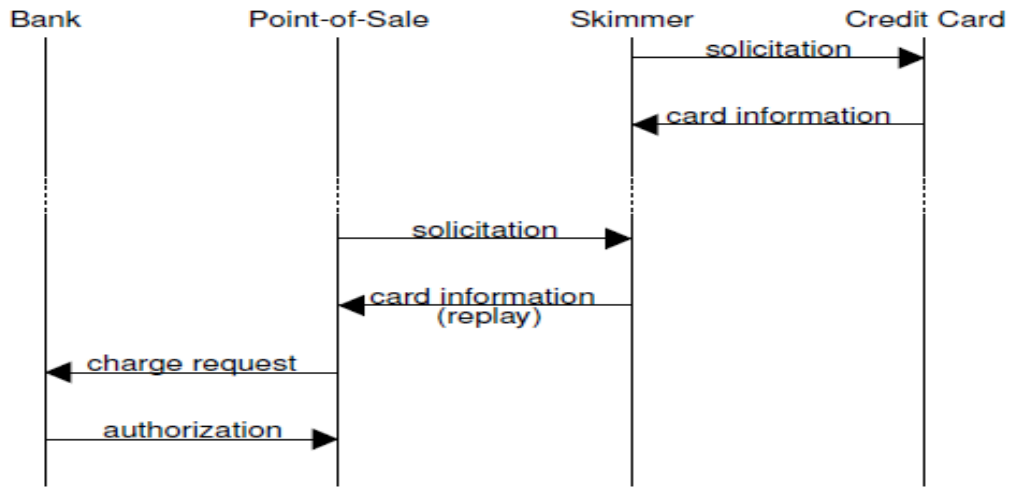


Fig. 3.4: Skimming

3. **Compromised Point-of-Sale fraud:** Any protocol in which the Point-of-Sale learns information capable of permitting multiple charges is vulnerable to Compromised Point-of-Sale attacks. We use this term to refer to any attack which involves the Point-of-Sale or merchant performing (possibly unintentional) actions leading to credit card theft (Eun, 2013). For example, a Point-of-Sale might be compromised and re-programmed to transmit credit card information to an attacker after every successful purchase. An outline of this attack is shown in Fig. 3.5.

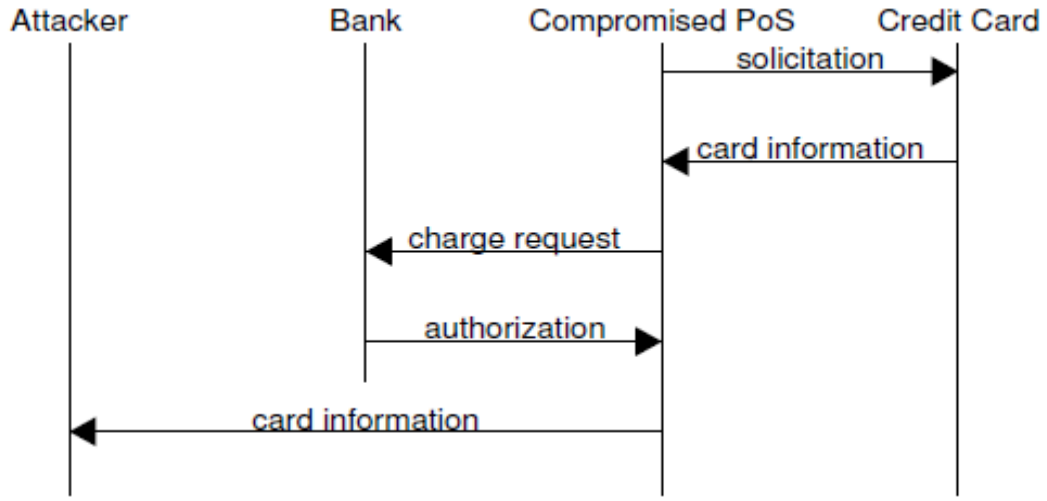


Fig. 3.5: Compromised Point-of-Sale (Robin, 2014)

3.2.2 Analysis of the New System

This dissertation focused on credit card application which is used to detect the fraudulent credit card activities on credit transaction. In this peculiar type, the pattern of current fraudulent usage of the credit card has been analyzed with the previous transactions, by using the multi- agents in data mining algorithm. Fig. 3.6 shows the data flow diagram of the new system model. The system has three data mining engines: customer/bank database and fraud detection database. The customer/bank database has the following: opening of account operation, withdrawal and deposit transaction and statement account. Fraud techniques database will give details of attack attempts on customer's credit card (such as date, time, amount and action taken). The New Credit Card Fraud Multi- Agents Model (CCFMAM) which is to detect the credit card fraud by analyzing the spending patterns on every card and figure out any inconsistency with respect to the usual spending patterns. Multi- agents will make use of these inputs (from user transaction input and past recorded credit fraud detection input) watch ongoing transaction to check whether is fraudulent or not, beginning from the most recent attack methods of fraudsters and concentrating on the most recent spending pattern of the transaction.

In the new system, when a credit card transaction is initiated, the system verifies the user's pin code and username by validating it on the bank database. If the pin fails to validate after three consecutive attempts, the account will be blocked and fraud alert sent to the fraud database. But if the pin verification was successful, the system will capture the credit card transaction details and verify the credit card information (such as name of the bank that issued the card, CCN, expiration date and iCVV) before passing the information to data monitoring agent.

The monitoring agent will use the last ten credit card transaction to build a transaction pattern for the customer and forward the pattern to the collating agent. The Monitoring agent will use machine learning technique to retrieve previous credit card fraud patterns from the credit card database and also retrieve the customer details from the bank database. At monitoring agent, each of these agents focuses on a particular type of credit card fraud, in parallel and report any suspicious attack to collating agent. However, the collating agent is responsible for communication with the diagnosing agent, which includes sending the task to be performed as input and providing the required data. The diagnosing agent will match the existing pattern of credit card transaction with the new transaction to check if there are variations in the pattern. If the transaction pattern does not match, the system will request for a secret question and answer from the user for more authentication. If the user fails the question, a fraud alert is sent

to the reporting agent. The reporting agent will then forward the extracted credit card transaction status to the database of the bank and the customer's phone and the transaction blocked. But where the credit card profile matched with the existing customer profile, the transaction is allowed to go through and the customer's account updated. At this, the transaction will be recorded on the credit card database and amount transferred will be deducted from the customer's account balance. Fig. 3.7 shows the Enterprise Architecture of the New System.

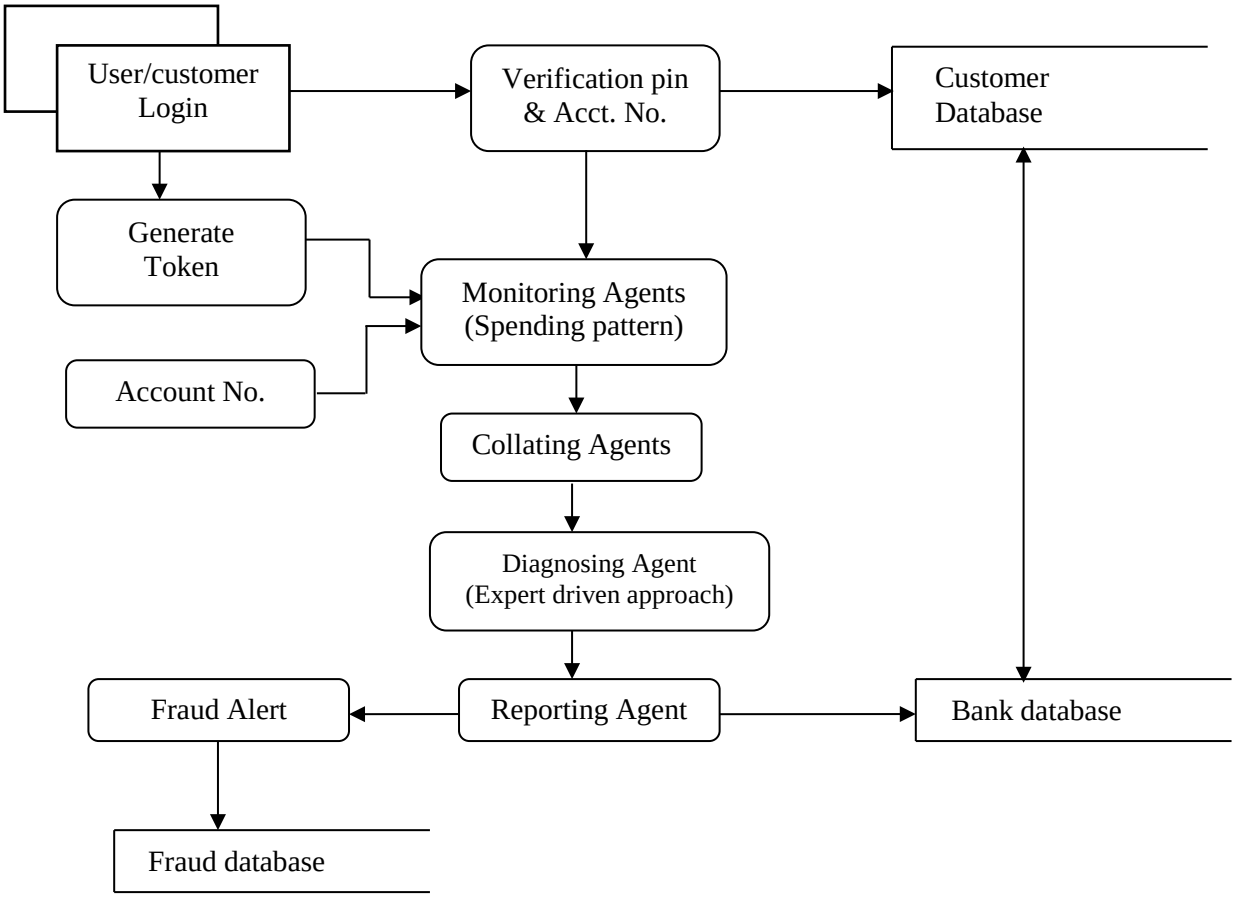


Fig. 3.6: Data Flow Diagram of the New System

Enterprise Architecture of the New System

The Enterprise Architecture of the New System is shown in Fig. 3.7

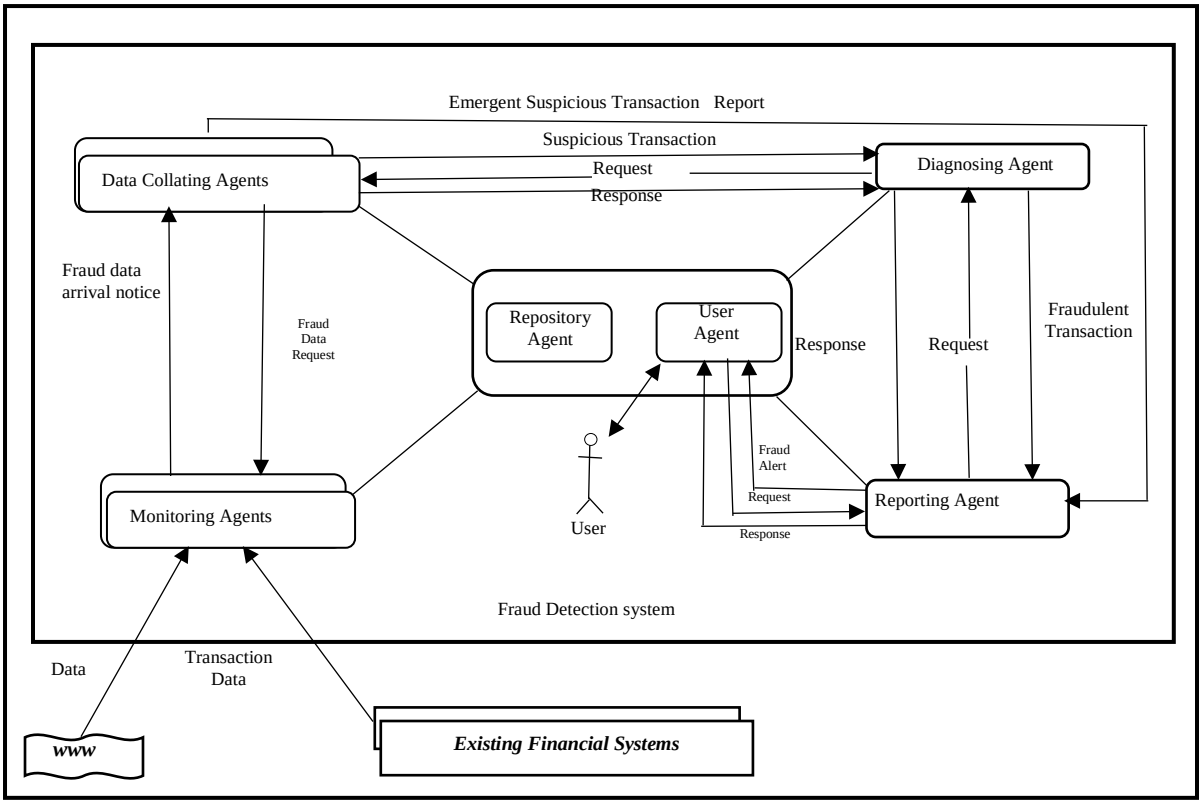


Fig. 3.7: Enterprise Architecture (EA) of the New System

3.2.2.1 Advantages of the New System

The new system will be of immense benefit to banks, and bank customers. The benefits include:

1. The adaptive data mining and multi-agents will introduce a more secured communication channels for credit card transactions thereby preventing loss of money by the customers to credit card fraudsters.
2. The bank customers will gain confidence that they are sending their personal information to legitimate banks' servers and not impostors. This will help to boost the electronic transactions thereby reducing the queue in the banking halls.
3. The fraud detection system ensures that all critical data (credit card numbers, for example) are encrypted and that only authorized users have access to data in its entirety.
4. The New system is featured with alert system to enable e-commerce owners receive alert of fraudulent activities and automatically disable customer's (victims) account involved.
5. With the New system, millions of transactions can be monitored in the real time.

3.2.2.2 Use Case Diagram of the New System

The model designed in this dissertation is divided into several modules that needs access restrictions. Different use cases were described in the way they were applicable in the software designed. Use cases are as listed below:

1. Bank staff Use Case
2. Credit card holder Use Case
3. Use Case diagram of the New System.

Use Case Boundary of Bank Staff

The system identified total of two roles that functions as access levels in the diagrams. A use case is a function to be performed by the system from the user's perspective. Fig. 3.8 is the use case boundary diagram of the new system. Fig. 3.8 represents the bank staff use case diagram. The bank staff will have access to opening a new account to customers, issue credit card pin to customers, credit or debit customers account during normal banking transaction within the banking hall.

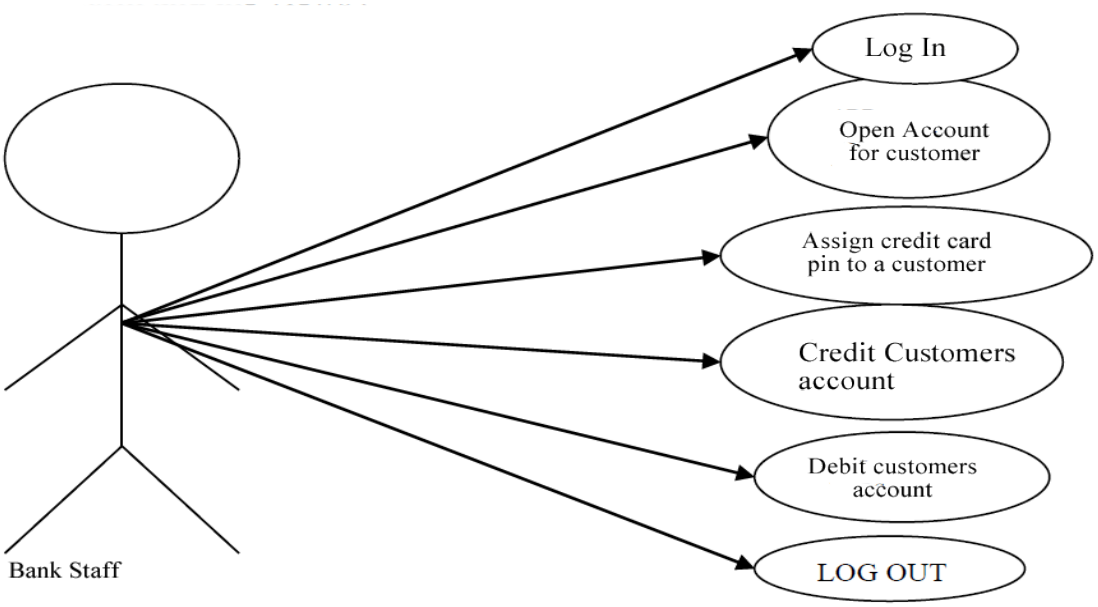


Fig. 3.8: Use Case Boundary of Bank Staff

Use Case Boundary of Credit Card Holder

The credit card holder can login to the system using credit card pin and username. The user can perform credit card transactions, view account balance, view account statement and also have access to changing the credit card pin as shown in Fig. 3.9.

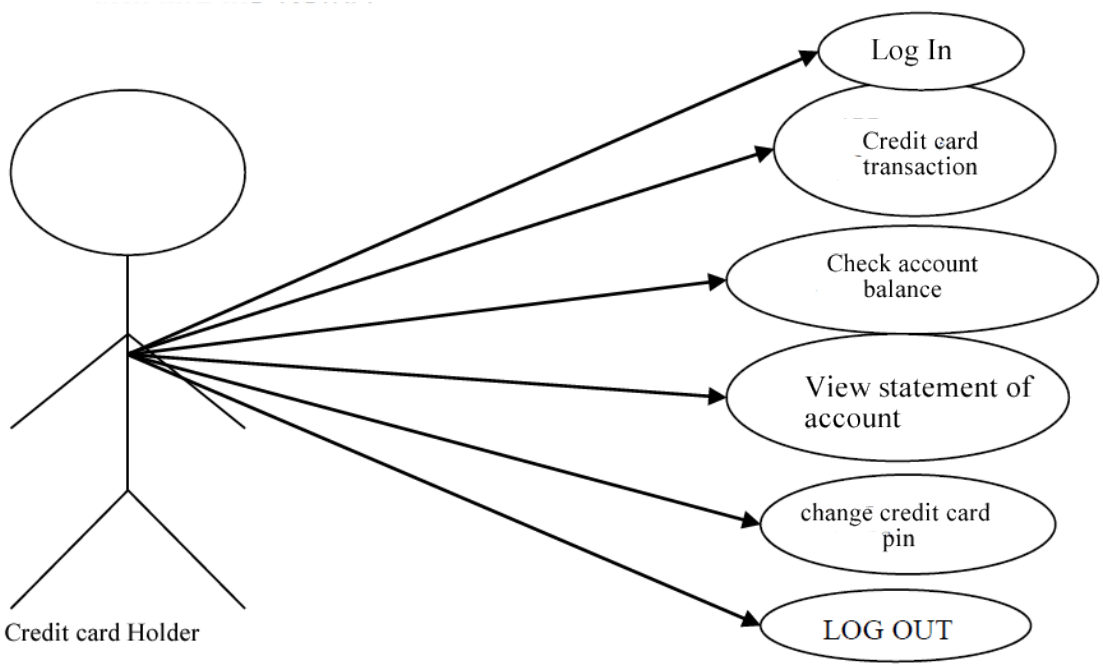


Fig. 3.9: Use Case Boundary of Credit Card Holder

Use Case Diagram of the New System

Fig 3.10 shows a use diagram of the new system, the large rectangle is the system boundary. Everything inside the rectangle is part of the system under development. Outside the rectangle are the actors that act upon the system. Actors are entities outside the system that provide the stimuli for the system. Typically, they are human users, or other systems. Inside the boundary rectangle are the use cases. These are the ovals with names inside. The lines connect the actors to the use cases that they stimulate.

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

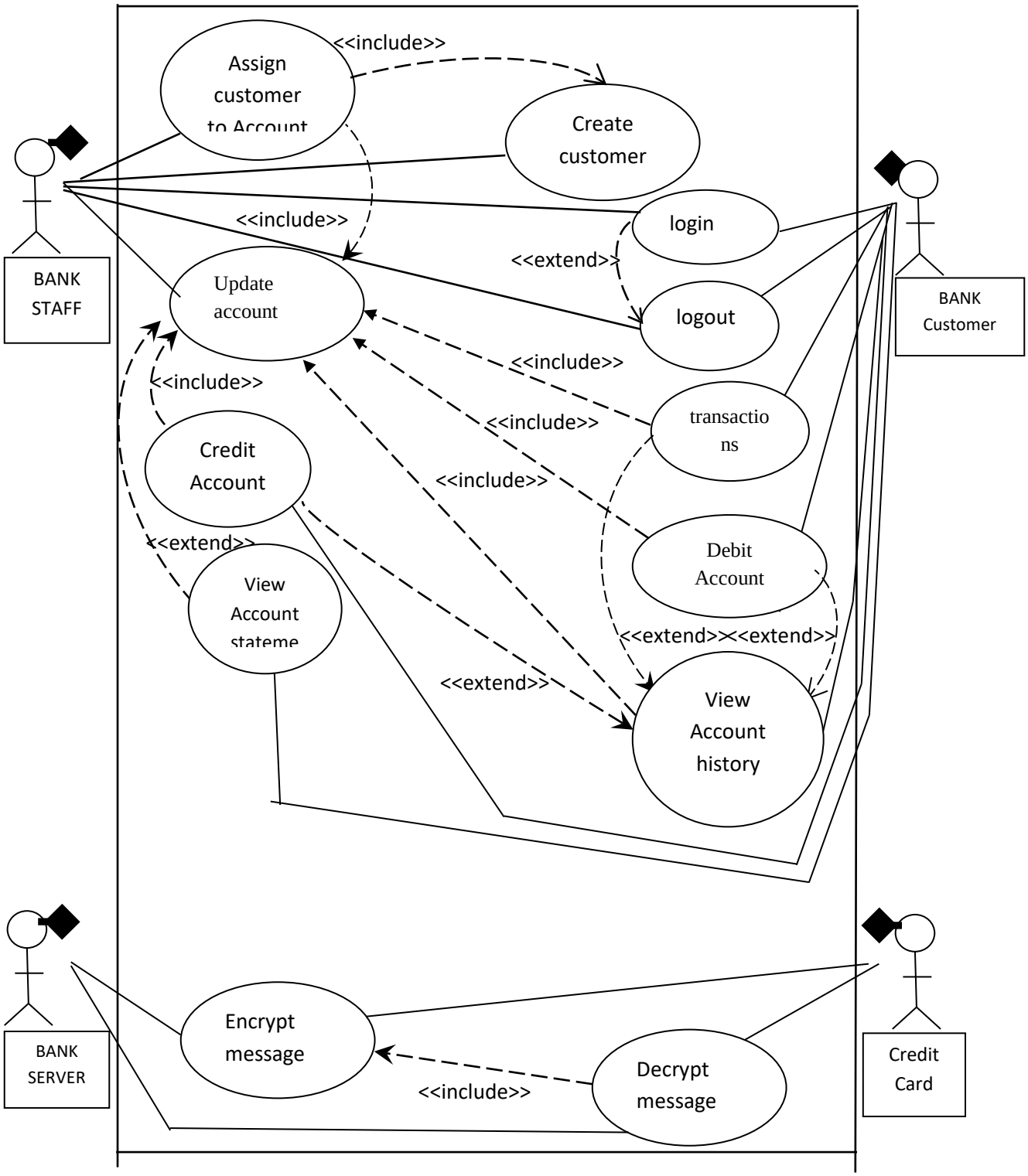


Fig. 3.10: Use Case Diagram of the New System

3.2.2.3 Justification of the New System

The new system will help to solve the problems inherent in the existing system by providing more secured credit card transactions using adaptive data mining and multi- agents for the fraud detection.

a. The model will maintain the database in which users transaction behaviors and spending patterns are saved.
b. The model will produce a better true positive since it will be the combination of recent credit card fraud techniques and user account transaction database to form an agent.
c. The model raises alarms if unusual transaction is observed at agent stage.
d. The security will be maintained and transaction secured from fraud.
e. The speed of fraud detection is high to compared with existing model (HMM, ANN etc.).Once fraud detection is enhanced in the financial institutions, people's confidence in online transactions will increase and thereby reduce the stress of using fiscal cash for every transaction. This justifies the need for the new system.

3.2.2.4 High-Level Model of the New System

Fig. 3.11 shows the high level model of the new system. It shows that there are two active players in the system; the bank staff and the credit card user. Their actions on the system are separated as show in the model.

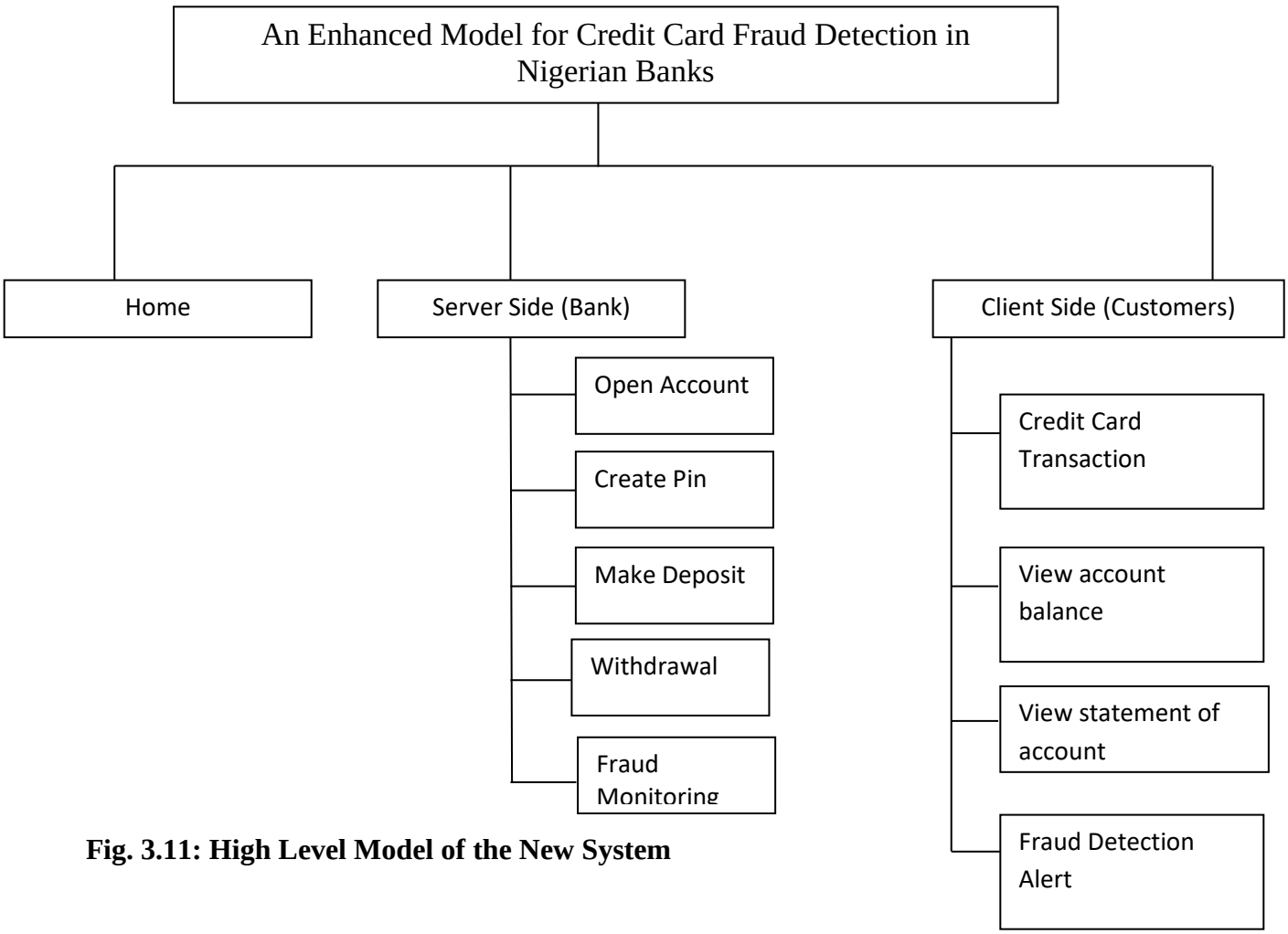


Fig. 3.11: High Level Model of the New System

CHAPTER FOUR

SYSTEM DESIGN AND IMPLEMENTATION

4.1 Objectives of the Design

a. To provide easy and well security to online transactions

b. To provide a proactive way of blocking or prevent human based frauds

c. To classify alarms generated by the system to help the experts to focus on the real dangerous ones.

d. To demonstrate an alert notification to the key system (customer database and credit card) on any suspicious transactions on the credit process during runtime.

4.2 Main menu/ Control Centre

The main menu contains the modules on the credit card fraud detection system. Each module has its class based on the three classes; system admin, bank staff and customers. Access to the system is controlled through the user password; which now determines what the user can have access to on the system. This is shown in Fig. 4.1.

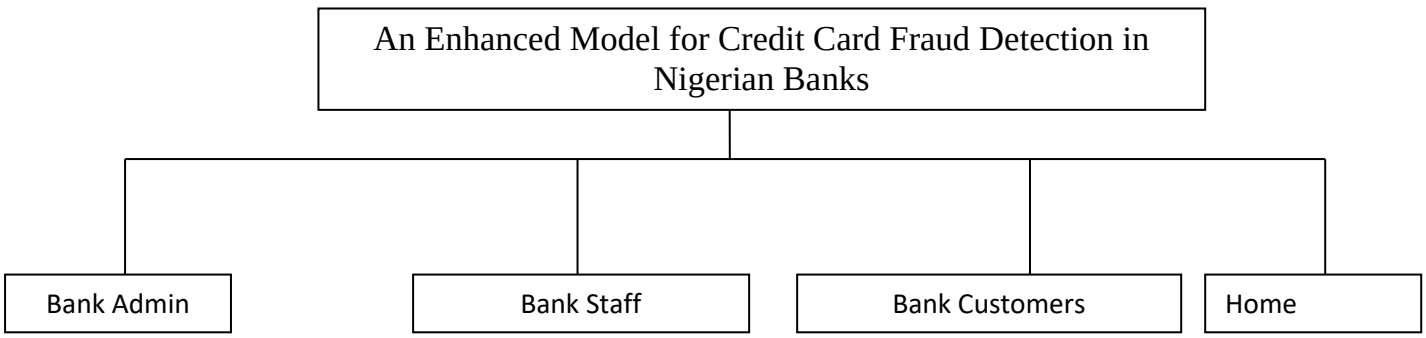


Fig. 4.1: Main menu

4.3 Submenus/Subsystems

The credit card fraud detection system was divided into sub systems. It was designed using Top –Down Approach. The system is structured in a way that each subsystem is accessed from the main menu and executed independently. The sub menus / sub systems are as follows:

4.3.1 Home Sub System

This subsystem as show in Fig 4.2 is the first interface the user encounters which using the software designed. It allows user to have access to admin or customers login forms. The sub system also contains information about the developer of the application and the exit button for exiting the system. Table 4.1 describes the privileges of Homepage.

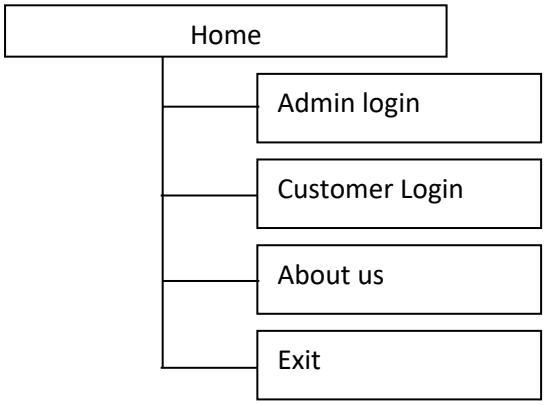


Fig. 4.2: Homepage Sub system Design

Table 4.1: Privileges of Homepage

S/N	Privileges	Description
1.	Admin Login	This module enables the admin to login
2.	Customer Login	This module enables the customer to login.

4.3.2 Admin Sub System

Fig. 4.3 which is the admin sub system is accessible by system administrator. The administrator has access to perform all the operation under this module. Managing credit card pin, fraud alert database, transaction database and users access control. Table 4.2 describes the privileges of the Bank Administrator.

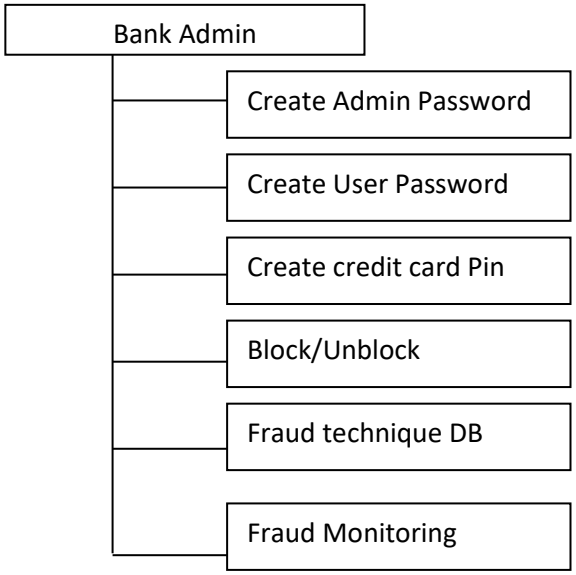


Fig.4.3: System Admin sub system

Tables 4.2: Privileges of Bank Administrator

S/N	Privileges	Description
1.	Create admin password	This is to create admin password
2.	Create user password	This module enables the administrator to create user password.
3.	Create credit card pin	This enables the administrator to create credit card pins for the user.
4.	Block / Unblock	This enables the administrator block any suspected account and unblock customers account.
5.	Fraud techniques	This module enables the administrator to trace fraudulent activities.
6.	Fraud monitoring	This module enables the administrator to monitor fraud activities.

4.3.3 Bank Staff Sub System

Bank staff sub system as show in Fig. 4.4 allows the bank staff to perform the normal banking operation of opening account for the staff, posting cash deposit and withdrawal, printing customers' bank statement. Table 4.3 describes the privileges of the Bank staff.

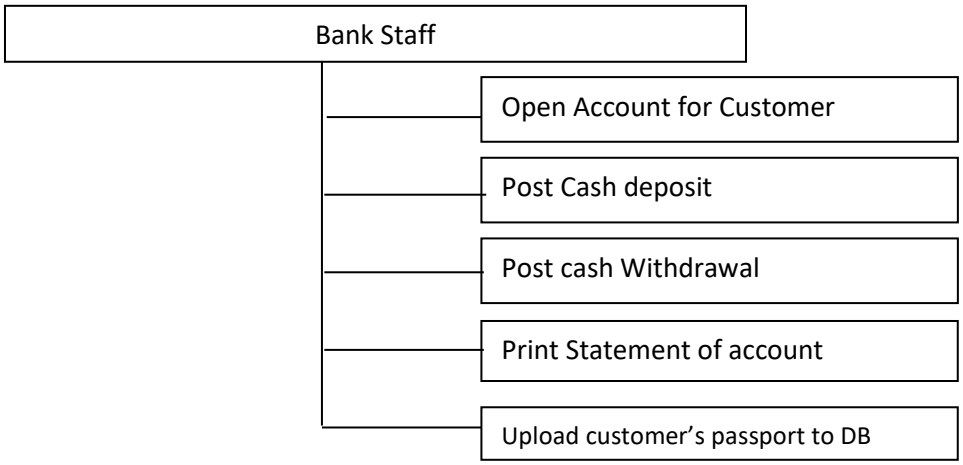


Fig. 4.4: Bank Staff Sub System

Table 4.3: Privileges of the Bank Staff

S/N	Privileges	Description
1.	Open account for customer	Bank staff can use this module to open account for customer.
2.	Post cash deposit	Bank staff can use this module to post cash deposit for customer
3.	Post cash withdrawal	Bank staff can use this module to post cash withdrawal for customer.
4.	Print statement of account	Bank staff can use this module to print statement of account for customer.
5.	Upload customer's passport to database	Bank staff can use this module to upload customer's passport to database.

4.3.4 Bank Customers Sub System

Fig 4.5 is the client side sub system and is accessible by bank customers. To access the sub system, the customer must have account with the bank which then gives room for the customer to obtain the account no, credit card pin and user password which is necessary for the user to have access to this sub system. The user can perform credit card transactions, check account

balance, view statement of account, and also view fraud detection alerts. Table 4.4 describes the privileges of Bank customers.

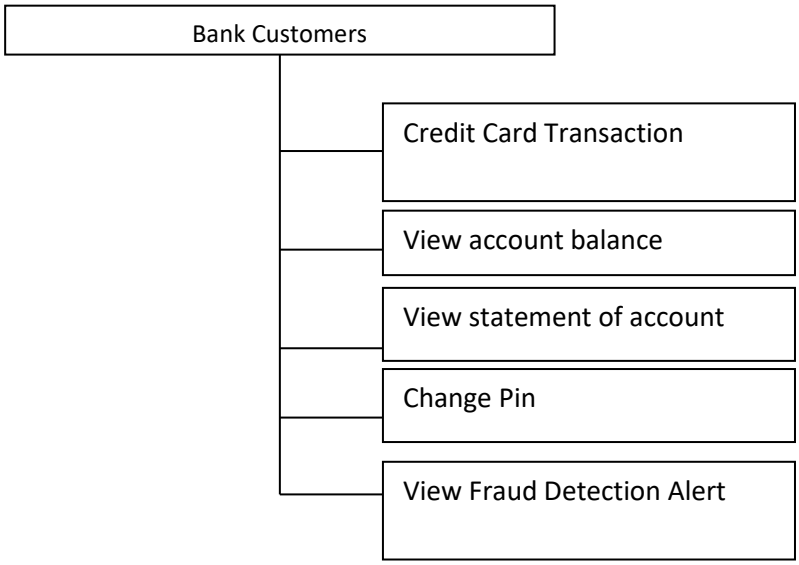


Fig. 4.5: Bank Customers Sub System

Table 4.4: Privileges of Bank Customers

S/N	Privileges	Description
1.	Credit card transaction	This module enables the user to make and complete credit card transaction
2.	View account balance	This module enables the user to view account balance
3.	View statement of account	This will enable the user to view all transaction (completed and pending transactions).
4.	Change Pin	This will enables the user to change pin
5.	View fraud detection alert	This will enable the user to view fraud detection alert.

4.4 System Specifications

4.4.1 Database Development Tool

A relational database design was used to design the database. A relational database management system (RDBMS) is an excellent tool for organizing large amount of data and defining the relationship between the datasets in a consistent and understandable way. A RDBMS provides a structure which is flexible enough to accommodate almost any kind of data. Relationships between the tables were defined by creating special columns (keys), which

contain the same set of values in each table. The tables can be joined in different combinations to extract the needed data using data mining. A RDBMS also offered flexibility that enabled redesign and regeneration of reports from the database without need to re-enter the data. Data dictionaries were used to provide definitions of the data used; these included the final data structures for the various tables and their corresponding data fields, description and sizes. The user application programs and interface were developed using PHP with support of structured query language (SQL) and MySQL Database.

4.4.2 Database Design and Structure

Creation of a database involves determining the name of the database, and the tables used to store data in that database. The following tables, data types, and data sizes were used in the design of the databases using MySQL database. The structure of the tables in the database includes:

a. Admin Table.
b. Customer Account Master Table.
c. Credit card Pin Table.
d. Fraud Alert Table.
e. Account transaction Table.

Table 4.5: Admin Login Table Structure

S/N0.	Field	Data Type(Size)	Description
1.	Username	Varchar (20)	The Username of the Admin.
2.	Password	Varchar (20)	The password of the Admin.

Table 4.6: Customers Account information Table Structure

S/N0.	Field	Data Type(Size)	Description
1.	Surname	Varchar (15)	The username of the customer
2.	Firstname	Varchar (15)	The first name of the customer
3.	Type	Varchar (20)	The type of the customer
4.	Phone	Varchar (11)	The phone number of the customer
5.	Email	Varchar (20)	The Email address of the customer
6.	Transdate	Date (8)	The transaction date of the customer

7.	Amount	Float (12.2)	Opening amount of the customer
8.	AccountNo.	Varchar (20)	The account number of the customer
9.	Address	Varchar (40)	The address of the customer
10.	Nextofname	Varchar (30)	The name of next kin of the customer
11.	Nextphone	Varchar (11)	The phone of next kin of the customer
12.	Nextaddress	Varchar (100)	The address of next kin of the customer
13.	Card No.	Varchar (20)	The card number of the customer

Table 4.7: User Pin Table Structure

S/N0.	Field	Data Type(Size)	Description
1.	Pin	Varchar (12)	The pin number of the customer
2.	Account No	Varchar (12)	The account number of the customer

Table 4.8: Fraud Alert Table Structure

S/N0.	Field	Data Type(Size)	Description
1.	Account no	Varchar (12)	The account number of the customer
2.	Amount	Float (12)	The amount of the transaction of the customer
3.	TransDate	Date (8)	The date of the transaction date of the customer
4.	Transtime	Varchar (10)	The time of the transaction of the customer

Table 4.9: Transactions Table Structure

S/N0.	Field	Data Type(Size)	Description
1.	Sn	Int (4)	The transaction serial number of the customer
2.	AccName	Varchar (20)	The account name of the transaction of the customer
3.	AccNo.	Varchar (20)	The account number of transaction of the customer
4.	DR	Float (12)	The database report transaction of the customer
5.	CR	Float (12)	The credit card report of the customer
6.	Date	Date (8)	The date of the transaction of the customer
7.	Balance	Float (12)	The balance of the transaction of the customer

Table 4.10: Table of agents, what they are doing and the existing algorithms they are using to do their job.

S/N	Agents	Function	Existing Algorithm
1	Diagnosing agent	Classification	Fuzzy Logic
2	Monitoring Agent	Build transaction pattern	HMM
3	Collating Agent	Data retrieval	Data mining
4	Reporting Agent	Reports the transaction status	SMS
5	User Agent	Takes action	Encryption Algorithm

4.4.3 Mathematical Specifications

The application verifies customers account balance before every transaction is completed. The system compares account balance with the transaction amount in cases of withdrawal or cash transfer. Below are some of the mathematical specifications.

Withdrawal Transaction

If the account balance is less than withdrawal amount then

Deny access to the transaction

Else

Account balance = account balance – transaction amount

End if

Deposit Transaction

Account balance = account balance + transaction amount.

4.4.4 Program Module Specification

The software is structured in such a way that each subsystem is selected and executed independently. The task is divided into several modules, which come together to give the solution to the problem. The modules are as follows:

1. **New Account:** In this module, the customer gives there information to enroll a new account with the bank. The information is all about their contact details. They can change their own login and password for their future use of the credit card.
2. **Login:** In Login Form module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on website. Which additional resources they will have access to can be configured separately.

3. **Security information:** In Security information module it will get the information detail and its store's in database. If the transaction is suspected to be fraudulent then the Security information module form arises. It has a set of question where the user has to answer the correctly to move to the transaction section. It contain informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to user, secure, search, process, and exchange personal and/or confidential information.
4. **Transaction:** The method and apparatus for pre-authorizing transactions includes providing a communications device to a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that characterizes a specific transaction to be made by an authorized user of the credit card at a later time. The information is accepted as "network data" in the data base only if a correct personal identification code (PIC) is used with the communication. The "network data" will serve to later authorize that specific transaction. The credit card owner or other authorized user can then only make that specific transaction with the credit card.
5. **Verification:** Verification information is provided with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party. In verification the process will seeks card number and if the card number is correct the relevant process will be executed. If the number is wrong and the user tried it three times, mail will be sent to the user saying the card no has been block and he can't do the further transaction.
6. **Deposit Module:** This module is used to credit customers account through bank transaction. This is done in the banking hall.
7. **Withdrawal Module:** The module debits customers account. The basic requirement for this is customers account no and signature.
8. **Statement of Account:** This module enables the user to view account statement of the customer.

4.4.5 Input/output Format

The lists of input forms that are available for the users to use in this new system include:

a. Login specification
b. Customer login form
c. Account opening form
d. Customer's picture uploads form
e. Customer cash deposit form
f. Cash withdrawal form
g. Customer account pin verification form
h. Customer transaction profiling form
i. Credit card details verification form
j. Account statement form
k. Fraud transaction alert form

Login Form

Fig. 4.6 contains the login specification for bank staffs which includes the username and the password. Once the specification is entered, clicking on the login button will validate the data before launching the user on the staff sub system.

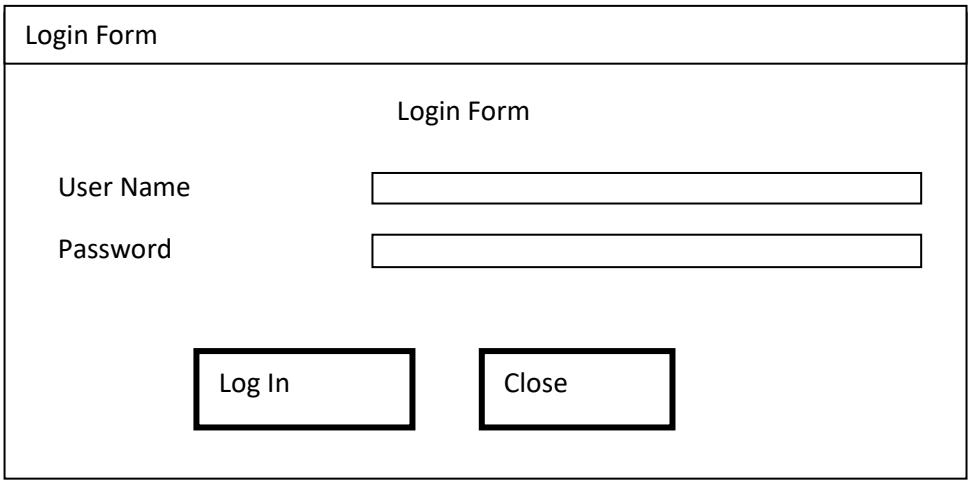


Fig. 4.6: Login Form

Customer Login form

Fig. 4.7 contains the login specification for bank customers which includes the account no and the pin code. Once the specification is entered, clicking on the login button will validate the data before launching the user on the customers sub system.

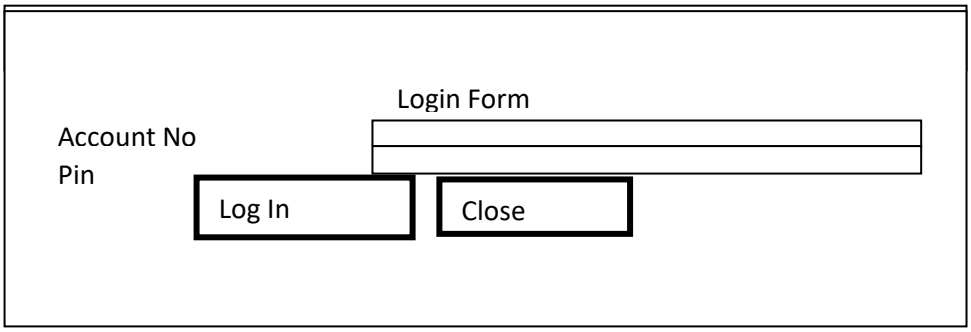


Fig. 4.7: Customer Login form

Account Opening Form

This form is used to open new account for a customer in the bank. The specifications as contained in the form in Fig. 4.8 must be fully entered.

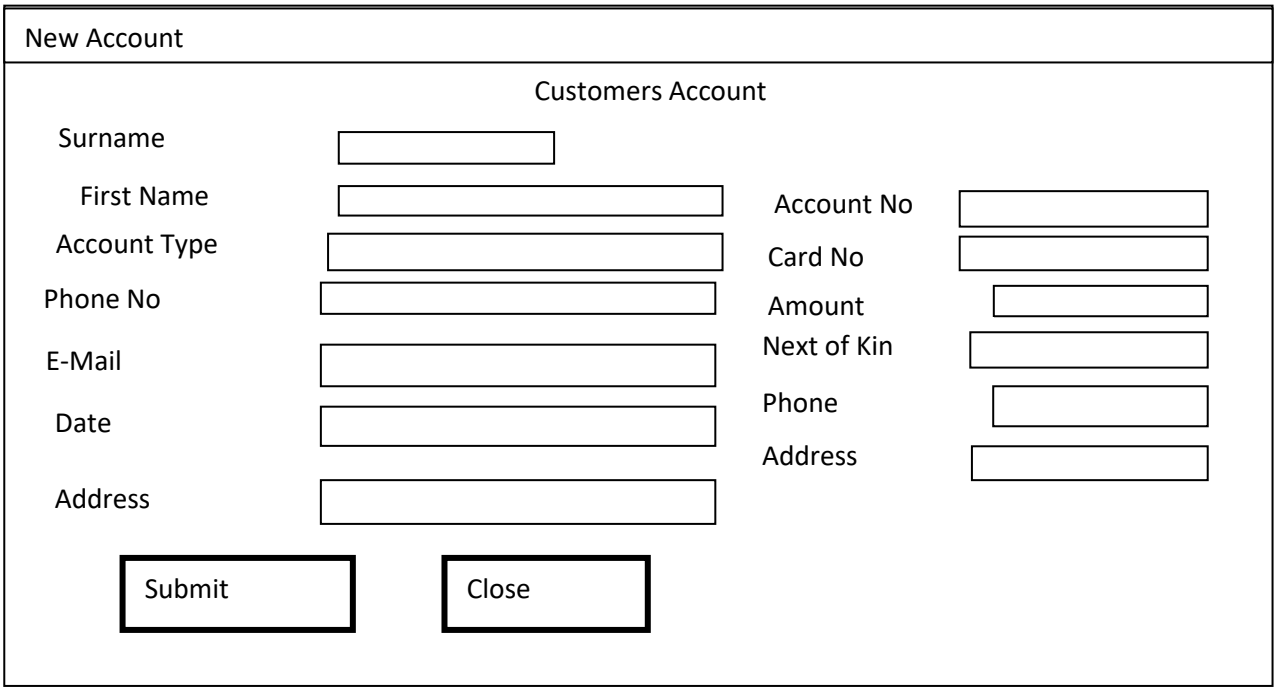


Fig. 4.9 requires the entry of customer's account no and picture scan. Once the specifications entered, click on the upload button to upload the picture to the database server.

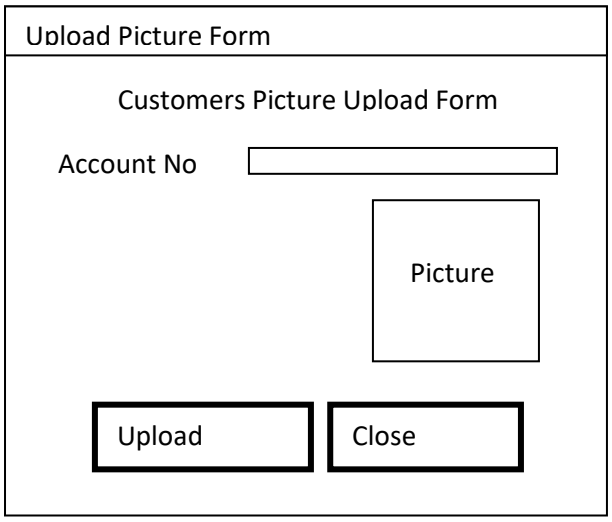


Fig. 4.9: Customer's Picture Upload Form

Customer Cash Deposit Form

This form is used to enter customers deposit in the bank. It is required that the fields specified on the form must be entered for the transaction to be submitted. Figure 4.10 contains customer cash deposit form such as deposit details and customer cash deposit form.

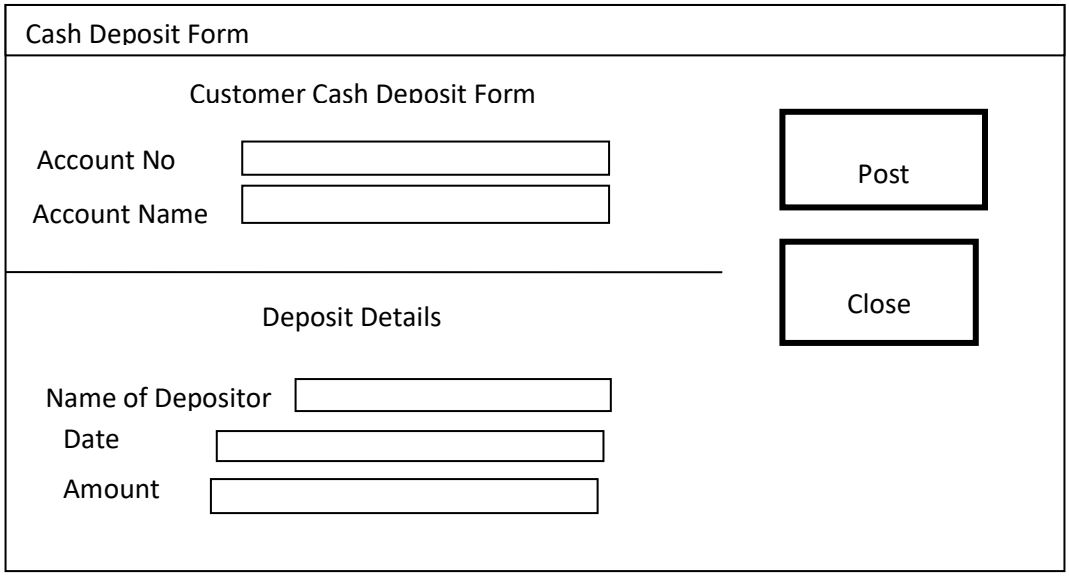


Fig. 4.10: Customer Cash Deposit Form

Cash Withdrawal Form

This form is used to enter withdrawal details of customer transaction in the bank. Figure 4.11 contains cash withdrawal and withdrawal details.

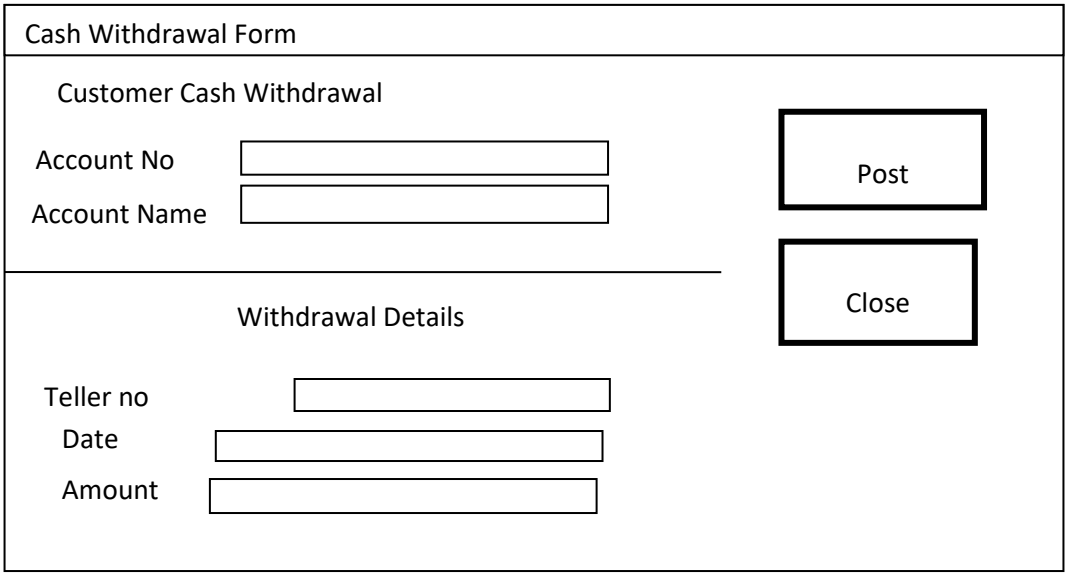


Fig. 4.11: Cash Withdrawal Form

Customer Account pin verification Form

Fig. 4.12 contains the account pin specification for bank customers which includes the account no and the pin code. Once the specification is entered, clicking on the verify button will perform the authentication by validate the data before launching the customer to second form.

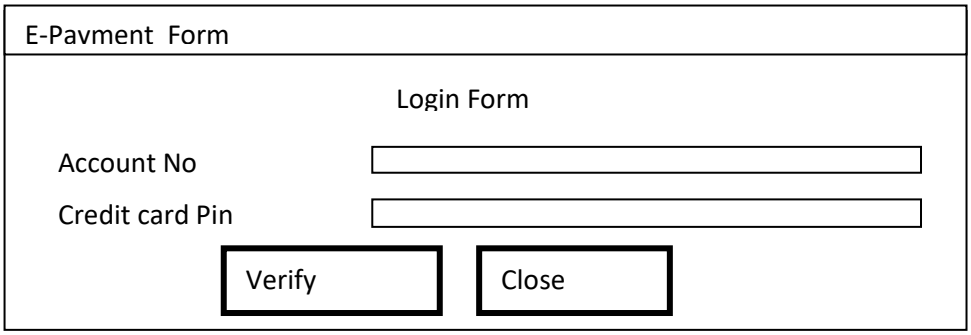


Fig. 4.12: Customer Account pin verification Form

Customer Transaction profiling Form

Fig. 4.13 captures the transaction amount and then the multi-agents will use the data mining to collect customers profile and diagnosis agent will diagnose the transaction based on the profile and then pass then information to reporting agent.

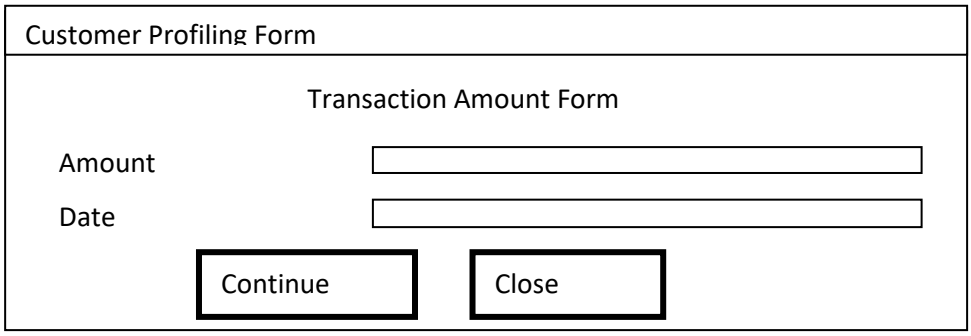


Fig 4.13: Customer Transaction profiling Form

Credit card details verification form

The specification in Fig. 4.14 below must be completed and verified before the transfer can go through.

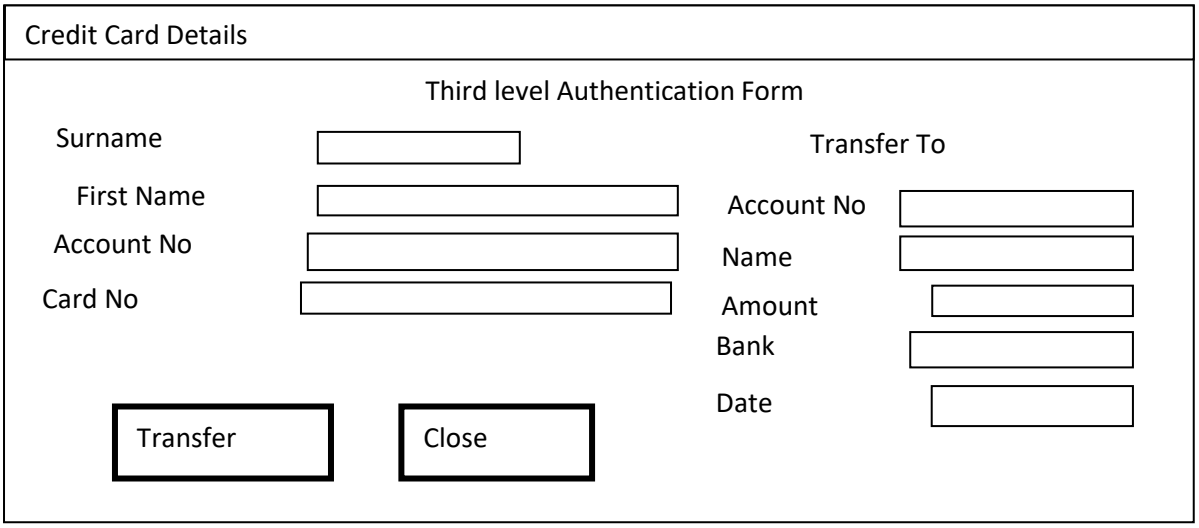


Fig. 4.14: Credit card details verification form

Account Statement

Fig. 4.15 displays all the customers' transaction details in a statement of account format.

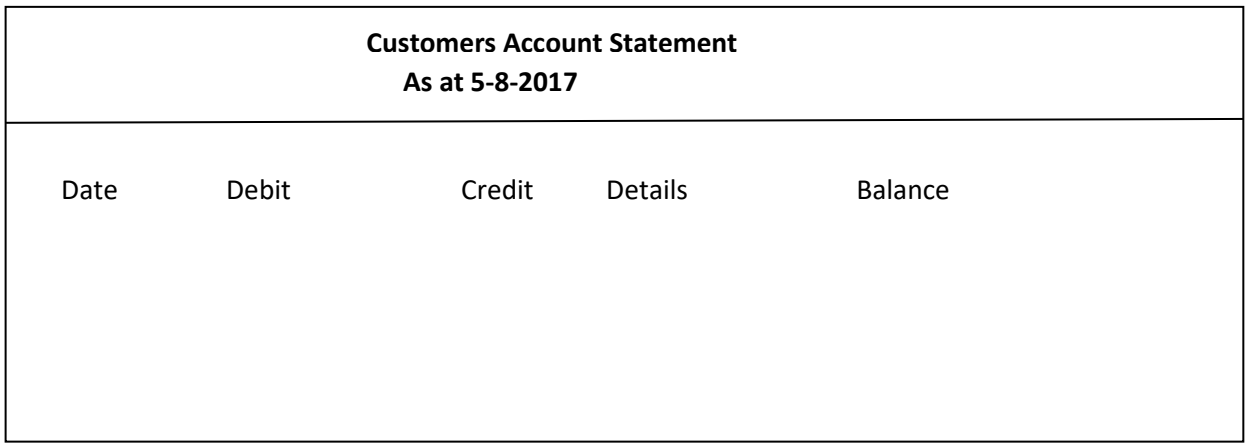


Fig.4.15: Account Statement

Fraud Transaction Alert

Fig. 4.16: contain fraud transaction alert such as: Date, Amount, Account N0., and Action Taken.

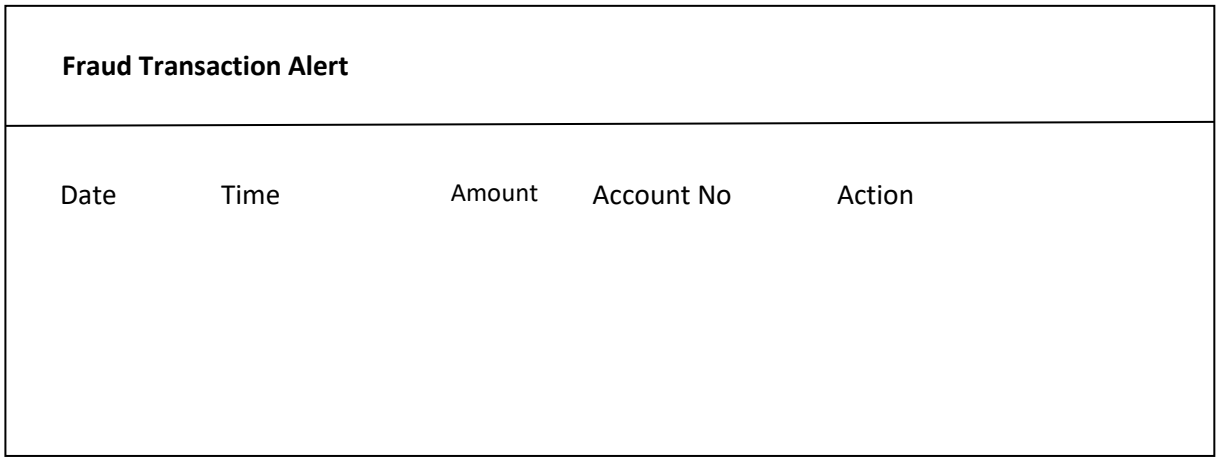


Fig 4.16: Fraud Transaction Alert

4.4.6 Machine Learning (Expert Driven Approach) Algorithm

Given:

Accts: set of all accounts

Rules: set of all fraud rules generated from Accts

Input Phase: user inputs the credit card transaction details

User posts into core system and transaction is stored into the daily transactions table

Monitoring Agent captures the Account Number being posted

Monitoring Agent passes the number to diagnosing agent

Diagnosing agent check on rule set against the Account number received

Training Phase: Cluster creation

STEP 1: To Identify the profile of cardholder from their purchasing

STEP 2: The probability calculation depends on the amount of time that has elapsed since entry into the current state.

STEP 3: To construct the training sequence for training model

1. /*Initialization*/
2. S = { };
3. for (a ∈ Accts) do Cover[a] = 0;
4. for (r ∈ Rules) do
5. Occur[r] = 0; /*Number of accounts in which r occurs*/
6. AcctsGen[r] = { }; /*Set of accounts generating r */
7. end for
8. Check the previous spending profile
9. for (a ∈ Accts) do
10. Ra = set of rules generated from a;
11. for (r ∈ Ra) do
12. Occur[r] : = Occur[r] + 1;
13. add a to AcctsGen[r];
14. end for; end for
15. if transaction is outside spending profile the send alert to diagnosing agent
16. for (a ∈ Accts) do
17. Ra = secret questions;
18. request for user to supply secret question and answer
19. while (cover[a] <Trules) do
20. r := correct from Ra
21. Remove r from Ra
22. if (r ∉ S and Occur[r] ≥ Taccts) then
23. add r to S;
24. for (a2 ∈AcctsGen[r]) do
25. Cover[a2] = Cover[a2] + 1;
26. end for; end if
27. end while; end for

Monitoring agents report to data collating agent if any rule is broken

Collating agent will send it to diagnosing agent for further authentication

Reporting agent send fraud alert received to the user agent

Monitoring Agent supervised by manager or rollback the transaction before being committed to database

Detection Phase: Fraud detection

STEP 1: To Generate the observation symbol

STEP 2: To form new sequence by adding in existing sequence

STEP 3: To calculate the probability difference and test the result with training phase

STEP 4: Finally, If both are same it will be a normal customer else there will be fraud signal will be provided.

The Algorithm for Adaptive fraud detection as show above depict the steps in credit card fraud detection as implemented in this dissertation.

4.4.7 Data Dictionary

Tables 4.11 are some of the data variables used in the program design and their full meaning.

Table 4.11: Data Dictionary

Variables	**Meaning/Functions**
Db	This is the database object used to access and transact with the banking database
Rset	This is the result of set object used by the database object to hold records returned from the database
Conn	This is the connection object used by the database object to connect to the physical database
mnuRecord	This is the object used to display the Record menu
mnuRecord	This is the object used to display Report menu
mnuChangePass	This is the object used to change password of user
mnuUserManager	This object is used to manage the user of the system

mnuLogin	This is the object that gives access to authorized users of the system
mnuPhone	This is the object used to display the phone number menu
mnuAccount N0.	This is the object used to display the Account Number menu
mnuCard N0.	This is the object used to display the card number menu
mnuAmount	This is the object used to display the account transaction amount menu
mnuEmail	This is the object used to display the E-mail menu.
mnuExit	This is the object used to exit the application
LoadPicture	This is the object that helps in loading pictures /images from the directories into the program.
LoadTemplate	This is the object that helps in loading photo (image) template from the directories into the program.

4.5 System Flow Diagram of Credit Card Transactions

The system flow diagram of the new system is shown in Fig. 4.17.

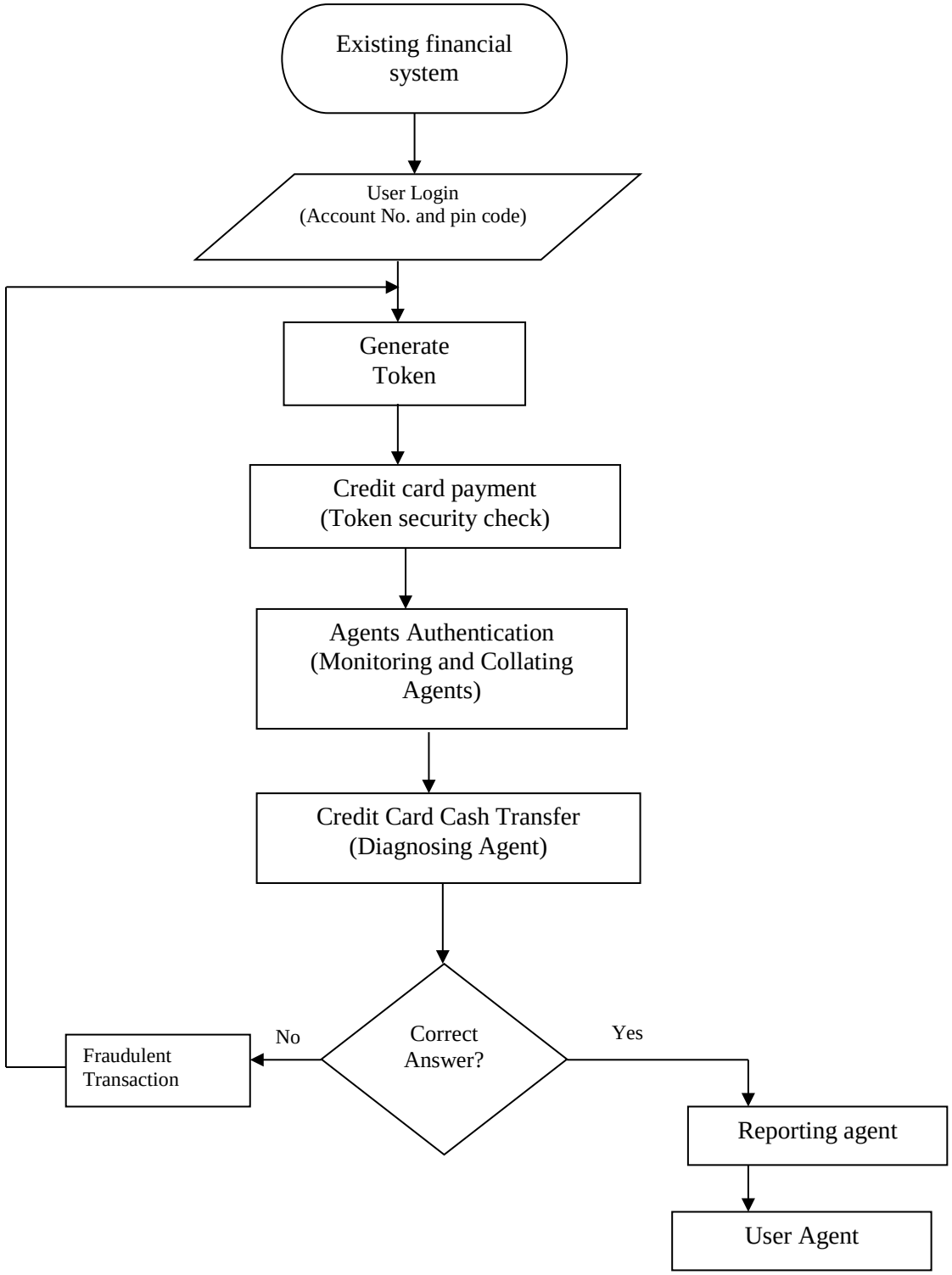


Fig. 4.17: System Flowchart of Credit Card Transactions

4.6 Object Diagrams

4.6.1 Sequence Diagram of the Credit Card Transactions

Figure 4.18 contains the following below:

New Credit card: Given Input- Request from the user for the card. Expected Output-Assigning an account to requested user.

Login: Given Input- Give username and password of particular user.

Expected Output- Login to user's account.

Security information: Given Input- Give the security information by answering security questions. Expected Output-Update of account with the security details.

Transaction: Given Input- Give the credit card details and performs transaction.

Expected Output- Update database.

Verification: Given Input- Checks with user's stored details like security answers or previous spending profile.

Expected Output-If the verification is success, user can perform transaction, else blocks the card.

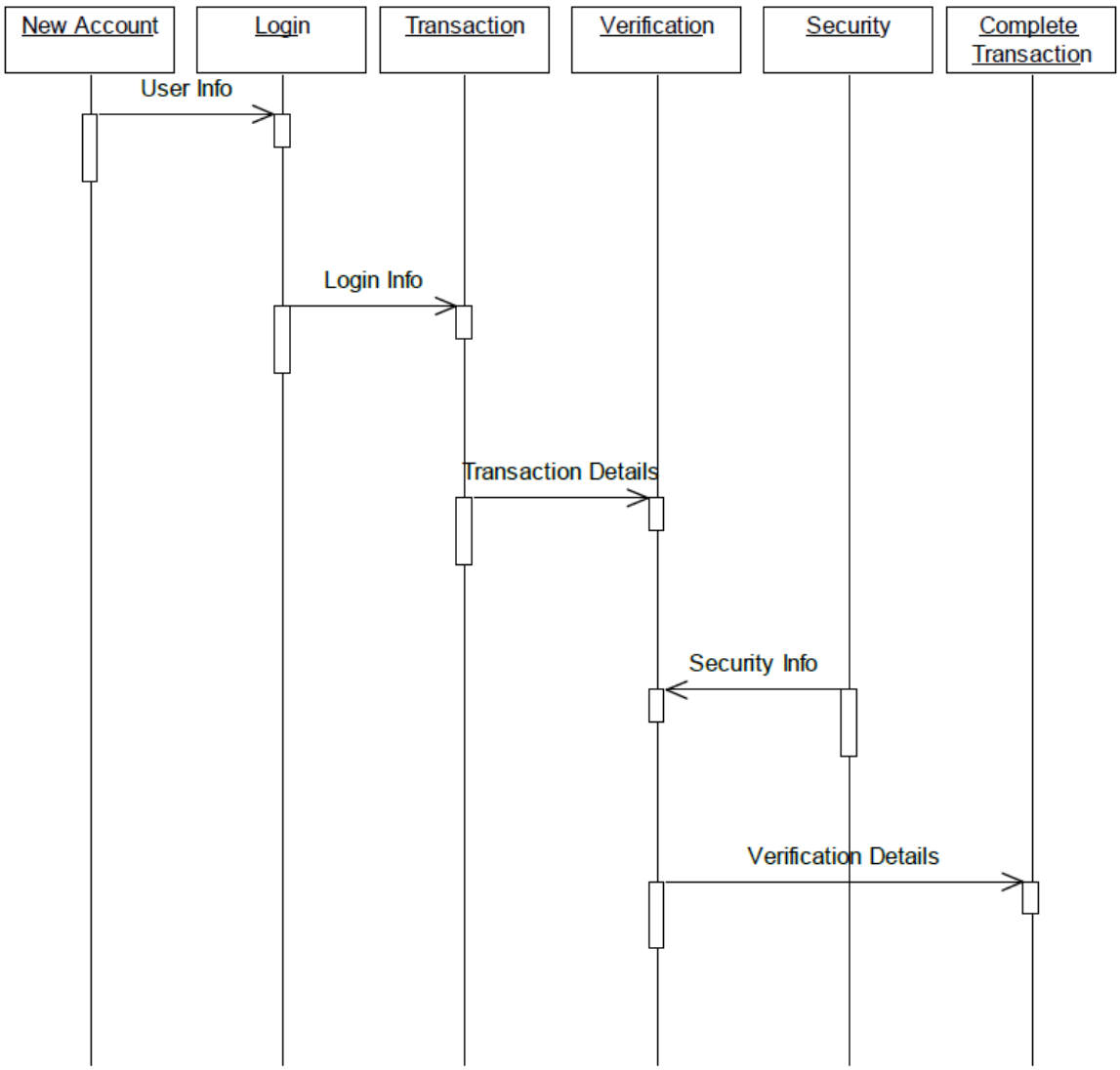


Fig. 4.18: Sequence Diagram of Credit Card Transactions

4.6.1.1 Sequence Diagram of the New System

Fraud Management Filters checks for payment characteristics that may indicate fraudulent activity. Fig. 4.19 set up Fraud detection Filters to provide the tightest control possible over payments so that you can deny payments that are likely to result in fraudulent transactions and accept payments that are not typically a problem. The customer initiates the online payment transactions, the multi-agents verifies the customers previous spending profile through the use of data mining and confirms the payment where the profile not suspicious otherwise the transaction is blocked. The bank processes the payment.

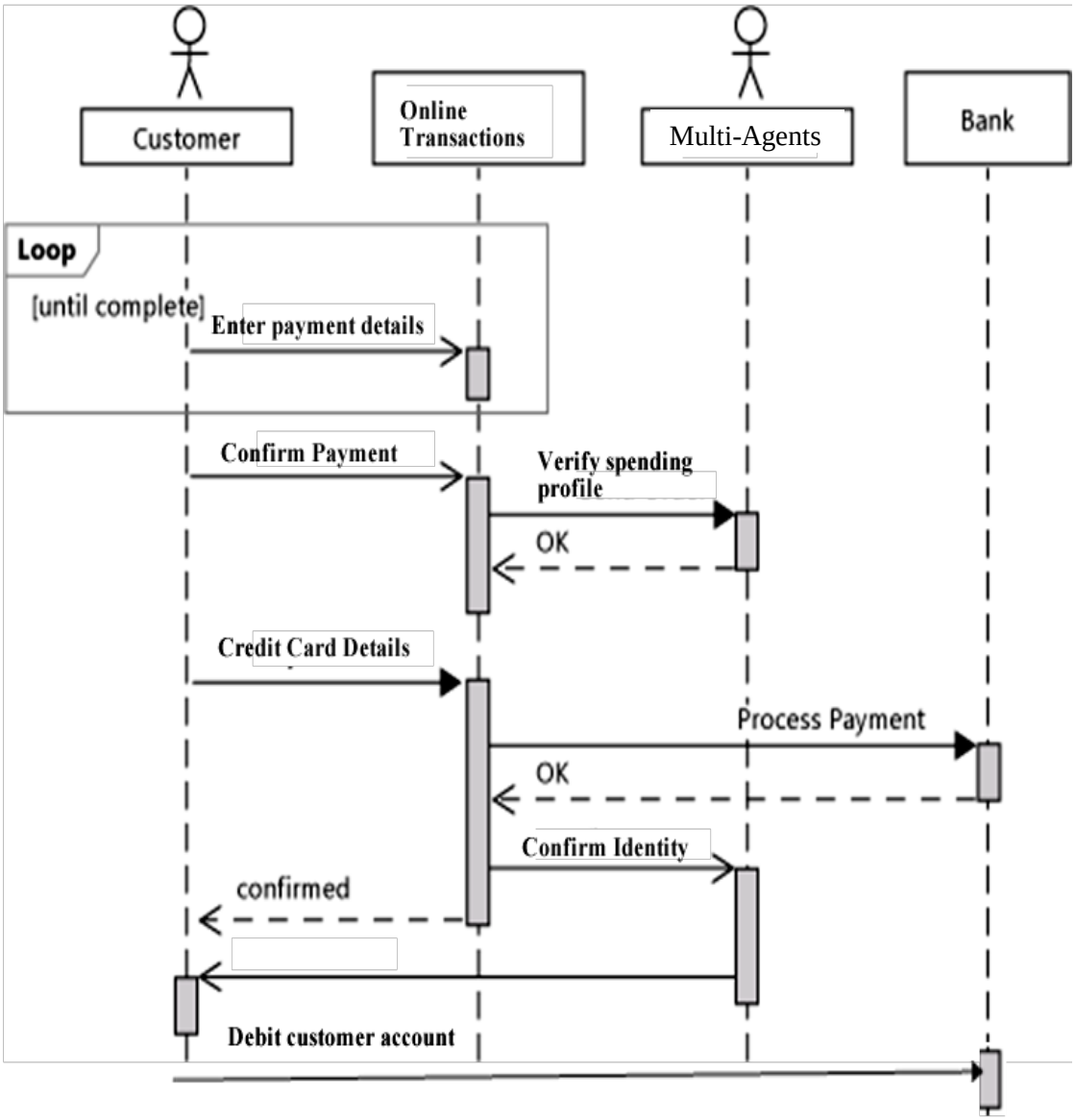


Fig. 4.19: Sequence Diagram of the New System

4.6.2 State Diagram of Credit Card Transactions

Fig. 4.20 shows the four states of the transactions. First the credit card user makes request for to use the credit card platform, provide credit card information and login. Then finally complete the transaction.

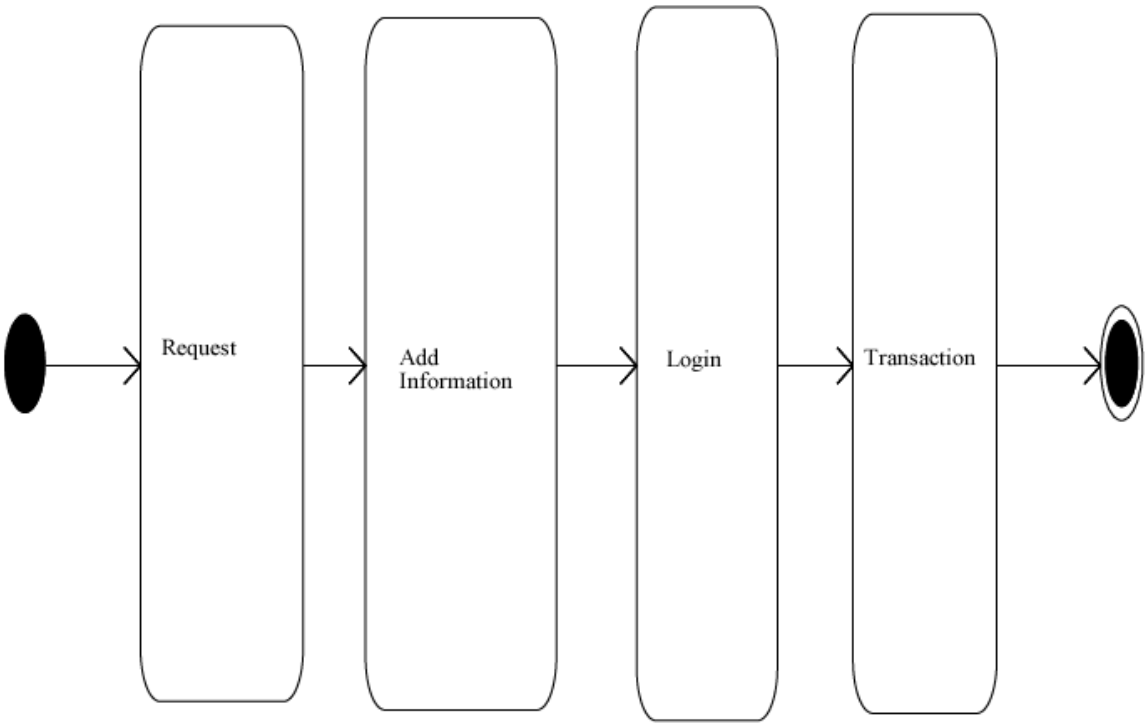


Fig. 4.20: State Diagram of Credit Card Transactions

4.6.3 Activity Diagram of the Credit Card Fraud Detection System

Fig. 4.21 shows the various processes that lead to credit card transactions. It starts with opening a credit card account, making purchase online, effecting payment with your credit card which will be verified before the transaction is completed.

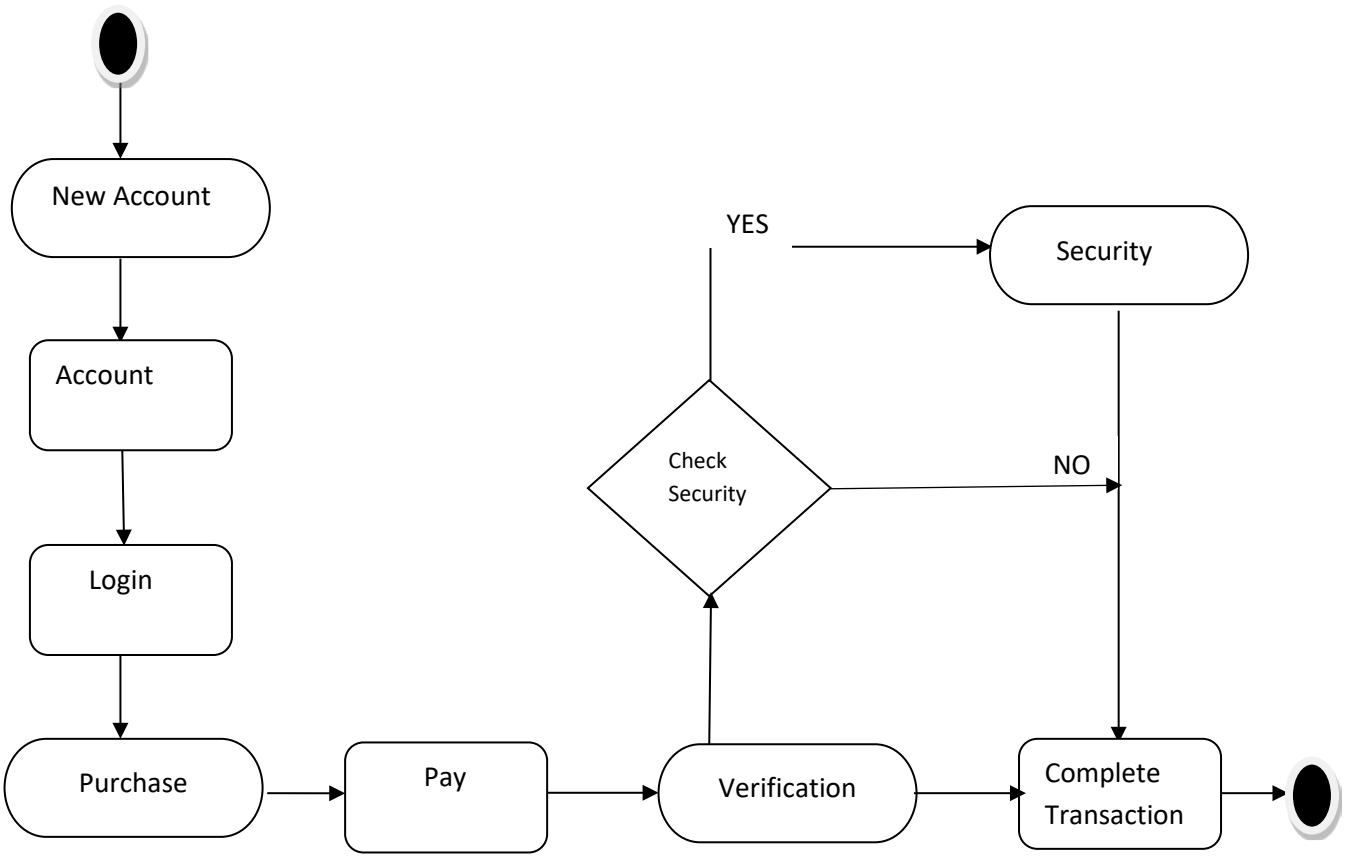


Fig. 4.21: Activity Diagram of Credit Card Transactions

4.6.4 Collaboration Diagram of Credit Card Transaction

Fig. 4.22 shows the various information that needed at each stage of the credit card transactions.

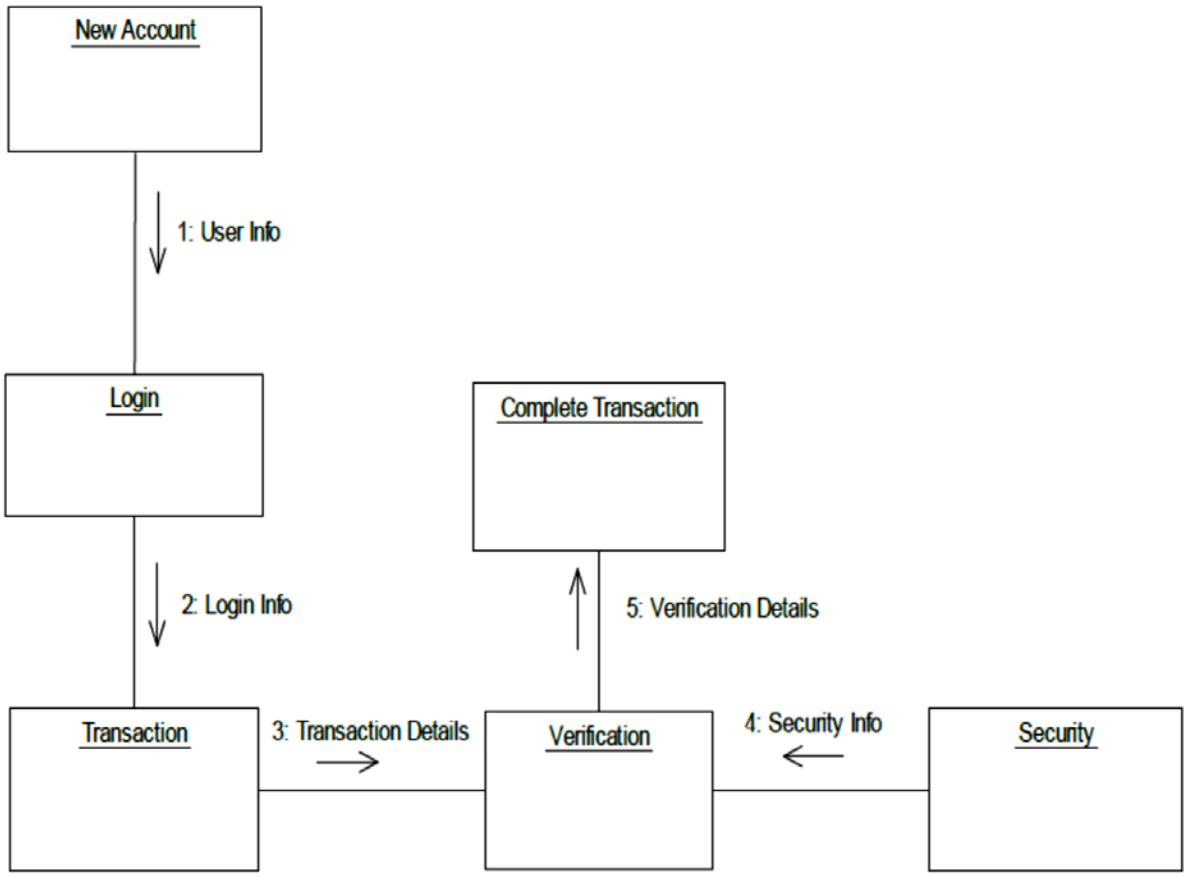


Fig. 4.22: Collaboration Diagram of Credit Card Transactions

4.6.5 Event Package Diagram

The event package diagram as shown in Fig. 4.23 shows the various stages of events in the process of using credit card for payment. It starts with entering the card details which needs to be verified before completing the transaction.

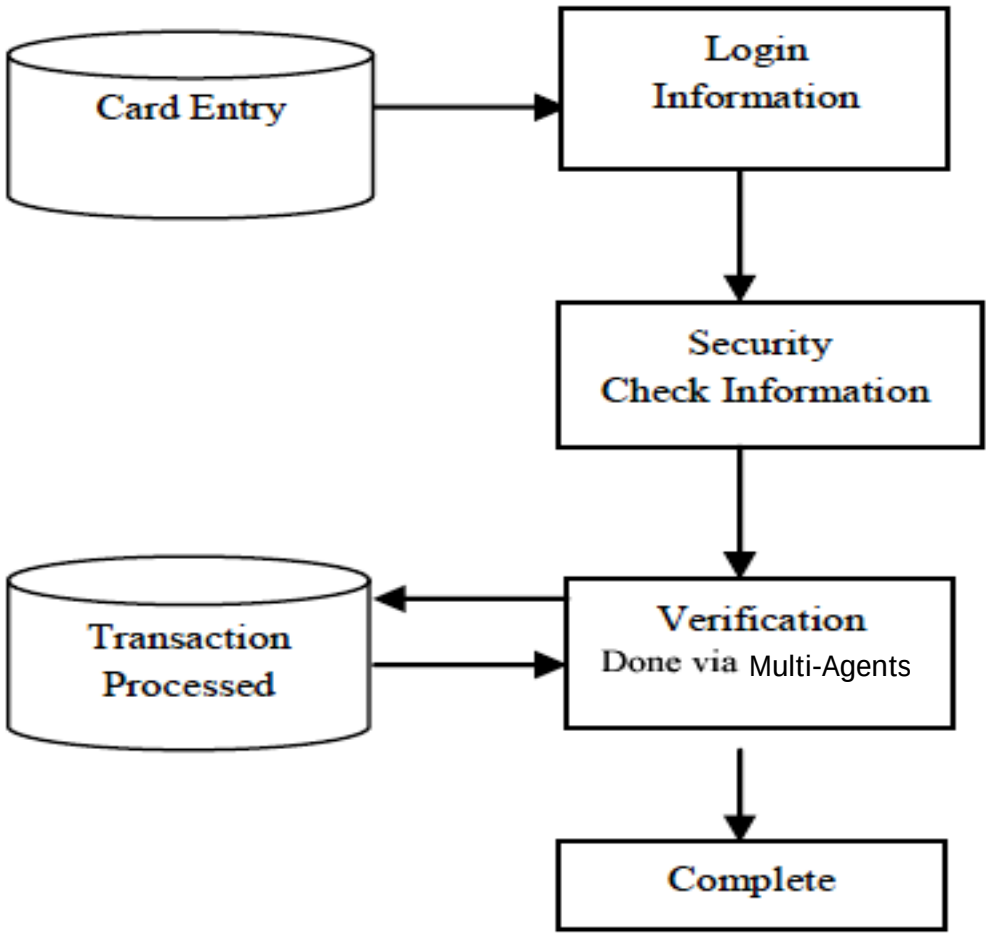


Fig. 4.23: Event Package Diagram of Credit Card Transactions

4.6.6 Class Diagram of the New System

Fig. 4.24 show the database class diagram of the new system. The line shows the associations between the various tables in the database.

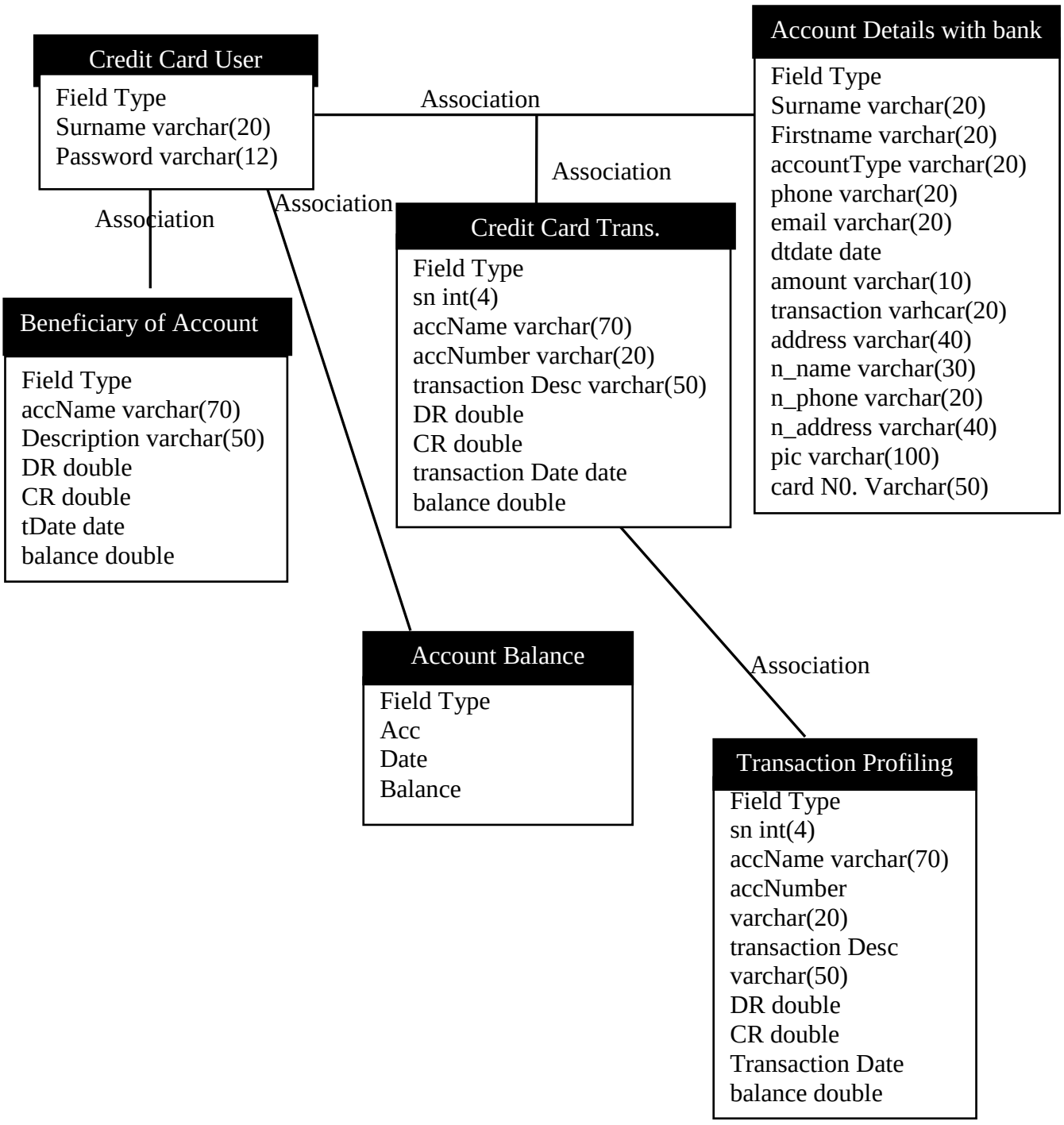


Fig 4.24: Class Diagram of the Credit Card Fraud Detection System

4.6.7 Entity Relationship Diagram of the New System

Entity Relationship diagrams is a specialized graphics that illustrate the interrelationship between entities in a database. Fig 4.25 shows the entity relationship in the database. The diagram above is an entity relationship diagram that is a major data modeling tool that helped database analysts to organize data into entities.

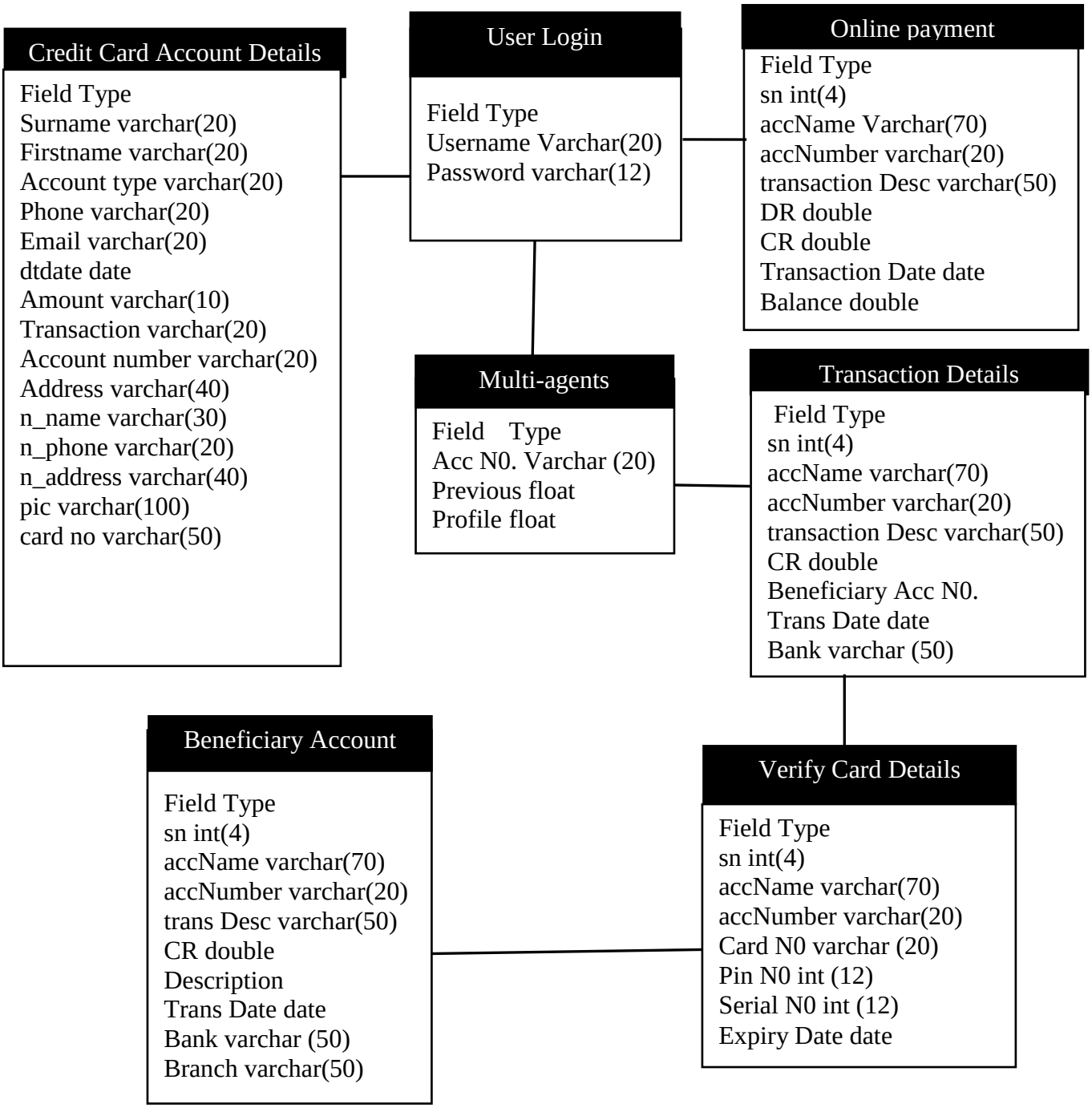


Fig. 4.25: Entity Relationship Diagrams of Credit Card Transactions

4.7 System Implementation

4.7.1 New System Requirements

The computer system is divided into software and hardware. Both works together to achieve the desired goal in any application developed. In the web based security system developed, the following are required.

4.7.1.1 Hardware Requirement

Computer system is made up of units that are put together to work as one in order to achieve a common goal. The requirements for the implementation of the new system are:

a. 2.4 GHZ of Intel Pentium Dual Core processor speed
b. 2GB RAM
c. 80 GB of Hard disk
d. Internet Facility
e. Printer

4.7.1.2 Software Requirement

For the effective implementation of the new system, the following software has to be installed on the computer system.

a. Windows Xp, Windows 2000 , Window 7 or Window 8
b. PHP
c. Java TM
d. Dream Weaver
e. Wamp Server
f. Swish Max
g. Fireworks
h. MySQL

4.7.2 Program Development

4.7.2.1 Choice of Programming Environment

The credit card fraud detection system in Nigerian banks using data mining and multi-agents was developed using a combination of programming frameworks. The Multi-agents component was developed using JADE (Java Agent Development Environment) to capture the transaction account on run time while the user interface is implemented using Java script. The core banking system in stored in a MySQL server and queries to the database were developed in SQL using PHP-MySQL program development platform.

4.7.2.2 Language Justification

The following attributes are the reasons why the new system was implemented using PHP and Java script programming language.

i. PHP and java script programming is done in a graphical environment
ii. Graphical object just needs to be dragged and dropped anywhere on the form and its properties can be changed using the properties window.
iii. Java program is made up of many classes, objects and inheritance, each has its own program code, and each can be executed independently and at the same time each can be linked together in one way or another.
iv. Debugging of the program code can be done independently before integration to the system.

4.7.3 System Testing

System testing is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. In this system testing, test has been done in both Windows 7 and 8 Operating System and it still function effectively.

4.7.3.1 Test Plan

A primary purpose of testing is to detect software failures so that defects may be discovered and corrected. Testing cannot establish that a product functions properly under all conditions but can only establish that it does not function properly under specific conditions. We therefore employed the following testing and debugging method to check for errors in the new system.

i. Unit/Module Testing
ii. Intergrated Testing
iii. Performance Testing

Unit/Module Testing

Unit/Module testing is the testing of the individual unit or group of related units. It is often done to test that the unit is producing expected output against given input. This method shall ensure and confirm the efficiency and reliability of the system. So far, the various units/modules have been tested and each has proved efficient as an entity.

Integration Testing

Integration testing is the testing in which a group of components are combined to produce output and the interaction between software and hardware is also tested. The essence of this intergrations is to check how these modules when they are intergrated into subsystem stand as main system. Therefore, the test carried out here is to ascertain that those modules do not loose their efficiency and reliability (which has been proved in the module testing above) due to the intergration into subsystem and system. The coordination and linking relationship existing between the form and procedure retained and performed the primary function for which they were designed.

Performance Testing

Performance testing is the testing to assess the speed and effectiveness of the system and to make sure it is generating results within a specified time as in performance requirements

4.7.3.2 Test Data

The system was tested using a system prototype where a sub set of the core banking system database was simulated, then users where given an opportunity to suggest various rules for system to check, which were incorporated into the system in the various multi-agents used. The Real time fraud detection system was connected to the simulated database and then users were asked to post transactions against accounts that had predefined conditions set in the simulated database, these predefined conditions included the following:

1. Using Invalid pin code
2. Entering transaction amount outside the users spending profile
3. Entering invalid credit card details
4. Supplying the wrong answer to the secret question

The credit card fraud detection system was checked to see if it detected these transactions as suspicious when users posted into the selected accounts and if it raises an alert and kept a log of the same.

4.7.3.3 Test Results (Actual Test Result versus Expected Test Result)

The credit card fraud detection using data mining and multi- agent was able to monitor and perform real time alert and notification to accounts that had suspicious entries based on the rules set to monitor what would be considered as suspicious as the transactions happen. It also was able to log the information into a log file.

The information on the log file is then made accessible to the user via an interface that the user can use to further analyze the data. The data can be selected by date, grouped by available account number.

Table 4.12: Expected Result vs Actual Result

Module	**Expected Test Result**	**Actual Test Result**
Home Page	Expected to see the page containing links to other modules	The home page displayed platform and contains all the links to the various modules in the credit card fraud detection system
Log In	Expected to see the Log In form so that users can log in.	When clicked on, a form appeared where the necessary details can be entered: username and password for admin, account number and account pin for customers.
New Account opening	When clicked on , it is expected to display the form for entering new account opening details	When the button was clicked on, the system displayed the customer account opening form.
Deposit/withdrawal form	It is expected to allow users to initiate deposit or withdrawal of money	The form allowed the user to enter the account no, transaction amount, date, and post it to the customer's account
Credit card transaction	It is expected to allow customer initiate transfer of money to another account	The customer was able to initiate transfer of money from his/her account to another account
Account Statement	In this module, it is expected to be used to view customers account statement	When you go to this module, the customers statement was displayed
Monitoring agent	It is expected to determine the user's spending profile.	The monitoring agent was able to determine user's spending profile and forward it to collating agent.

Data Collating agent	It is expected to use data mining to extract users previous transactions and send it to diagnosing agent	The data collating agent was able to use data mining technique to extract the data set for the users credit card and forward it to diagnosing agent
Diagnosing agent	It is expected to monitor the transaction and detect fraud where it exists.	The diagnosing agent was able to determine user's spending profile and compare it with the current transaction to determine if it is fraudulent transaction and send it to reporting agent.
Reporting agent	Expected to generate fraud alert where fraud is suspected.	The reporting agent was able to forward an alert to the bank database indicating that the transaction is fraudulent and the account will be blocked

4.7.3.4 Performance Evaluation

The existing credit card fraud detection systems adopted pin or token in detecting credit card fraud. Most of these techniques have their setbacks as access to the credit card details gives room for credit card fraud. Attempt to use two level authentications yielded a better security system. Since the use of one factor or two factors authentication is still prone to security treats. The use of adaptive data mining and multi-agents improves the security of credit card transactions, making it almost impossible for attackers and hackers to perfecting a credit card fraud without specialized aid. In search for improved performance in credit card fraud detection system, data mining and multi- agent can make a significant positive impact by helping to reduce the number of fraud carried out using credit card and even improve overall operating efficiencies.

There are two ways to examine the performance of classifiers:

i. confusion matrix, and

ii. To use a Receiver Operating curve (ROC) graph.

Given a class, *Cj*, and an alert, *ti*, that alert may or may not be assigned to that class while its actual membership may or may not be in that class. With two classes, there are four possible outcomes with the classification as:

i. True positives (legal transaction),

ii. False positives (false alarms),

iii. True negatives (correct rejections), and

iv. False negatives.

False positive occurs if the actual outcome is legal but incorrectly predicted as fraud.

False negative occurs when the actual outcome is fraud but incorrectly predicted as legal.

A confusion matrix, Table 4.13, contains information about actual and predicted classifications.

Performance is evaluated using the data in the matrix.

Table 4.13: Confusion matrix of a model applied to test dataset (Pin)

		Observed	
		Legal	**Fraud**
Predicted	**Legal**	44	15
	Fraud	28	13

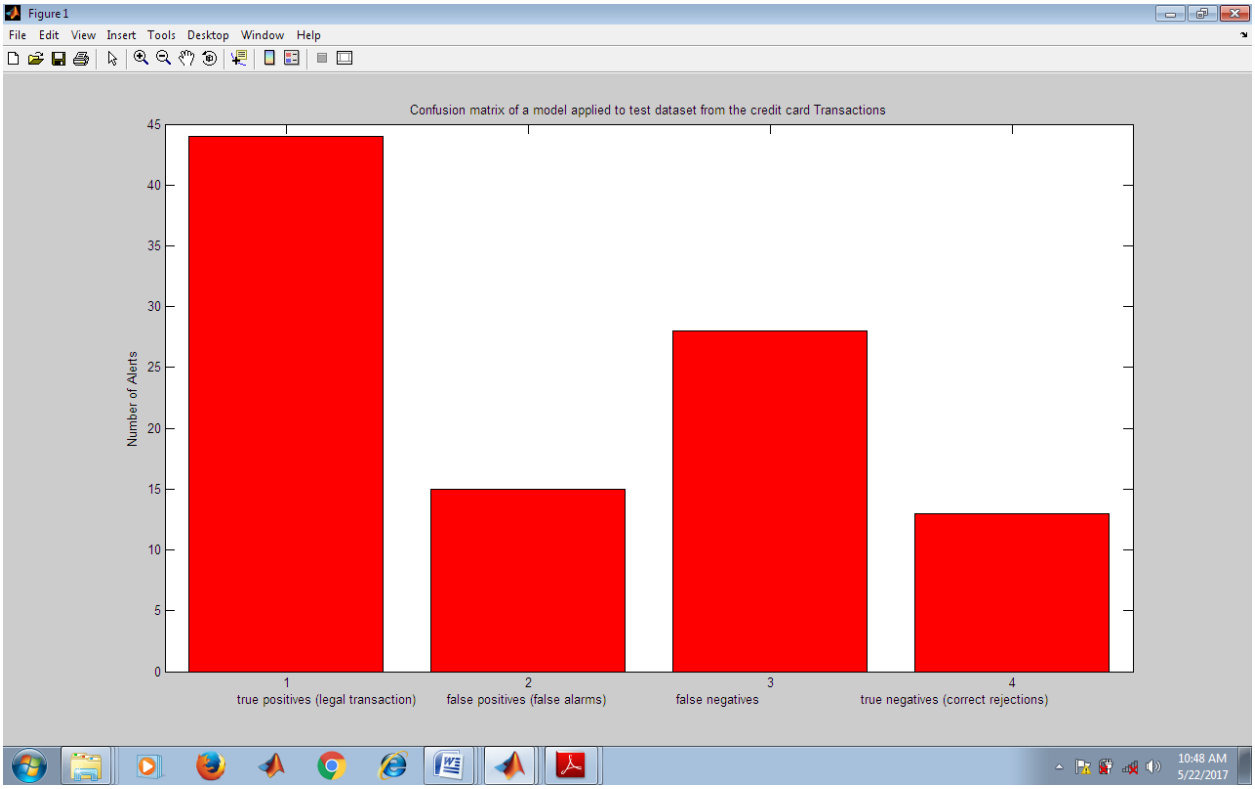


Fig. 4.26: Confusion matrix of a model applied to test dataset fromthe credit card Transactions using pin as the only security mechanism

Figure 4.26 shows the alerts on 100 transactions carried out using credit card. The graph shows that 44 transactions are legal and was predicted correctly. Table 4.13 shows confusion matrix built on simulated data. It shows the classification model being applied to the test data that consists of 100 instances roughly split evenly between two classes. The model commits some errors and has an accuracy of 94%. 15 legal transactions are detected to be fraudulent they are thereby denying the owner access to the transaction. False negative alarm occurred 28 times in which the transaction was allowed to go through while it is fraudulent. Finally, 13 fraudulent transactions were detected. A model of performance metrics can be derived from the confusion matrix as show in equation 4.1, which show the accuracy of the credit card fraud detection system.

$$AC = \frac{a+d}{a+b+c+d} \quad (4.1)$$

a = True Positive

b = False Positive

c = False Negative

d = True Negative

Substituting the values we have

AC = (44 + 13) / (44 + 15 + 28 + 13)

AC = 0.57 i.e 57% accuracy in detection

From the calculations above, the existing system of detecting fraudulent credit card transactions using pin code as the security technique provides 57% accuracy in fraud detection.

Table 4.14: Confusion Matrix

		Observed	
		Legal	**Fraud**
Predicted	**Legal**	TP	FP
	Fraud	FN	TN

Table 4.15: Confusion matrix of a model applied to test dataset

		Observed	
		Legal	**Fraud**
Predicted	**Legal**	55	4
	Fraud	2	39

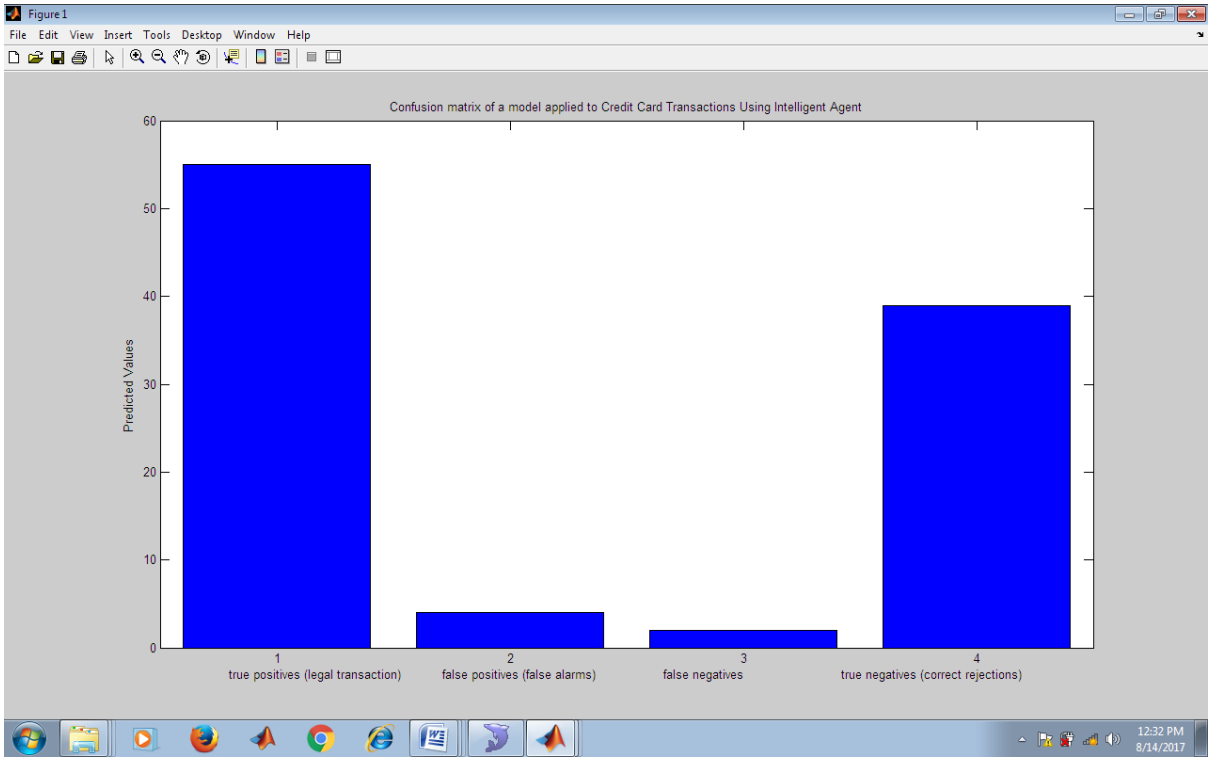


Fig. 4.27: Confusion matrix of a model applied to test dataset from the credit card Transactions using multi-agents as the only security mechanism

Figure 4.27 shows the alerts on 100 transactions carried out using credit card. The graph shows that 55 transactions are legal and was predicted correctly. 4 transactions are detected to be fraudulent while it is not thereby denying the owner access to the transaction. False negative alarm occurred 2 times in which the transaction was allowed to go through while it is fraudulent. Finally, 39 fraudulent transactions were detected. A model of performance metrics can be derived from the confusion matrix as show in equation 4.2, which show the accuracy of the credit card fraud detection system.

$$AC = \frac{a+d}{a+b+c+d} \qquad (4.2)$$

a = True Positive

b = False Positive

c = False Negative

d = True Negative

Substituting the values we have

AC = (55+39) / (55+4+2+39)

AC = 0.94 i.e. 94% accuracy in detection

4.7.3.5 Limitations of the System

The assumption in this dissertation is that the existing checks on credit card fraud detection that is based on credit card pin and other card details are sufficient. The moment a credit card is stolen and the card details provided on the credit card transaction platform, it will go unnoticed unless added to the existing multi-agents to detect such occurrences.

The limitation of the new system is that it will require extra computer processing time to complete a credit card transaction due to the processes the transaction will go through as a result of the activities of the multi-agents while trying to detect credit card fraud.

4.7.4 System Security

The security of the system is an important factor as computing systems become more essential to our daily lives, it becomes ever more important that the services they provide are available whenever one need them. The use of username and password in the case of bank staff and credit card details and pin code for bank customers is used to prevent unauthorized use of the system and downloads of software. Role assignment and centralized process in software procurement and deployment are also used to ensure that an organization acquire only what it needs. There is a provision for Backup and restore in case of loss of information or system failure.

4.7.4 .1 Reliability

The use of data mining and multi- agent in the process of credit card fraud detection makes the new system reliable. The new system performs a check on the credit card previous transactions to ascertain the spending profile of the user and match it with the new transactions. Where it does not match, the system prompts for answer to some secret question to authenticate the user. Where the answer to the question is wrong, a fraud alert will be generated by the multi- agent and subsequently blocks the transaction. So the new system is reliable.

4.7.4.2 Process-Oriented

The process of using the new system is as follows:

a. The user enters the account no and the pin code
b. Then the system will prompt for the transaction amount after validating the pin code
c. The transaction amount will be captured by the multi- agent and use it to perform fraud check on the transaction
d. If no fraud is detected then the user is required to enter the credit card details and the account no of the recipient
e. The transaction will then be completed

4.7.4.3 Information Oriented

The new system is interactive and user friendly. Every step needed in the process of the transaction, the system generates information to guide the user on what to do next.

4.7.4.4 Operational Requirement

During data collection, the researcher investigated and found out how the current system operates, not only that, but also tried out which problems are faced and how best they can be settled. The users described some of the operational requirements of the system. This includes opening account for customers, posting deposit and withdrawal transactions, making payment online through the use of credit card and View all types of reports.

4.7.4.5 Functional Requirements

The Desired system should be able to perform the following tasks:-

1. Capture Account number that user is accessing on core banking system
2. Pass the number to multi-agents
3. Check each account number against set rules
4. Report back any set of rules that are broken in terms of fraudulent transactions
5. Display an alert for every rule broken
   Block the account where fraudulent.

4.7.5 Training

Training is the aspect of system implementation that describes the guidelines that users can follow to use a system. The training of users is very important to run the new system successfully. The users must be trained properly to use the new system effectively and efficiently. Training is conducted for the staff selected to carryout credit card transactions and running of the system. The members of staff selected are trained for a period of time on how

to manipulate and operate the system so as to be acquainted with the processes and procedures of the system designed. Procedural manuals are also provided to assist them in operating the system.

4.7.6 Documentation

Documentation is critical to an effective program implementation. It is a written text that accompanies the new system that was developed. It explains how the system operates or how to use it and explains the different roles of different individuals. In this research, our documentation is mainly on how the application can be used, how it can be installed following the stated system requirements and roles and responsibilities of various individuals in an organization explained.

The Software was stored in a CD. To install it on the system to run from the hard disk, follow the procedure below.

i. Install Micromedia Dreamweaver 8 on the Computer
ii. Install Wamp Server on the computer
iii. Install My-SQL
iv. Install Java Virtual Machine
v. Install jQuery files
vi. Click Start Button on the desktop
vii. Select program
viii. Click Windows explorer
ix. Click Drive D:
x. Select the folder “creditcardfrauddetection”
xi. Click Edit
xii. Click Copy
xiii. Select drive C:
xiv. Select Wamp
xv. Select www
xvi. Click paste to Copy the Folder “creditcardfrauddetection” from drive D: to Drive C:
xvii. The folder contains the entire sub program that makes up the software developed will be copied to the www root
xviii. Open internet explorer
xix. Type http://localhost/creditcardfrauddetection
xx. Select the login page
xxi. Enter the user name and password and click login

xxii. Select options from the menu

4.7.7 System Conversion

The system has been implemented using a combination of frameworks. The multi-agents component has been implemented using JADE [Java Agent Development Environment] to capture the transaction account on run time while the user interface is implemented using Java script. The core banking system is stored in a MySQL server and queries to the database were developed in SQL using PHP-MySQL program development platform. A system can be implemented after it has been tested and this is known as system conversion. It is a process of changing over from the old system to a new secured system.

4.7.7.1 Changeover Procedures

There are numerous changeover methods, specifying different ways of switching over from the old system to the new system. Below is the different change over procedures:

a. **Parallel Approach** – In this approach, old and new system are operated side by side until the new one has shown that it is reliable. This approach is low risk. If the new system fails, the organization can just switch to the old system to keep going. This method, however, is expensive as it keeps people and equipment active to manage the two systems.
b. **Pilot Approach** – This approach involves the trial of the new system in only one part of the organization. Once the system is working out smoothly in that part, focus is then shifted to other parts of the organization.

   Phased Change Over Approach – This approach is similar to the parallel approach except that initially, only a portion of the current data is run in parallel on the new system for instance, that pertaining to one department or unit only. During the following weeks, more sections are transferred onto the new system. In each case, the old system runs in parallel for one processing cycle only. Thus, the old system is phased out as the new system builds up.

4.7.7.2 Recommended Procedure

Although there are numerous change over methods, the one recommended for this system is a parallel run implementation in which both the old and new system are operated concurrently for a period of time until the new system is certified functional. This is to enable the management fall back to the old system should the new system pose some challenges in its usage.

4.8 Results and Discussions

An agent based information, that is, credit card frauds prediction, and data sets were produced; Presentation of the obtained data is in form of SMS notification on the fraudulent attempt were it sent to customer and bank database. Multi-agents classified the spending pattern of credit card owners and detected when the transactions fall outside the spending pattern. The novel credit card fraud that was developed was able to detect and monitor existing credit card frauds found in the network of the developed system. An enterprise architecture model was developed, tested for the accuracy using confusion matrix which shown a significantly positive impact of 94% in credit card fraud detection system.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

As every country is striving to attain cashless society where fiscal cash will no longer be the major means of transaction but through the use of credit card, there is need to secure the credit card transaction channels to reduce the rate of fraud that is associated with online transactions. Credit card fraud has become more and more rampant in recent years. To improve merchants' risk management level in an automatic and efficient way and build an accurate and easy handling credit card, risk monitoring system is one of the key tasks for the merchant banks. The aim of this dissertation is to identify the user model that best identifies fraud cases. There are many ways of detection of credit card fraud. If one of these or combination of algorithm is applied into bank credit card fraud detection system, then the probability of fraud transactions can be predicted soon after credit card transactions by the banks. This dissertation gives contribution towards the effective ways of credit card fraudulent detection. In the dissertation, the system utilized adaptive data mining and multi-agents technique to classify credit card user's spending profile and monitor where the transaction falls outside the spending profile. This is done in other to introduce more security measures in checking credit card transaction frauds and block the transactions.

5.2 Conclusion

The work developed a new approach of solving bank frauds problems especially in the area of credit card fraud. A conceptual framework for a system based on credit card fraud (CCF) process was developed. Various classes of were proposed to provide a set of functionalities for CCF in electronic environment for banks. The model is therefore recommended for use by banks, financial agencies and government agencies. They are robust enough to defeat sophisticated fraudsters, they are fast enough to minimize fraud damages, and they are scalable enough to tackle huge volumes of data. Multi- agent will eventually be the ultimate means to fight against credit card frauds. The study resulted in a model, which is used to detect abrupt changes in established patterns and recognize typical usage patterns of fraud. The credit card fraud detection system was designed to run at the background of existing banking software and attempt to discover illegitimate transaction entering on real-time basis. This proved to be very efficient method of discovering fraudulent transactions. The data used was a mixture of normal and fraudulent with an unknown mixing mechanism. Credit card fraud detection system

detected most of the fraudulent transactions. The research presented the following contributions to knowledge –enterprise architecture of multi- agent credit card fraud (CCF) detection model, an agent based information, that is , credit card frauds, and data seta were produced and design of the CCF detection alert to key system (customer and bank database) were produced..

An approach is used to develop the credit card fraud detection system that utilizes both adaptive data mining and multi-agents approaches to achieve a synergy that better handles the Nigerian credit card fraud situation using instead of two-stage model normally used in fraud detection algorithm. This reduced the classification of legitimate transactions as fraudulent, ensured accurate and reliable result. The study reinforces the validity and efficiency of data mining and multi- agent as a research tool and laid a solid groundwork for intelligent detection methodologies to be used in an operational fraud detection system. The objective of the research which was to develop an adaptive data mining and multi-agents based fraud detection system is considered to have been technically achieved. The research demonstrated that through treasuring the knowledge and the opinions collected during the meetings, an adaptive data mining and multi-agents system prototype of real time agents intended to detect fraud using rules set to determine suspicious activities in the credit card transactions is achievable. The prototype is intended for the management of fraud detection situations where system users and are collaborating according to a three-phase detection process. In the first phase users keep their credit card pin and secret question private without sharing it with any other person. In the second phase, the credit card user's transaction components are structured into rules that act as thresholds used for monitoring each account that is transacted into in the credit card transactions. In the third phase an alarm is raised for each threshold reached. The successful solution of this kind of problem depends to a large extent on a proper definition of rules that determine a suspicious event. So the model developed was able to show the classification model being applied to the test data that consists of 100 instances roughly split evenly between two classes. The model archived 94% accuracy in detecting credit card fraud.

5.3 Recommendation

It is recommended that all banking sectors should integrate the model developed in this dissertation into their banking software so as to help detect credit card frauds. In addition, credit card users are advised to maintain secrecy about their credit card pins and other details. This will help eliminate credit card fraud and encourage cashless transactions.

5.3.1 Application Areas

The credit card fraud detection modeled in this dissertation can be applied in online payment channels that utilize credit cards. The banks, super stores and online shopping platforms can link the software to their bank database servers so that the software will connect the payment platform to the database server in other to check the spending profile of the card holder for the purpose of detecting credit card fraud.

5.3.2 Suggestion for Further Research

The system can be improved and advanced based on the following:

1. To integrate voice recognition on the credit card transaction channel so as to confirm through voice, the identity of the credit card users in case fraud is suspected.
2. To explore such multi-entity involved credit card transaction solution.

5.4 Contributions to Knowledge

The dissertation has focused on a practical fraud detection mechanism that demonstrates the agent based technology approach in detection of suspicious transactions in the bank. The fraud detection using adaptive data mining and multi- agents technology is expert driven approach in that as a transaction takes place on the financial system the agents perform a check against a set of rules to determine any suspicious anomaly in the involved account to prevent data manipulation or user assumption on key aspects pertaining to the account that could lead to fraud. One develops the software from the scratch.

REFERENCES

Abdechalin, A., & Traore, I. (2009). Identity Application Fraud Detection using Web Mining and rule-based decision tree. *International Journal of Computer and Network Security,* 1(1), 31-44.

Abhinav, S., Amlan, K., & Shamik, S. (2008). A Revealing Introduction on to Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48.*

Abhinav, S., Kundu, S., Shamik, S., & Arun, K. (2008). Credit Card Fraud Detection Using Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing,* 5(1). 83-86

Aburrous, M., Hossain, M., Dahal, K., & Thabtah, F. (2010). Intelligent Phishing Detection system for e-banking using fuzzy data mining. *Expert System Application,* 37(12), 7913-7921.

Adebayo, O. G., & Ajinaji, O.T. (2014). Bank Frauds and Forgeries in Nigeria. A study of the causes, Types, Detection and Prevention. *IOSR Journal of Economics and Finance, 4(2), 41-50.*

Adebisi, (2009). Credit Card Fraud Detection Using Hidden Markov Model. *International Journal of Computer Science and Engineering,* 4(2), 57.

Adekanye, F. (2008). Fraud in Banking Transactions. *The Nigerian Bankers, 6(1), 7-15.*

Adewunmi, W. (1999). Fraud in Banks Lagos; Nigerian Institute of Bankers, 26-36.

Adeyemo, K.A., (2012). Frauds in Nigeria Banks. Nature, Deep-Seated causes, Aftermaths and Probable Remedies. *Mediterranean Journal of Social Sciences, 3(2), 279-289.*

Adnan, M., &Khatib, A. (2012). Electronic Payment Fraud Detection Techniques, *World of Computer Science and Information Technology Journal,* 2(4) 137-141.

Ahhinav, S., Amlan, K., Shanlik, S., Run, K. (2008). *IEEE Transactions on Dependable and Secure Computing,* 5(1) 37.

Akoroda, G.C.O. (2004). Frauds and Forgeries. *WAJFEM Regional course on Banking Supervision, Lagos.*

Akshada, K; Chhajed, k.k; & Kapse, A.S. (2017). Review on Fraud Detection in Electronic Payment Gateway. *International Journal of Engineering and Technology,* 4(1), 841-844.

Alashi, S.O., (1994) Fraud Prevention and Control. Role of Government and its Agents.
Journal of the institute of Bankers of Nigeria (July-December, 1994) pp11-15.

Aleskerov, E., Fieisleben, B., & Bharat, R. (1997). CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, *Department of Electrical Engineering and Computer Science, University of Siegen,* 220-226.

Alessandro B (2012): Fraud Detection in the Banking Sector. A Multi-agents Approach. *International conference on management and service & science, 24-26 August, Wuhan, 1-4.*

Alexopoulos, P., & Kafentzis, K. (2007). Towards a Generic Fraud Ontology in E-Government,*ICE-B,* 269-276.

Alowais, M., & KiSoon, L. (2012). Credit Card Fraud Detection: Personalized Aggregated Model", *Mobile, Ubiquitous, and intelligent Computing (MUSIC), Third FTRA international Conference* Anomaly Detections –Wikipedia, the free encyclopedia. (ONLINE). Available at: *http//en.wikipedia.org/wiki/Anomaly detection.*

Anshul, S., & Devesh, N. (2012). A Survey on Hidden Markov Model for Credit Card Fraud Detection. *International Journal of Engineering and Advanced Technology (IJEAT), 1(3), 49-52*

Anuar, N., Sallehudin, H., Gani, A., & Zakari, O, (2008). Identifying False Alarm for Network Intrusion Detection System using Hybrid Data Mining and Decision Tree, *Malaysian Journal of Computer Science, 2(1), 110-115.*

Aashlesha, B., & Avnish, B. (2015). Credit Card Fraud Detection Using Hidden Markov Model. *International Journal of Innovative Research in Computer and Communication Engineering, 5(6), 19*

Arthisree, K., & Jaganraj, A. (2013). Crime Detection using Data Mining Techniques *International Journal of Advanced Research in Computer Science and Software engineering, 3 (8) 977-983*.

Asghar, S.,&Iqbal, K. (2009). Automated Data Mining Techniques: A critical literature Review. *IEEE Proceedings of the International Conference on Information Management and Engineering, IEEE Xplore Press, Kuala Lumpur, 75-79.*

Ashish, T., Bushra, S., Vinita, J., & Magar, A.M. (2015). Credit Card Fraud Detection Using hidden Markov Model and Enhanced Security Features. *International Journal of Engineering Schemes and Research Technology, 4(4), 72-77. http://www.ijesrt.com*

Ashphak, P. (2013). Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model. *International Journal of Innovation Research in Computer and Communication.* 1(1), 15.

Ashphat, K., &Singh, I. (2012). Observation Probability in Hidden Marko; Model for Credit Card Fraudulent Detection System. *Proceedings of the Second International Conference on Soft Computing for Problem Solving.*

Avinash, I., & Thool, R.C. (2013). Credit Card Fraud Detection Using Hidden Markov Model and Its Performance. *International Journal of Advanced Research in Computer Science and Software Engineering, 3(6), 626-632.*

Bentley, J., & Kim, J. (2000). Fuzzy Darwinian Detection of Credit Card Fraud *Proceedings of 14th Annual Fall Symposium of the Korean Information Processing Society.*

Bhalta, T.P. (2013). Understanding Credit Card Trends' Card Business Review. *http:/www.tcs.com/o_whitepapers/htdocs/cr_1.0.pdfedit_card_fraud_whitepaper_V.*

Bhambri, V. (2011). Application of Data Mining in Banking Sector. *International Journal of Computer Science Technology, 2(2), 199-201.*

Bharati, M. R. (2010). Data Mining Techniques and Applications. *International Journal of Computer Science and Engineering*, 1(4), 301-305.

Bhusari, V., & Paul, S. (2011). Study of Hidden Markov Model in Credit Card Fraudulent Detection. *International Journal of Computer Applications, 20(5), 33.*

Biddhant, P. (2015). A Review on Multi-agents Data Mining Systems. *International Journal of Computer Science & IT, 6 (6), 4888-4893.*

Bilonikar, P., & Deokar, M. (2014). Survey on Credit Card Fraud Detection Using Hidden Markov Model*. IJRCCF, 3, (2) [Online] Available; www.bsys.monosh.eduau/people/cphua.*

Bolton, R., & Hand, D. (2002).Unsupervised Profiling Methods for Fraud Detection*. London.*

Bose, R. (2006). Intelligent Technologies for Managing Fraud and Identity Theft*. International Journal of E-business Research*, 2(1), 1-18.

Brabazon, A.J., Cahil, J., Keenan, P., & Walsh, D. (2010). Identifying Online Credit Card Fraud using Artificial Immune. *IEEE Congress on Evolutionary Computations, Dublin.*

Caglayan, A., & Harrison, C. (1997).Agent Sourcebook*: A Complete Guide to Desktop, Internet, and Intranet Agent, John Wiley & Sons, New York, NY.*

CBN (2014). *"Central Bank of Nigeria Annual Report and Statement of Accounts"*.

Chang. W.H., & Change, J.S. (2012). An early Fraud Detection Methods for Online Auctions *Science Direct Electronic Commerce Research and Applications*, 346-360.

Chen R.C., Chen, T.S., & Lin C.C. (2006). Detecting Credit Card Fraud by using Questionnaire – Responded Transaction Model based on support vector machines *Springer-Verlag Berlin Heidelberg.* 800-806.

Chitra, B., & Subashini, D. (2012). Data Mining Techniques and its Applications in Banking Sector. *International Journal of Emerging Technology and Advanced Engineering, 3, (8). 45.*

Chitra, K., & Subashini D. (2012*).* Fraud Detection in the Banking Sector*. Proceedings of National Level Seminar on Globalization and its Emerging Trends.*

Chiu, C., & Tsai, C. (2004). A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection. *Proceedings of IEEE International Conference C-Technology, C-Commerce and E-Service.*

Cho, B., & Park, H. (2003). Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model. *International Journal of Computer and Security, 22(I), 45-55.*

Chopra, B., Bhambri, V., & Krishnan, B. (2011). Implementation of Data Mining Techniques for Strategic CRM Issues. *International Journal of Computer Technology Application,* 2(), 879-883.

Clifton, P., Lee, V., & Ross, G. (2012). Resilient Identity Crime Detection.*IEEE Transactions on Knowledge and Data Engineering, 24(3).*

Clifton, P., Damminda, A., & Vincent, L. (2004). Minority Report in Fraud Detection*: Classification of Skewed Data. Explorations Newsletter, 6(), 50-59.*

Costa, G., Folino, F., Locane, A., Manco. G., & Ortale R. (2007). Data Mining for Effective Risk Analysis in a Bank Intelligence Scenario. *Proceedings of the 23rd International Conference on Data Engineering Workshop, IEEE Xplore Press, Istanbul, 904-911.*

Cybercrime: protecting against the growing threat Global Economic Crime survey-PWC Global Economic. *(ONLINE) Available at: http://www.com/en_GX/gx/economic-crime survey/ass ets/GECS_GLOBAL_REPORT.pdf. (Accessed 12 December 2012).*

Data Analysis Techniques for Fraud Detection. (*ONLINE) Available at: http//en.wikipedia.org/wiki/Data_Analysis_Techniques_for Fraud Detection.*

Delamaire, L., Hussein, A.,& John P (2009). Credit Card Fraud and Detection Techniques: A Review, International of Journal of Technology and, 4(2), 57-68.

Desai, D and Anita D. (2004). The Role of Data mining in Banking Sector, *IBA Bulletin.*

Deshpande, M., & Thakar, D. (2010). Data Mining System and Applications: A Review. *International Journal of Distributed Parallel System, 1(2), 32-44.*

Dheepa, V., & Dhanapal, R. (2009). Analysis of Credit-Card Fraud Detection Methods. *International Journal of Recent Trends in Engineering*, 2(3), 126-128.

Egu, J. (2010).The Role of Information and communication Technology (ICT) in Fraud Detection in Nigeria Banks.

Ekechi, A. (1990). Frauds and Forgeries in Banks, Causes, Types and Prevention. *Seminar in Bank Audit Organized by Institute of Chartered Accountant of Lagos, Nigeria.*

Ekrem, D., & Mehmet Hamdi Ozcelik (2011). Detecting Credit Card Fraud by Genetic Algorithms and Scatter Search. *: An International Journal on Expert Systems with applications, 38(10), 13057-13063.*

Esakkiraj, S., &Chidambaram, S. (2013). A Predictive Approach for Fraud Detection using Hidden Markov Model. *International Journal of engineering Research and Technology, 2(6), 43*

Ezeuduj, F. (2005). Historical Perspective in Banking Practices Worldwide.

Fan, W., Prodromidis, A., & Stolfo, S. (l999).Distributed Data Mining in Credit Card Fraud Detection. *IEEE Intelligent System,* 14(6).

Farvaresh, H., & Sepehri, M.M (2010). A Data Mining Framework for Deleting Subscription Fraud in Telecommunication. *Engineering Applications of Artificial intelligence. (24), 182-194.*

Faweett, T.,& Provost, F. (1997). Adaptive Fraud Detection, Data mining and knowledge Discovered. *Kluwer Academic Publishers, Boston, Massachusetts,* 1-28.

Franklin, S., & Graesser, A. (1997). Is it an agent, or just a program? Multi-agents III: Agent Theories, Architectures, and Language; Proceedings ECAI Workshop (ATAL), Budapest, *Hungary* Springer-Verlag, *Berlin*, 1-20.

Friedrichs, D. (2009). Trusted Criminals: White Collar Crime in Contemporary Society, *Wadsworth Publishing.*

Gadi, M.F., & Wang, X. P. (2008). Credit Card Fraud Detection with Artificial Immune System.*Springer-Verlag Berlin Heidelberg.*119-131.

Gamma, E., Helm, R., Johnson, R., &Vlissides, J. (1995). Design Patterns*: Elements of Reusable Object Oriented Software* Addison-WesleyRiel,

Geng, L., &Hamilton, J. (2006). Interestingness Measures for Data Mining: A survey. *ACM Computer Surveys.*

Ghosh and Reilly (1994). Credit Card Fraud Detection with a Neural Network. *IEEE Proceedings of the Twenty-Seventh Annual Hawaii International Conference on System Sciences, 3, 621-630.*

Giannis, P. (2013): Designed Implementation of a Fraud Detection using Expert System Ontology Based Techniques.

Gosset, P., &Hyland, M. (1999). Classification, Detection and Prosecution of Fraud on Mobile Networks. *Proceedings of ACTS Mobile Summit.*

Gunn, S.R. (1998). Support Vector Machines for Classification and Regression .*University of Southampton, U.K.*

Guo, T. & Li, G.U. (2008). Neural Data Mining for Credit Card Fraud Detection. *Proceeding of the Seventh International Conference on machine learning and cybernetics, Kunming.*

Hamid, F., & Mohammed, M .S. (2011). A Data Mining Framework for Detecting Subscription Fraud in Telecommunication. *ELSEVIER (Engineering Applications of Artificial Intelligence,* 24(1), 182-194.

Hand,D. J. (2010). Fraud Detection in Telecommunications and Banking. *Technimetrics,* 52(1) 34-38.

He, J., Zhang, Y., Shi Y., & Huang, G. (2010).Domain-Driven Classification Based on Multiple Criteria and Multiple Constraint-level Programming for Intelligent Credit Scoring. *IEEE Trans. Knowledge. Data Eng,* 5(5), 826-838.

Hillol, K., Anupaw, J., Krishnamurthy, S., & Yelena, Y. (2005). Data Mining: Next Generation Challenges and Future Directions. *Prentice-Hall of India, Private Limited.*

Hoang, X., Hu, J., & Bertok, P. (2003). A Multi- Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls. *Proc. 11th IEEE Int'l Conference Networks, 531-536*

Hormozi, A.M & Giles, S. (2004). Data Mining: A Competitive Weapon for Banking and Retail Industries. *Information Systems Management,* 62-71.

Ingle, D., & Meshram, B. (2012). E-Investment Banking: Next Generation Investment. *International Journal of Advanced Research Computer Engineering Technology 3(4), 45*

Ionita, L. (2011). A Decision Support Based on Data Mining in E-Banking. *IEEE Proceedings of the 10th Reodunet International Conference (RoEduNet), Jun. 23-25, IEEE XplorePress, lasi, 1-5.*

Iyer, D., Mohanpurkar, A., Janard, S., Ratho, D., & Sardeshmukh, A. (2011). Credit Card Fraud Detection using Hidden Markov Model. *Information and Communication Technologies (WICT), World Congress.*

Jennings, N.B., Faratin, P., Normap, T.J., O'Brien, P., & Odgers, B. (2000). Autonomous Agent's Business Process Management. *International Journal of Applied Artificial Intelligence,* 14(2), 145-89.

Jia, W.U. and Jongwoo, P. (2005). Multi-agents and Fraud Detection.

Jiawen, H., Micheline, K., & Jian, P. (2011). Data Mining: Concepts and Techniques. *The Morgan Kaufmann Series, 244-254.*

John, A. (2013). Data Mining Application for Cyber Credit-Card Fraud Detection System. *Proceedings of the World Congress on Engineering, Volume 3, wce 2013, july 3-5, London, U.K.*

Joshi, S., & Phoha, V. (2005). Investigating Hidden Markov Models Capabilities in Anomaly Detection. *Proc. 43rd ACM Ann. Southeast Regional Conference, 1, 98-103.*

Kappelin, F. and Rudvall, J. (2015): "Fraud Detection within Mobile Money: A mathematical statistics approach" MSc Thesis submitted to the Dept. Computer Science &

Engineering Blekinge Institute of Technology SE–371 79 Karlskrona, Sweden.

Kaptan, S. (2002).New Concepts in Banking. *Sarup and Sons, Edition.*

Kaur, G., & Sing, L. (2011).Data Mining: An Overview. *International Journal of ComputerScience Technology, 2,(4), 336-339.*

Kaur, S., & Kaur, U (2013). A Survey on Various Clustering Techniques with K-means Clustering Algorithm in Detail. *International Journal of Computer Science2, (6), 155-159.*

Kazi, I.,& Qazi, B. A. (2012). Use of Data Mining in Banking. *International Journal of Engineering Research and Applications, 2(2),*38-742.

Khac, N., Markos, S., Brabazon, A., &Kechadi, M. (2011). An Investigation into Data Mining Approaches for Anti-Money Laundering. *Proceedings of the International Conference on Computer Engineering Applications, Lacsit Press, Singapor,*504-508.

Khan, M., Jahir, P., Ali, H., & Ekbal, A. (2014). Credit Card Fraud Detection System using Hidden Markov Model and K-Clustering. *International Journal of Advanced Research in Computer and Communication Engineering, 3(2), 40*

Khan, A., & Sinhal, A. (2012). Implement Credit Card Fraudulent detection System using Observation Probabilistic in Hidden Markov Model. *Engineering (NUiCONE), Nirma University International conference.*

Khan, A. P., Mahajan, V. S., Shaikh, S. H and Koli, A. B. (2013): "Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model" International Journal of Thesis Projects and Dissertations (IJTPD) Vol. 1, Issue 1, PP: (7-16), Month: October-December 2013, Available At: www.researchpublish.com.

Khyrati, C., Jyoti, Y., & Bhawna M. (2012). A Review of Fraud Detection Techniques Credit-Card. *International journal of Computer Applications,* 45, (1), 39-44.

Khyati Chaudhary and Bhawna Mallick (2012). Credit card fraud: Bang in E-commerce. *International Journal of Computational Engineering Research, 2(3), 935-941.*

Kin, K. (2013). Pricing Fraud Detection in Online Shopping using a Finite Mixture Model. *Science Direct Electronic Commerce Research and Applications,* 195-207

Kim, H.S., Lee J.K., & Yoo, K.Y., (2003). ID-Based Password Authentication Scheme using Smart Cards and Fingerprints. *ACM SI90PS Operating System,* 37(4), 32-41.

Koru (2014). Real Time Multi-agents Based Fraud Detection. Tool for Banking Institutions.

Korfredt, H.S., & Mjlsnes, S.F. (2009). Eavesdropping NFC. *The Norwegian Information Security Conference (NISK),* 57-68.

Kovach, S and Ruggiero, W. V. (2011): "Online Banking Fraud Detection Based on Local and Global Behavior" ICDS 2011: The Fifth International Conference on Digital Society.

Kumar, P., Nitin, S., & Chauhan, D. (2011).Performance Evaluation of Decision Tree versus Artificial Neural Network Based Classifiers in Diversity of Datasets. *Proceedings of the World Congress on Information and Communication Technologies, IEEE Xplore Press, Mumbai, 798-803.*

Laleh, N., &Azgomi, A. (2009). A Taxonomy of Frauds and Fraud Detection Techniques.*ICISTM*3(1), 256-267.

Lamond, K. (2013). Credit Card Transactions – Real World and Online http://www.virtualschool.edu/mom/electronicproperty/klamond/CCard.htm.

Lane, T. (1999). Hidden Markov Models for Human Computer Interface Modeling *Proceedings International Joint Conference, Artificial Intelligence, Workshop Learning about Users, 35-44.*

Larman, C., & Basili, V.R. (2003). Iterative and Incremental Development: A Brief History: International Journal of Computer science and research, 36(6), 47-56.

Lee, W., Stolfo, S., & Mok, K. (2011). Adaptive Intrusion Detection: Data Mining Approach, *Kulwer Academic Publishers.*

Li, W., & Liao. J, (2011). An Empirical Study on Credit Scoring Model for Credit Card by using Data Mining Technology. *Proceedings of the 7th International Conference on Computational Intelligence and Security, IEEE Xplor Press, Hainan, 1279-1282.*

Liu, K., Sun, L., Dix, A., & Narasipuram, M. (2001). Norm Based Agency for Designing Collaborate Information Systems. *Information Journal of computer Science and Technology,*11(3), 229-47.

Lloyd, R. (2003). Hidden Markov Model and Baum-Welch Algorithm.*Welch IEEE Information Theory Society Newsletter, 5(3)4.*

Macs, S., Tuyls, K., Vanschoen Winkel, B., & Manderick, B. (2002). Credit Card Fraud Detection using Bayesian and Neural Networks. *Proc. of 1st NAISO Congress on Neuro Fuzzy Technologies.*

Madey, G., Freeh, V., & Tynan, R. (2002). TheOpen Source Software Development Phenomenon an Analysis Based on Social Network Theory. *Proceedings of the 8th Americas Conference on Information Systems, AMCIS, Dallas, 1806-1813.*

Mandeep, Singh., & Parvinder, Singh .(2015). Fraud Detection by Monitoring Customer Behaviour and Activities. *International Journal of Computer Applications, 3(2), 23 – 32.*

Margaret, R., Retrieved Oct. 12, 2014 from http://www.searching.techtarget.com/definition/two_factor_authentication.

Meyer, D. (2012). Support Vector Machines. *Technische University at Wien, Australia.*

Models to Detecting Multi-Stage Network Attacks. *Proceedings 36th Ann. Hawaii International Conference System Sciences,(9) 334- 344, 2003.*

Muneendra, B., &Muhammad, S. (2013). A Focus on Different Frauds and using Data Mining to Enhance Business Process in Banking Sector. *International Journal of Engineering Sciences Research, 4(1), 45*

Murad, U., & Pinkas, G. (2009). "Unsupervised profiling for identifying superimposed fraud", in proceedings of the 3rd European Conference on Principles of Data Mining and knowledge discovery, 2009, pp. 251-266.

Nabha, K., Neha, P., Shraddha, K., Suja, S., & Amol, P. (2015). Credit Card Fraud Detection System using Hidden Markov Model and Adaptive Communal Detection. *International Journal of Computer Science and Information Technologies, 6 (2), 1795-1797.*

Naeini, M., Taremian, H., & Hashemi, H. (2010).Stock Market Value Prediction using Neural Networks. *Proceedings of the International Conference on Computer Information Systems and Industrial Management Applications, IEEE Xplore Press, Krackow, 132-136.*

NeFF Pledges Sustained Fight Against e-fraud in 2016.

NIBSS Annual Report and Statement of Account, 2018.

NDIC Annual Report and Statement of Account, 2014.

Ngai, E., Xiu, L., & Chau, D. (2009). Application of Data Mining Techniques in Customer Relationship Management: A literature Review and Classification. *Expert System Application, (36), 2592-2602.*

Ngai, E., Yong, H., Wong, H., Yijun, C., &Xin, S. (2011). The Application of Data Mining Techniques in Financial Fraud Detection: *Decision Support System,* (50), 559-569.

Nitin, K. (2016). Credit Card Fraud Detection using Hidden Markov Model. *International Journal of Advance Scientific Research and Engineering Trends, 1(4) 4, 83-86.*

Nwankwo, G.O. (1991). Banking Management Policy and Practices. *Malthouse Press Ltd, Lagos, Nigeria.*

Nwanna, O.J. (2006). The Role of the Bank System in an Economy *(Financial standard).*

Nwaze, C. (2008). Quality and Internal Control Challenges in Contemporary Nigeria Bank. *Zenith Economic Quarterly, Zenith Bank Plc, 3(2), 21-32*

Ogwueleka, F. (2011). Data Mining Application in Credit Card Fraud Detection System. *Journal of Engineering Science and Technology, 6(3), 311-322.*

Ojeigbede, F. (2000). Fraud in Banks. *A Paper Presented at the Effective Bank Institute Course Organized by FITC, Lagos.*

Ojo, J.A., (2008). Effect of Bank Frauds on Banking Operations in Nigeria. *InternationalJournal of investment and Finance, 1(1).*

Olfati-Saber, R., Fax, J.A., & Murray, R.M. (2007). Consensus and Cooperation in Networked Multi-agents Systems. *Proceedings of IEEE, (95), 215–233.*

Oloaye, C.C., Dada, R.A., & Adebayo, A.I., (2014). Analysis Fraud in Banks. Nigeria's Experience. *International Journal of innovative Research and Development, 3(1), 357-369.*

Osama, D., & Bala, S. (2007). Security Analysis for Internet Banking. *Eighth ACIS International Conference on software Engineering, Artificial Intelligence Networking, and Parallel/distributed computing IEEE DOI 10. 1109/SNPD.*

Osama, D., Phudung, L., & Bala, S. (2008). Fraudulent Internet Banking Payments Prevention using Dynamic Key. *Journal of Networks, 3(1).*

Ovuakporie, V. (1994). Bank Frauds: Cause and Prevention-an Empirical Analysis. *Ibadan, ATT Book Ltd. 23.*

Patel, Twinkle, & Ompriya, Kale. (2014). A Secured Approach to Credit Card Fraud Detection using Hidden Markov Model. *International Journal of Advanced Research in computer Engineering and technology,* 3(5), 1576.

Patidar, R., &Sharma, L. (2011). Credit Card Fraud Detection using Neural Network. *International Journal of Soft Computing and Engineering,* 1(2), 2231-2307.

Phua, C., Aloha, K., & Lee, V. (2009). Minority Report in Fraud Detection: Classification of Skewed Data.*ACM SIGKDD Explorations Newsletter,* 6(1), 50-59.

Phua, C., Lee, V., Smith, K.,& Gayler, K. (2005).A Comprehensive Survey of Data Mining-Based Fraud Detection Research. *Artificial Intelligence Review, 1—14.*

Phua, C., Monash, U., Gayler, R., Smith-Miles, K., &Lee, V. (2006). Implicit Personal Identity Streams using Communal Detection. *Sixth IEEE International Conference.*

Ping, Z., & Liang, S. (2010). Data Mining Application in Banking-Customer Relationship Management. *Proceedings of the International Conference on Computer Application and System Modeling, IEEE Xplore Press, Taiyuan, 124-126.*

Priyanka, Y., Pavan, W., Manish, T., Mohammed, F., & Gayatric, H. (2016). Proposal Distributed Data Mining in Credit Card Fraud Detection. *International Research Journal of engineering and Technology, 3(4), 460-463.*

Qinghan, Z. (2009). Study on Fraud risk Prevention of Online Banks. *International Conference on Networks Security, Wireless Communications and Trusted Computing.*

Qiu, D., Wang, Y., & Zhang. (2009).A Mode for a Bank to Identify Cross-Selling Opportunitie s. *Proceedings of the International Conference on Computational*

Intelligence and Software Engineering, Dec. 11-13, IEEE Xplore Press, Wuhan, 1-4.

Quah, J.T.S.,& Sriganesh, M. (2008). Real Time Credit Card Fraud Detection using Computational Intelligence. *Expert Systems with applications,* 35(4), 112-118.

Raghavendra Patider, & Lokesh Sharma. (2011). Credit Card Fraud Detection using Neural Network. *International Journal of Sort Computing and Engineering,* NCA 12011, 32-38.

Rajdeepa,& Nandhitha. (2013). Fraud Detection in Banking Sector using Data mining. *International Journal of Science and Research.*

Ramageri, B. (2010). Data Mining Techniques and Applications. *International Journal of Computer. Science and Engineering, (1) 301-305.*

Ratha, N.K., & Bolle R.M. (2014). Smart Card Based Authentication. *IBM System Journal retrieved. http://www.csc.msu.edu/rcsc891/sect601/textbook/18.pdf*

Ren, S.,& Sh. (2010).Customer Segmentation of Bank Based on Data Warehouse and Data Mining. *Proceedings of the 2nd IEEE International Conference on Information Management and Engineering, IEEE Xplore Press, Chengdu, 349-353.*

Royce, W. (2007). Managing the Development of Large Software Systems: Concepts and Techniques, *IEEEWESCON*, 26(8), 1-9.

Sahil Hak, Suraj Singh, &Varun Purohit. (2015). Credit Card Fraud Detection using Advanced Combination Heuristic and Bayes' Theorem. *International Journal of Innovative Research in Computer and Communication Engineering. 3(4), 2756-2763*

Sahin, Y.,& Duman, E. (2011). Detecting Credit Card Fraud by Decision Trees and Support Vector Machines. *Proceedings of the International Multi-conference of Engineers and Computer Scientist,* (1) 1-6.

Salman Raju, Rama Bai, & Krishna Chaitanya. (2014). Data Mining: Techniques for Enhancing Customer Relationship Management in Banking and Retail Industries. *International Journal of Innovative Research in Computer and Communication Engineering*, 2(1), 2655.

Sasirekha, I., & Samava T, Satra .B. (2012). An Integrated Intrusion Detection System for Credit Card Fraud Detection. *Proceeding of Second International Conference on Advances in Computing and Information Technology (ACITy), Chennai, India-Volume 1.*

Shakadwipi, A., & Kalavadekar N. (2014). Real-Time Credit Application Fraud Detection System Based on Data mining. *Third Post Graduate Symposium on computer engineering cPGCON Organized by Department of Computer Engineering, MCERC Nasik.*

Sharraa, A., & Panigrahi P. (2012). A Review of Financial Accounting Fraud Detection Based on Data Mining Techniques. *International Journal Computer Application, (39) 37-47.*

Shashidhar, H., & Varadarajan, S. (2011).Customer Segmentation of Bank Based on Data Mining-Security Value Based Heuristic Approach as a Replacement to k-means Segmentation. *International Journal of Computer Application,* (19)13-18.

Shin, J. (2011). Using Self-Organizing Maps for Analyzing Credit Rating and Financial Data. *Proceedings of the IEEE International Summer Conference of Asia Pacific Business Innovation and Technology Management, IEEE Xplore Press, Dalian,* 109-112.

Shinde, R., Vaghurdekar P.,& Shinde S. (2012).Deliberation of Data Mining in Banking. *International Journal Engineering. Research. Technology,* (1) 1-7.

Siklos, & Pierre. (2001). Money, Banking, and Financial Institutions. *Canada in the Global Environment. Toronto: McGraw-Hill Ryerson, 40.*

Singh, H., & Rajan. (2014). Impact of Information Technology on Indian Banking Services. *Proceedings of the 1st International Conference on Recent Advances in Information Technology, IEEE Xlore Press, Dhanbad, 662-665.*

Singh Mandeep, Perminderpal Singh & Rajan Kumar (2014). Fraud Detection by Monitoring User Behavior and Activities. *International Conference on Computer and Intelligent Systems,4(4) 6-14.*

Siva, P., Shaik, N., & Kishore, K. (2012). Credit Card Fraud Detection using Hidden Markov Model (HMM).*International Journal of Engineering Research and Technology, 1(5),45*

Soheila, Ehramikar. (2013).The Enhancement of Credit Card Fraud Detection Systems using Machine Learning Methodology. *Department of chemical engineering and applied chemistry, university of Toronto.*

Sonia, & Anil Arora (2015). Review on Use of Data Mining in Focusing Bank Frauds and Enhancing Business. *International Journal for Research in applied Science and Engineering Technology, 3(4),* 177.

Souza,S., Leao, M., &Richard. (2011). Performance Evaluation of Hidden Markov Model.*Performance Evaluation of computer and Communication Systems. Milestones and Future challenges Lecture notes in computer Science. 112-128.*

Srivastava, J., & Raghubir, P. (2008). Monopoly Money, the Effect of Payment Coupling and form on spending behavior. *Journal of Experimental Psychology, 27(4), 460-474*

Stolfo, S., Fan, W., & Lee, A. (2000). Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results, *Proc. AAAI Workshop Al Methods in Fraud and Risk Management, (2), 130-144.*

Syeda, M., Zhang, Y., & Pan, V. (2002). Parallel Granular Networks for Fast Credit Card Fraud Detection. *Procceding. IEEE International Conference of Fuzzy Systems*. 572-577.

Tae, Kyungklim, Hyung, Jin, Lim & Jae. (2013). Analysis on Fraud Detection for Internet Service. *International Journal of Security and its applications*, 7(6), 277-284.

Tak-chung, F. (2011).A Review on Time Series Data Mining. *Engineering Application for Artificial Intelligence, (24) 164-181.*

Tiwari, M. (2010). Data mining: A Competitive Tool in Retail Industries. *Global Journal Enterprise Information System.*

Varun, K., Chaitanya, V., & Madhavan M. (2012).Segmenting the Banking Market Strategy by Clustering. *International Journal Computer Application*, (45) 10-10.

Vasudevan, A. (1999). Report of the Committee on Technology up Gradation in the Banking Sector. *Constituted by Reserve Bank of India.*

Vatso, V., Sural, S., & Majumdar, A. (2005). A Came-Theoretic Approach to Credit Card Fraud Detection. *Proc. First Int'l Conf. Information Systems Security, 263-276.*

Wang, H.Q.,& Wang, C. (2006).Multi-agents in the Nuclear Industry. *IEEE Computer*, 30(11), 28-34

Wang, H.Q., Mylopoulos, J.,& Liao, S. (2002). Multi-agents and Financial Risk Monitoring systems. *Communications of the ACM*, 45(3), 83-8.

Wang, M., & Wang, H. (2006). Multi-agents Supported Flexible Workflow Monitoring System. *Advanced Information System Engineering.* 787–791.

Wells, Fargo (2016).Customers over Fraudulent Accounts.

Wells, J.T. (2002). Occupational Fraud. The Audit as Deferent. *Journal of Accountancy, 193(4), 24-29.*

Wiese, B., & Omlin, C. (2009). Credit Card Transaction's Frauds Detection, and Machine Learning: Modeling Time with LSTM Recruitment Neural Network, *Innovations in Neural Information Paradigms and Application. 231-268.*

WooIdridge, M., & Jennings, N.R. (2000). Multi-agents: Theory and Practice, *Knowledge Engineering Review*, 10(2), 115-52.

Wooldridge, M. (2002).An Introduction to Multi-agents Systems, *Wiley, Chichester*.

Xhac, N., Kechadi, M. (2010). Application of Data Mining for Anti-Money Laundering Detection: A case study. *Proceedings of the International Conference on Data Mining Workshop, Dec. 13-13, IEEE Xplore Press, Sydney, NSW. pp: 577-584*.

Xiong, T., Wang, S., Mayers, A., & Monga, E. (2013). Personal Bankruptcy Prediction by Mining Credit Card Data. *Expert Systems with Applications*, 665-676, 2013.

Yamanishi, K.,& Takeuchi, J.I. (2004). Online Unsupervised Outlier Detection using Finite Mixtures with Discounting Algorithms. *Data mining and knowledge discovering pp. 275-300.*

Yashpal, S., & Singh, C. (2009). Neural Networks in Data Mining. *Journal of theoretical and Applied Information Technology 2009), 5(6), 37-42.*

Yu, W.F.,& Wang, N. (2009). Research on Credit Card Fraud Detection Model Based on Distance Sum. *International Joint Conference on Artificial Intelligence*, 353-356.

Yusuf, Sahin, Serol, Bulkan, & Ekrem Duman (2013). A Cost Sensitive Decision Tree Approach for Fraud Detection. *Elsevier (Expert Systems with Applications), (40), 5916-5923.*

Zhang, G., Zhou, F., Wang, F., & Luo, J., (2008).Knowledge Creation in Marketing Based on Data Mining. *Proceedings of the International Conference on Intelligent Computation Technology and Automation, Oct. 20-22, IEEE Xplore Press, Hunan, 782-786*

Zhuge, H. (2003). Workflow- and Agent-Based Cognitive Flow Management for Distributed team. *International Journal of Information and Management*, 40(5), 419-29.

APPENDIX A

PROGRAM CODING

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />

<title>Credit card fraud detection system</title>

<script type="text/javascript" src="jprototype.js"></script>

<script type="text/javascript" src="ajax1.js"></script>

<script type="text/javascript" src="js/jquery-1.6.2.js"></script>

<style type="text/css">

#fade { /*--Transparent background layer--*/

        display: none; /*--hidden by default--*/

        /*background: #000; */

        background: #ffffff;

        position: fixed; left: 0; top: 0;

        width: 100%; height: 100%;

        opacity: .80;

        z-index: 1;

}

.popup_block{

        display: none;

        padding: 8px;

        border: 2px solid #ddd;

        float: left;

        font-size: 1.2em;
```

```
        position: fixed;
        top: 50%;
        left: 50%;
        /*overflow: scroll;*/
        /*height: 400px;*/
        /*width: 800px;*/
        /*height: 200px;*/
        /*width: 400px;*/
        /*overflow: scroll;*/
        z-index: 2;
        /*--CSS3 Box Shadows--*/
        -webkit-box-shadow: 0px 0px 20px #000;
        -moz-box-shadow: 0px 0px 20px #000;
        box-shadow: 0px 0px 20px #000;
        /*--CSS3 Rounded Corners--*/
        -webkit-border-radius: 10px;
        -moz-border-radius: 10px;
        border-radius: 10px;
        background-color: #ffffff;
        /*background-image: url(images/div_bg.jpg);*/
}
.hid_div{
display: none;
}
img.btn_close {
        float: right;
        margin: -10px -10px 0 0;
```

```
}
/*--Making IE6 Understand Fixed Positioning--*/
*html #fade {
	position: absolute;
}
*html .popup_block {
	position: absolute;
}
.specialLink {
	color: #ffffff;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
.divContent {
	font-family: "Trebuchet MS";
	font-size: 13px;
	color: #F4F4F4;
}
.specialLink1 {
	color: #999999;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
.jbutton {
	color: #999999;
	font-family: "Trebuchet MS";
	font-size: 12px;
```

```
}
ody {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
}td img {display: block;}
body {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
	background-color: #FFFFD2;
	background-image: url(images/bg.jpg);
}
.slide{
width:580PX;
height:230PX;

}
</style>

<script type="text/javascript">
<!--
&(document).ready(function() {
	&('#image_holder').crossSlide({
sleep: 2,
```

```
fade: 4

}, [

{ src: 'images/s1.jpg', dir: 'up'},

{ src: 'images/s2.jpg' , dir: 'down'  },

{ src: 'images/s3.jpg', dir: 'up' },

{ src: 'images/s4.jpg', dir: 'down' }


]);

&('a.specialLink[href^=#],a.hid_div[href^=#]').click (function() {


/*&('#form3').submit(); return false;*/

var popID = &(this).attr('rel'); //Get Popup Name

var popURL = &(this).attr('href'); //Get Popup href to define size

   //Pull Query & Variables from href URL

var query= popURL.split('?');

var dim= query[1].split('&');

var popWidth = dim[0].split('=')[1]; //Gets the first query string value

   //Fade in the Popup and add close button

&('#' + popID).fadeIn().css({ 'width': Number( popWidth ) }).prepend('<a href="#"
class="close"><img src="images/btn_close.jpg" class="btn_close" title="Close Window"
alt="Close" /></a>');


   //Define margin for center alignment (vertical   horizontal) - we add 80px to the
height/width to accomodate for the padding  and border width defined in the css

var popMargTop = (&('#' + popID).height() + 80) / 2;

var popMargLeft = (&('#' + popID).width() + 80) / 2;

   //Apply Margin to Popup

&('#' + popID).css({
```

```
        'margin-top' : -popMargTop,
        'margin-left' : -popMargLeft
    });
    //Fade in Background
&('body').append('<div id="fade"></div>'); //Add the fade layer to bottom of the body tag.
&('#fade').css({'filter' : 'alpha(opacity=80)'}).fadeIn(); //Fade in the fade layer - .css({'filter' : 'alpha(opacity=80)'}) is used to fix the IE Bug on fading transparencies
            &('#j').click();
return false;
});
//Close Popups and Fade Layer
&('a.close, #fade').live('click',  function cl() { //When clicking on the close or fade layer...
&('#fade , .popup_block').fadeOut(function() {
&('#fade, a.close').remove();  //fade them both out
    });
return false;
});
});
//-->
</script>

<script type="text/JavaScript">
<!--
var counter=0;
var images = new Array();
&('#j').click(function(){
            alert('j was clicked');});
```

```
function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}
function show()
{
alert("Working");
}
function adminLogin(){
}
function  win(){
//&('#e').click();
//alert();
//document.write("<div id=e><a href=create_user.php>hi</a></div>");
//document.location.href=('create_user.php').getAttribute('admin_login');
&('#news').click();
//<aadmin href="#?w=400"
//document.write("<b>hello<\/b>");

}
function MM_openBrWindow(theURL,winName,features) { //v2.0
window.open(theURL,winName,features);
}
</script>
<link href="file:///C|/wamp/www/FreeIM/css.css" rel="stylesheet" type="text/css" />
<style type="text/css">
```

```
<!--
@import url("css/css.css");
body {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
	background-image: url(images/bg.jpg);
	background-color: #6699FF;
}
.style5 {font-family: Georgia, "Times New Roman", Times, serif; font-size: 12px; }
.style6 {font-family: Georgia, "Times New Roman", Times, serif}
.style7 {font-size: 12px}
.style9 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; }
.style11 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; color: #FFFFFF;
}
a:link {
	text-decoration: none;
}
a:visited {
	text-decoration: none;
}
a:hover {
	text-decoration: none;
}
a:active {
	text-decoration: none;
```

```
}
.style13 {
	color: #FF0000;
	font-weight: bold;
}
.style18 {color: #02042D}
.style19 {font-size: 36px}
-->
</style></head>
<body>
<table width="980" height="500" border="0" align="center" cellpadding="0" cellspacing="0" bgcolor="#DD6C40">
<tr>
<td align="center" valign="top"><table width="800" height="500" border="0" cellpadding="0" cellspacing="0" bgcolor="#FFFFFB">
<tr>
<td width="602" height="200" align="center" valign="top" background="images/Corporate.jpg"><table width="780" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="615"> </td>
<td width="176" height="30" align="center" valign="middle" background="images/login.jpg"><span class="style11"><a href="#?w=400" rel="admin_login"  class="specialLink" id="admin">Admin login</a> |<a href="#?w=400" rel="user_login"  class="specialLink"> User login</a></span></td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
```

```
</table></td>

</tr>

<tr>

<td height="30" align="center" valign="middle"
background="images/link/link_01.jpg"><table width="770" border="0" cellspacing="0"
cellpadding="0">

<tr>

<td width="110"><span class="style9">Home</span></td>

<td align="left"><span class="style9">Create New Account </span></td>

<td width="69" align="left"><span class="style9">Deposit</span></td>

<td width="88" align="left"><span class="style9">Withdrawal</span></td>

<td width="156" align="left"><span class="style9">Statement of Account </span></td>

<td width="75" align="left"><span class="style9">Credit card </span></td>

<td width="104" onclick="MM_openBrWindow('about.php','','width=400,height=500')"><a
href="#">About us</a></td>

</tr>

</table></td>

</tr>

<tr>

<td align="center" valign="top"><table width="800" height="270" border="0"
cellpadding="0" cellspacing="0">

<tr>

<td width="200" align="center" valign="top"><br />

<table width="180" border="0" cellpadding="0" cellspacing="0" class="bdr1">

<tr>

<td height="23" background="images/mnu_Linl.jpg"><span class="style18">24 hrs Banking
Operations </span></td>

</tr>

<tr>
```

<td height="20" align="left" valign="baseline">NewsCredit Card Transactions </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">Bills Payment </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">Online Account Statements </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">Account Opening </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">Deposit / Withdrawals </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">Account Balance </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline"> </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline"> </td>

</tr>

</table>

<p>

<label></label>

```
</p></td>

<td width="600" align="center" valign="top">

                    <div id="admin_login" class="popup_block"><table width="400" height="150" border="0" cellpadding="0" cellspacing="0" class="bdr1">

<tr>

<td><form id="form1" name="form1" method="post" action="admin_login.php">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="52" colspan="2" align="center" valign="bottom"><img src="images/admin_login.jpg" alt="login" width="400" height="52" /></td>

</tr>

<tr>

<td width="133" height="30" align="center"><span class="style6 style7">Usename</span></td>

<td width="267"><label>

<input name="admin_user" type="text" class="textbox" id="admin_user" />

</label></td>

</tr>

<tr>

<td height="30" align="center"><span class="style6 style7">Password</span></td>

<td><label>

<input name="admin_pass" type="password" class="textbox" id="admin_pass" />

</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="Submit" type="submit" class="button" value="Login" />

</label></td>
```

```
</tr>

</table>

</form></td>

</tr>

</table></div>



<div id="user_login" class="popup_block">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0"
class="bdr1">

<tr>

<td><form id="form2" name="form2" method="post" action="user_login.php">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="52" colspan="2" align="center" valign="bottom"><img
src="images/user_login.jpg" alt="login" width="400" height="52" /></td>

</tr>

<tr>

<td width="133" height="30" align="left"><span class="style7">Account
number:</span></td>

<td width="267"><label>

<input name="user_user" type="text" class="textbox" id="user_user" />

</label></td>

</tr>

<tr>

<td height="30" align="left"><span class="style7">Pin code:</span></td>

<td><label>

<input name="user_pass" type="password" class="textbox" id="user_pass" />
```

```
</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="user_Submit" type="submit" class="button" id="user_Submit" value="Login"
/>

</label></td>

</tr>

</table>

</form></td>

</tr>

</table>

</div>

<table width="580" height="250" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="20"> </td>

</tr>

<tr>

<td height="230" align="center" valign="middle"><div id="image_holder"
class="slide"><img src="images/slide.gif" width="580" height="230" /></div></td>

</tr>

</table></td>

</tr>

</table>

<p class="style13"><br />

<span class="style19"><marquee>

        Security Guaranteed

</marquee></span></p></td>
```

```
</tr>

<tr>

<td align="center" valign="top" bordercolor="#DD6C40"
bgcolor="#DD6C40"> </td>

</tr>

</table></td>

</tr>

</table>

</body>

</html>

<?php

&accountNumber = &_POST['accountNumber'];

&surname = &_POST['surname'];

&firstname = &_POST['firstname'];

&accType = &_POST['accType'];

&mobile = &_POST['mobile'];

&email = &_POST['email'];

&dtDate = &_POST['dtDate'];

&address = &_POST['address'];

&amount = &_POST['amount'];

&n_name = &_POST['n_name'];

&n_mobile = &_POST['n_mobile'];

&n_address = &_POST['n_address'];

&cardno = &_POST['cardno'];

&accName = &_POST['surname'] . " " . &_POST['firstname'];

mysql_connect("localhost","root")

or die (mysql_error());
```

```
mysql_select_db("bank");

&create = " insert into tbl_account_info (accountNumber , surname ,
firstname,accountType,phone,email,dtDate,address,amount,n_name,n_phone,n_address,trans
action, cardno) values ('&accountNumber', '&surname'    ,
'&firstname','&accType','&mobile','&email','&dtDate','&address','&amount','&n_name','&n_
mobile','&n_address','Opening Acc.', '&cardno')";

&trans = "insert into tbl_transaction (accname, accNumber, transactionDesc, transactionDate,
cr, balance,dr) values ('&accName','&accountNumber', 'Opening Acc.',
'&dtDate','&amount','&amount','')";

mysql_query(&create) or die("error");

mysql_query(&trans);

?>

<?php

&money=&_POST['textfield7'];

&dt=&_POST['textfield8'];


&ms = "Fill the  transfer amount and Click continue";

mysql_connect("localhost","root")

or die (mysql_error());

mysql_select_db("bank");

if (&money !="")

{

session_start();

if(isset(&_SESSION['acount']))

{

&accno=&_SESSION['acount'] ;

&_SESSION['amt'] = &money;

&morkov = "select * from tbl_transaction where accNumber = '&accno'";

&detect = mysql_query(&morkov) ;//or die(mysql_error());
```

```
if (mysql_num_rows(&detect)<10)
{
header("Location: nn5.php");
 }
else
 {
//check transaction value
&tim =0;
&valu=0;
while (&details = mysql_fetch_object(&detect))
  {
&amt = "&details->DR";

if (&amt !=0)
  {
&valu =&valu +&amt;
&tim = &tim +1;
 }
  }
&avr= &valu / &tim;
&limitlow= &avr/2;
&limithigh = &avr * 3;
if ((&money <&limitlow) || (&money >&limithigh))
{
header("Location: nn5.php");
 }
else
```

```
 {
 // stop check
header("Location: nn4.php");
}
}
}
}
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>Modeling a Web - Based Security System in the Banking Industry</title>
<script type="text/javascript" src="jprototype.js"></script>
<script type="text/javascript" src="ajax1.js"></script>
<script type="text/javascript" src="jQuery.js"></script>
<style type="text/css">
#fade { /*--Transparent background layer--*/
        display: none; /*--hidden by default--*/
        /*background: #000; */
        background: #ffffff;
        position: fixed; left: 0; top: 0;
        width: 100%; height: 100%;
        opacity: .80;
        z-index: 1;
}
```

```
.popup_block{
	display: none;
	padding: 8px;
	border: 2px solid #ddd;
	float: left;
	font-size: 1.2em;
	position: fixed;
	top: 50%;
	left: 50%;
	/*overflow: scroll;*/
	/*height: 400px;*/
	/*width: 800px;*/
	/*height: 200px;*/
/*	width: 400px;*/
	/*overflow: scroll;*/
	z-index: 2;
	/*--CSS3 Box Shadows--*/
	-webkit-box-shadow: 0px 0px 20px #000;
	-moz-box-shadow: 0px 0px 20px #000;
	box-shadow: 0px 0px 20px #000;
	/*--CSS3 Rounded Corners--*/
	-webkit-border-radius: 10px;
	-moz-border-radius: 10px;
	border-radius: 10px;
	background-color: #ffffff;
	/*background-image: url(images/div_bg.jpg);*/
}
```

```
.hid_div{
display: none;
}
img.btn_close {
	float: right;
	margin: -10px -10px 0 0;
}
/*--Making IE6 Understand Fixed Positioning--*/
*html #fade {
	position: absolute;
}
*html .popup_block {
	position: absolute;
}
.specialLink {
	color: #ffffff;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
.divContent {
	font-family: "Trebuchet MS";
	font-size: 13px;
	color: #F4F4F4;
}
.specialLink1 {
	color: #999999;
	font-family: "Trebuchet MS";
```

```
	font-size: 12px;
}
.jbutton {
	color: #999999;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
ody {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
}td img {display: block;}
body {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
	background-color: #FFFFD2;
	background-image: url(images/bg.jpg);
}
</style>
<script type="text/javascript">
<!--
&(document).ready(function() {
&('a.specialLink[href^=#],a.hid_div[href^=#]').click (function() {
/*&('#form3').submit(); return false;*/
```

```
var popID = &(this).attr('rel'); //Get Popup Name

var popURL = &(this).attr('href'); //Get Popup href to define size

   //Pull Query & Variables from href URL

var query= popURL.split('?');

var dim= query[1].split('&');

var popWidth = dim[0].split('=')[1]; //Gets the first query string value

   //Fade in the Popup and add close button

&('#' + popID).fadeIn().css({ 'width': Number( popWidth ) }).prepend('<a href="#"
class="close"><img src="images/btn_close.jpg" class="btn_close" title="Close Window"
alt="Close" /></a>');

   //Define margin for center alignment (vertical   horizontal) - we add 80px to the
height/width to accomodate for the padding  and border width defined in the css

var popMargTop = (&('#' + popID).height() + 80) / 2;

var popMargLeft = (&('#' + popID).width() + 80) / 2;

   //Apply Margin to Popup

&('#' + popID).css({

      'margin-top' : -popMargTop,

      'margin-left' : -popMargLeft

   });

   //Fade in Background

&('body').append('<div id="fade"></div>'); //Add the fade layer to bottom of the body tag.

&('#fade').css({'filter' : 'alpha(opacity=80)'}).fadeIn(); //Fade in the fade layer - .css({'filter' :
'alpha(opacity=80)'}) is used to fix the IE Bug on fading transparencies

         &('#j').click();

return false;

});

//Close Popups and Fade Layer

&('a.close, #fade').live('click',  function cl() { //When clicking on the close or fade layer...
```

```
&('#fade , .popup_block').fadeOut(function() {
&('#fade, a.close').remove();  //fade them both out
    });
return false;
});


});
</script>
<script type="text/JavaScript">
<!--
&('#j').click(function(){
          alert('j was clicked');});
function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}
function show()
{
alert("Working");
}
function adminLogin(){
//&('#admin').click();
}
function  win(){
//&('#e').click();
//alert();
```

```
//document.write("<div id=e><a href=create_user.php>hi</a></div>");
//document.location.href=('create_user.php').getAttribute('admin_login');
&('#news').click();

//<aadmin href="#?w=400"
//document.write("<b>hello<\/b>");
}
function account_stmt(){
//alert("OK");
&('#stmt_form').submit();
}
function MM_displayStatusMsg(msgStr) { //v1.0
status=msgStr;
  document.MM_returnValue = true;
}
//-->
</script>
<link href="file:///C|/wamp/www/FreeIM/css.css" rel="stylesheet" type="text/css" />
<style type="text/css">
<!--
@import url("css/css.css");
body {
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
        background-image: url(images/bg.jpg);
```

```
}
.style5 {font-family: Georgia, "Times New Roman", Times, serif; font-size: 12px; }
.style6 {font-family: Georgia, "Times New Roman", Times, serif}
.style7 {font-size: 12px}
.style9 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; }
.style11 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; color: #FFFFFF;
}
.style13 {
	font-family: Georgia, "Times New Roman", Times, serif;
	font-size: 14px;
	color: #FFFFFF;
}
a:link {
	text-decoration: none;
}
a:visited {
	text-decoration: none;
}
a:hover {
	text-decoration: none;
}
a:active {
	text-decoration: none;
}
.style14 {
	font-size: 24px;
	font-weight: bold;
```

```
        color: #FF0000;
}
.style15 {
        color: #FF0000;
        font-weight: bold;
}
.style16 {
        color: #DE6D45;
        font-weight: bold;
}
.style17 {
        color: #DD6C44;
        font-weight: bold;
}
-->
</style></head>

<body>
<table width="980" height="500" border="0" align="center" cellpadding="0"
cellspacing="0" bgcolor="#DD6C44">
<tr>
<td align="center" valign="top"><table width="800" height="500" border="0"
cellpadding="0" cellspacing="0" bgcolor="#FFFFFB">
<tr>
<td width="602" height="200" align="center" valign="top"
background="images/Corporate.jpg"><table width="780" border="0" cellspacing="0"
cellpadding="0">
<tr>
```

<td colspan="2"> </td>

<td width="129" height="30" align="center" valign="middle" background="images/login.jpg"> </td>

</tr>

<tr>

<td width="303"> </td>

<td colspan="2" align="right">e <?php echo &name ?></td>

</tr>

</table></td>

</tr>

<tr>

<td height="30" align="center" valign="middle" background="images/link/link_01.jpg"><table width="770" border="0" cellspacing="0" cellpadding="0">

<tr>

<td width="104" bgcolor="#D96840"> </td>

<td width="60" align="left" bgcolor="#D96840"></td>

<td width="109" align="left" bgcolor="#D96840"> </td>

<td width="75" align="left" bgcolor="#D96840"> </td>

<td width="85" align="left" bgcolor="#D96840"> </td>

<td width="154" align="left" bgcolor="#D96840"></td>

<td width="72" align="left" bgcolor="#D96840"></td>

<td width="111" bgcolor="#D96840"> </td>

</tr>

</table></td>

</tr>

<tr>

<td align="center" valign="top"><table width="800" height="270" border="0" cellpadding="0" cellspacing="0">

<tr>

<td width="200" align="center" valign="top">

<table width="180" border="0" cellpadding="0" cellspacing="0" class="bdr1">

<tr>

<td height="23" background="images/mnu_Linl.jpg"> Account No and Pin Code Verified

  </td>

</tr>

<tr>

<td height="20" align="left" valign="baseline">News</td>

</tr>

</table>

<label></label>

</td>

<td width="600" align="center" valign="top">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0" class="bdr1">

<tr>

<td><form id="form1" name="form1" method="post" action="admin_login.php">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">

<tr>

```
<td height="52" colspan="2" align="center" valign="bottom"><img
src="images/admin_login.jpg" alt="login" width="400" height="52" /></td>

</tr>

<tr>

<td width="133" height="30" align="center"><span class="style6
style7">Usename</span></td>

<td width="267"><label>

<input name="admin_user" type="text" class="textbox" id="admin_user" />

</label></td>

</tr>

<tr>

<td height="30" align="center"><span class="style6 style7">Password</span></td>

<td><label>

<input name="admin_pass" type="password" class="textbox" id="admin_pass" />

</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="Submit" type="submit" class="button" value="Submit" />

</label></td>

</tr>

</table>

</form></td>

</tr>

</table></div>


<div id="user_login" class="popup_block">
```

```
<table width="400" height="150" border="0" cellpadding="0" cellspacing="0"
class="bdr1">

<tr>

<td><form id="form2" name="form2" method="post" action="">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="52" colspan="2" align="center" valign="bottom"><img
src="images/user_login.jpg" alt="login" width="400" height="52" /></td>

</tr>

<tr>

<td width="133" height="30" align="center"><span class="style7">Pin code</span></td>

<td width="267"><label>

<input name="user_user" type="text" class="textbox" id="user_user" />

</label></td>

</tr>

<tr>

<td height="30" align="center"><span class="style7">Password</span></td>

<td><label>

<input name="user_pass" type="password" class="textbox" id="user_pass" />

</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="user_Submit" type="submit" class="button" id="user_Submit"
value="Submit" />

</label></td>

</tr>

</table>
```

```
</form></td>

</tr>

</table>

</div>

<div id="div_balance" class="popup_block" align="left"><?php echo "Account name: " . &name . ". Account balance: " . &balance . "."?></div>

<div id="transfer" class="popup_block"><?php include "transfer.php" ?></div>

<table width="580" height="250" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="20"><div align="center"><span class="style14">Credit Card Cash Transfer</span></div></td>

</tr>

<tr>

<td height="230" align="center" valign="top"><form id="form3" name="form3" method="post" action="">

<table width="500" border="0" cellspacing="0" cellpadding="0">

<tr>

<td colspan="2"><span class="style16">Multi-agents Authentication</span></td>

</tr>

<tr>

<td width="200"><strong>Transaction Amount</strong></td>

<td width="300"><div align="left">

<label>

<input type="text" name="textfield7" />

</label>

</div></td>

</tr>

<tr>
```

```
<td><strong>Date</strong></td>
<td><label>
<div align="left">
<input name="textfield8" type="text" value="<?php echo date('Y-m-d'); ?>" />
yy-mm-dd</div>
</label></td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
<tr>
<td><div align="right">
<label>
<input type="submit" name="Submit2" value="Continue" />
</label>
</div></td>
<td> </td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
```

```
</table>

</form></td>

</tr>

</table></td>

</tr>

<tr>

<td height="50" colspan="2" align="center" valign="top"
bgcolor="#DD6C44">&amp;nbsp;</td>

</tr>

</table>

<p><div  id="stmt_div" class="popup_block"><form id="stmt_form" name="stmt_form"
method="post" action="statement.php">

<table width="400" height="60" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="30" colspan="2" align="center" valign="bottom"><img
src="images/fin_trans.jpg" width="400" height="30" /></td>

</tr>

<tr>

<td width="133" height="30" align="center"><span class="style7 style1">Account number
</span></td>

<td width="267"><label>

<input name="accNumber" type="text" class="textbox" id="accNumber" value="<?php echo
&amp;user ?>" />

</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="user_Submit" type="submit" class="button" id="user_Submit"
value="Continue&amp;gt;&amp;gt;" />
```

```
</label></td>
</tr>
</table>
</form></div><?php echo &ms; ?><br />
</p>
</td>
</tr>
</table></td>
</tr>
</table>
</body>
</html>
<?php

&fna=&_POST['textfield'];
&sna=&_POST['textfield2'];
&acn=&_POST['textfield3'];
&cd=&_POST['textfield4'];

&ac2=&_POST['textfield6'];
&amt=&_POST['textfield7'];
&dt=&_POST['textfield8'];

&bk=&_POST['textfield9'];
&ms = "Fill the transfer form and Click Transfer";

mysql_connect("localhost","root")
```

```
or die (mysql_error());

mysql_select_db("bank");


session_start();

if(isset(&_SESSION['acount']))

{

&ac1=&_SESSION['acount'] ;

&mo=&_SESSION['amt'] ;







}









if (&acn !="")

{


&select5 = "select * from tbl_account_info where surname= '&sna' and firstname = '&fna'
and accountNumber = '&acn' and cardno = '&cd'";

&login5 = mysql_query(&select5) ;//or die(mysql_error());

if (mysql_num_rows(&login5)==1)

{

&welcome = &fna +" " +&sna;

&card = "select sum(dr) as wt, sum(cr) as pd from tbl_transaction where accNumber =
'&acn'";

&card1 = mysql_query(&card);
```

```
if (mysql_num_rows(&card1)==1)
{
&gAmount = mysql_fetch_object(&card1);
&dra = "&gAmount->wt";
&dep = "&gAmount->pd";
&tAmount= &dep - &dra;
if (&tAmount>=&amt)
{
        &balance = &tAmount - &amt;

        &na2= &fna. " ". &sna;
        &des ="Money transfered to account no: ". &ac2 ." by self";
        &payment = "insert into tbl_transaction(
accName,accNumber,transactionDesc,DR,CR,transactionDate,balance) values
('&na2','&acn','&des', '&amt','0','&dt','&balance')";
        mysql_query(&payment);

// post to credit the account
&card = "select * from tbl_account_info where accountNumber = '&ac2'";
&card1 = mysql_query(&card);
if (mysql_num_rows(&card1)==1)
{
&gAmount = mysql_fetch_object(&card1);
&nn1 = "&gAmount->surname";
&nn2 = "&gAmount->firstname";
}
&nna= &nn1 . " ". &nn2;
```

```
&card = "select sum(dr) as wt, sum(cr) as pd from tbl_transaction where accNumber =
'&ac2'";

&card1 = mysql_query(&card);

if (mysql_num_rows(&card1)==1)

{

&gAmount = mysql_fetch_object(&card1);

&dra = "&gAmount->wt";

&dep = "&gAmount->pd";


&tAmount= &dep - &dra;


        &balance = &tAmount + &amt;


        &na2= &fna. " ". &sna;

        &des ="Credit through transfer by ". &na2 ;

        &payment = "insert into tbl_transaction(
accName,accNumber,transactionDesc,DR,CR,transactionDate,balance, bank) values
('&nna','&ac2','&des', '0','&amt','&dt','&balance','&bk')";

        mysql_query(&payment);


        }

        &ms = "Transaction completed successfully";



header('location: nn8.php');

}

else

{
```

/// Amount no reach

&ms = "Your account balance is not enough for the transfer, reduce the amount and try again";

}

}

else

{

&ms = "The Account no you entered is wrong";

}

}

else

{

&ms = "The card no or the Account No or account name you entered is wrong";

}

}

?>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>Credit card fraud detection system</title>
<script type="text/javascript" src="jprototype.js"></script>
<script type="text/javascript" src="ajax1.js"></script>
<script type="text/javascript" src="jQuery.js"></script>



<style type="text/css">
#fade { /*--Transparent background layer--*/
	display: none; /*--hidden by default--*/
	/*background: #000; */
	background: #ffffff;

	position: fixed; left: 0; top: 0;
	width: 100%; height: 100%;
	opacity: .80;
	z-index: 1;
}
.popup_block{
	display: none;
	padding: 8px;
	border: 2px solid #ddd;
	float: left;
	font-size: 1.2em;
	position: fixed;
	top: 50%;
```

```
        left: 50%;
        /*overflow: scroll;*/
        /*height: 400px;*/
        /*width: 800px;*/
        /*height: 200px;*/
/*      width: 400px;*/
        /*overflow: scroll;*/
        z-index: 2;
        /*--CSS3 Box Shadows--*/
        -webkit-box-shadow: 0px 0px 20px #000;
        -moz-box-shadow: 0px 0px 20px #000;
        box-shadow: 0px 0px 20px #000;
        /*--CSS3 Rounded Corners--*/
        -webkit-border-radius: 10px;
        -moz-border-radius: 10px;
        border-radius: 10px;
        background-color: #ffffff;
        /*background-image: url(images/div_bg.jpg);*/
}
.hid_div{
display: none;
}
img.btn_close {
        float: right;
        margin: -10px -10px 0 0;
}
/*--Making IE6 Understand Fixed Positioning--*/
```

```
*html #fade {
	position: absolute;
}
*html .popup_block {
	position: absolute;
}
.specialLink {
	color: #ffffff;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
.divContent {
	font-family: "Trebuchet MS";
	font-size: 13px;
	color: #F4F4F4;
}
.specialLink1 {
	color: #999999;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
.jbutton {
	color: #999999;
	font-family: "Trebuchet MS";
	font-size: 12px;
}
ody {
```

```
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
}td img {display: block;}
body {
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
        background-color: #FFFFD2;
        background-image: url(images/bg.jpg);

}

</style>

<script type="text/javascript">
<!--
&(document).ready(function() {
        //Code goes here

        //When you click on a link with class of specialLink and the href starts with a #

&('a.specialLink[href^=#],a.hid_div[href^=#]').click (function() {

/*&('#form3').submit(); return false;*/
```

```
var popID = &(this).attr('rel'); //Get Popup Name

var popURL = &(this).attr('href'); //Get Popup href to define size


   //Pull Query & Variables from href URL

var query= popURL.split('?');

var dim= query[1].split('&');

var popWidth = dim[0].split('=')[1]; //Gets the first query string value


   //Fade in the Popup and add close button

&('#' + popID).fadeIn().css({ 'width': Number( popWidth ) }).prepend('<a href="#"
class="close"><img src="images/btn_close.jpg" class="btn_close" title="Close Window"
alt="Close" /></a>');


   //Define margin for center alignment (vertical   horizontal) - we add 80px to the
height/width to accommodate for the padding  and border width defined in the css

var popMargTop = (&('#' + popID).height() + 80) / 2;

var popMargLeft = (&('#' + popID).width() + 80) / 2;


   //Apply Margin to Popup

&('#' + popID).css({

      'margin-top' : -popMargTop,

      'margin-left' : -popMargLeft

   });


   //Fade in Background

&('body').append('<div id="fade"></div>'); //Add the fade layer to bottom of the body tag.
```

```
&('#fade').css({'filter' : 'alpha(opacity=80)'}).fadeIn(); //Fade in the fade layer - .css({'filter' : 'alpha(opacity=80)'}) is used to fix the IE Bug on fading transparencies

        &('#j').click();

return false;




});



//Close Popups and Fade Layer

&('a.close, #fade').live('click',  function cl() { //When clicking on the close or fade layer...

&('#fade , .popup_block').fadeOut(function() {

&('#fade, a.close').remove();  //fade them both out

    });

return false;

});







});


//-->

</script>

<script type="text/JavaScript">

<!--

&('#j').click(function(){

        alert('j was clicked');});
```

```
function MM_preloadImages() { //v3.0
var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

function show()
{
alert("Working");
}
function adminLogin(){

//&('#admin').click();

}

function  win(){
//&('#e').click();
//alert();
//document.write("<div id=e><a href=create_user.php>hi</a></div>");
//document.location.href=('create_user.php').getAttribute('admin_login');
&('#news').click();
//<aadmin href="#?w=400"
//document.write("<b>hello<\/b>");
```

```
}
function account_stmt(){
//alert("OK");
&('#stmt_form').submit();
}

function MM_displayStatusMsg(msgStr) { //v1.0
status=msgStr;
  document.MM_returnValue = true;
}
//-->
</script>
<link href="file:///C|/wamp/www/FreeIM/css.css" rel="stylesheet" type="text/css" />
<style type="text/css">
<!--
@import url("css/css.css");
body {
	margin-left: 0px;
	margin-top: 0px;
	margin-right: 0px;
	margin-bottom: 0px;
	background-image: url(images/bg.jpg);
}
.style5 {font-family: Georgia, "Times New Roman", Times, serif; font-size: 12px; }
.style6 {font-family: Georgia, "Times New Roman", Times, serif}
.style7 {font-size: 12px}
.style9 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; }
```

```
.style11 {font-family: Verdana, Arial, Helvetica, sans-serif; font-size: 12px; color: #FFFFFF;
}

.style13 {
	font-family: Georgia, "Times New Roman", Times, serif;
	font-size: 14px;
	color: #FFFFFF;
}
a:link {
	text-decoration: none;
}
a:visited {
	text-decoration: none;
}
a:hover {
	text-decoration: none;
}
a:active {
	text-decoration: none;
}
.style14 {
	font-size: 24px;
	font-weight: bold;
	color: #FF0000;
}
.style15 {
	color: #FF0000;
	font-weight: bold;
```

```
}
.style16 {
	color: #DE6D45;
	font-weight: bold;
}
.style17 {
	color: #DD6C44;
	font-weight: bold;
}
-->
</style></head>

<body>
<table width="980" height="500" border="0" align="center" cellpadding="0" cellspacing="0" bgcolor="#DD6C44">
<tr>
<td align="center" valign="top"><table width="800" height="500" border="0" cellpadding="0" cellspacing="0" bgcolor="#FFFFFB">
<tr>
<td width="602" height="200" align="center" valign="top" background="images/Corporate.jpg"><table width="780" border="0" cellspacing="0" cellpadding="0">
<tr>
<td colspan="2"> </td>
<td width="129" height="30" align="center" valign="middle" background="images/login.jpg"> </td>
</tr>
<tr>
<td width="303"> </td>
```

<td colspan="2" align="right">e <?php echo &name ?></td>

</tr>

</table></td>

</tr>

<tr>

<td height="30" align="center" valign="middle" background="images/link/link_01.jpg"><table width="770" border="0" cellspacing="0" cellpadding="0">

<tr>

<td width="104" bgcolor="#D96840"> </td>

<td width="60" align="left" bgcolor="#D96840"></td>

<td width="109" align="left" bgcolor="#D96840"> </td>

<td width="75" align="left" bgcolor="#D96840"> </td>

<td width="85" align="left" bgcolor="#D96840"> </td>

<td width="154" align="left" bgcolor="#D96840"></td>

<td width="72" align="left" bgcolor="#D96840"></td>

<td width="111" bgcolor="#D96840"> </td>

</tr>

</table></td>

</tr>

<tr>

<td align="center" valign="top"><table width="800" height="270" border="0" cellpadding="0" cellspacing="0">

<tr>

<td width="200" align="center" valign="top">

<table width="180" border="0" cellpadding="0" cellspacing="0" class="bdr1">

```
<tr>

<td height="23" background="images/mnu_Linl.jpg"><p>Account No and Pin Code
Verified <img src="images/check.gif" width="21" height="22" /></p>

<p><img src="images/7.jpg" width="200" height="150" /></p>

<p>Multi-agentsssss  Verified<img src="images/check.gif" width="21" height="22" /></p>

<p> </p></td>

</tr>

<tr>

<td height="20" align="left" valign="baseline"><span class="style5"><a href="#?w=400"
rel="user_login"  class="hid_div" id="news">News</a><a
href="finger/Fingerverify.exe"></a></span></td>

</tr>

</table>

<p>

<label></label>

</p></td>

<td width="600" align="center" valign="top">


                    <div id="admin_login" class="popup_block"><table width="400"
height="150" border="0" cellpadding="0" cellspacing="0" class="bdr1">

<tr>

<td><form id="form1" name="form1" method="post" action="admin_login.php">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="52" colspan="2" align="center" valign="bottom"><img
src="images/admin_login.jpg" alt="login" width="400" height="52" /></td>

</tr>

<tr>
```

```
<td width="133" height="30" align="center"><span class="style6
style7">Usename</span></td>

<td width="267"><label>

<input name="admin_user" type="text" class="textbox" id="admin_user" />

</label></td>

</tr>

<tr>

<td height="30" align="center"><span class="style6 style7">Password</span></td>

<td><label>

<input name="admin_pass" type="password" class="textbox" id="admin_pass" />

</label></td>

</tr>

<tr>

<td height="38" colspan="2" align="center" valign="middle"><label>

<input name="Submit" type="submit" class="button" value="Submit" />

</label></td>

</tr>

</table>

</form></td>

</tr>

</table></div>


<div id="user_login" class="popup_block">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0"
class="bdr1">

<tr>

<td><form id="form2" name="form2" method="post" action="">

<table width="400" height="150" border="0" cellpadding="0" cellspacing="0">
```

```
<tr>
<td height="52" colspan="2" align="center" valign="bottom"><img
src="images/user_login.jpg" alt="login" width="400" height="52" /></td>
</tr>
<tr>
<td width="133" height="30" align="center"><span class="style7">Pin code</span></td>
<td width="267"><label>
<input name="user_user" type="text" class="textbox" id="user_user" />
</label></td>
</tr>
<tr>
<td height="30" align="center"><span class="style7">Password</span></td>
<td><label>
<input name="user_pass" type="password" class="textbox" id="user_pass" />
</label></td>
</tr>
<tr>
<td height="38" colspan="2" align="center" valign="middle"><label>
<input name="user_Submit" type="submit" class="button" id="user_Submit"
value="Submit" />
</label></td>
</tr>
</table>
</form></td>
</tr>
</table>
</div>
```

<?php echo "Account name: " . &name . ". Account balance: " . &balance . "."?>

<?php include "transfer.php" ?>

<table width="580" height="250" border="0" cellpadding="0" cellspacing="0">

<tr>

<td height="20"> Credit Card Cash Transfer </td>

</tr>

<tr>

<td height="230" align="center" valign="top"><form id="form3" name="form3" method="post" action="">

<table width="500" border="0" cellspacing="0" cellpadding="0">

<tr>

<td> </td>

<td> </td>

</tr>

<tr>

<td width="200">First Name </td>

<td width="300">

<label>

<input type="text" name="textfield" />

</label>

</td>

</tr>

<tr>

<td>Surname</td>

<td>

<label>

<input type="text" name="textfield2" />

</label>

</td>

</tr>

<tr>

<td>Account No </td>

<td>

<label>

<input name="textfield3" type="text" value="<?php echo &ac1; ?>" />

</label>

</td>

</tr>

<tr>

<td>Card No </td>

<td>

<label>

<input type="password" name="textfield4" />

</label>

</td>

</tr>

<tr>

<td>Cash Transfer To </td>

<td> </td>

</tr>

<tr>

<td>Credit Account</td>

```
<td> </td>
</tr>
<tr>
<td><strong>Account No </strong></td>
<td><div align="left">
<label>
<input type="text" name="textfield6" />
</label>
</div></td>
</tr>
<tr>
<td><strong>Amount</strong></td>
<td><div align="left">
<label>
<input name="textfield7" type="text" value="<?php echo &mo; ?>" />
</label>
</div></td>
</tr>
<tr>
<td><strong>Bank</strong></td>
<td><div align="left">
<label>
<input type="text" name="textfield9" />
</label>
</div></td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td><label>
<div align="left">
```

```
<input name="textfield8" type="text" value="<?php echo date('Y-m-d'); ?>" />
yy-mm-dd</div>
</label></td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
<tr>
<td><div align="right">
<label>
<input type="submit" name="Submit2" value="Transfer" />
</label>
</div></td>
<td> </td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
<tr>
<td> </td>
<td> </td>
</tr>
</table>
</form></td>
</tr>
</table></td>
</tr>
<tr>
<td height="50" colspan="2" align="center" valign="top"
bgcolor="#DD6C44"> </td>
</tr>
</table>
```

```
<td width="133" height="30" align="center"><span class="style7 style1">Account number
</span></td>
<td width="267"><label>
<input name="accNumber" type="text" class="textbox" id="accNumber" value="<?php echo
&user ?>" />
</label></td>
</tr>
<tr>
<td height="38" colspan="2" align="center" valign="middle"><label>
<input name="user_Submit" type="submit" class="button" id="user_Submit"
value="Continue&gt;&gt;" />
</label></td>
</tr>
</table>
</form></div><?php echo &ms; ?><br />
</p>
</td>
</tr>
</table></td>
</tr>
</table>
</body>
</html>
```

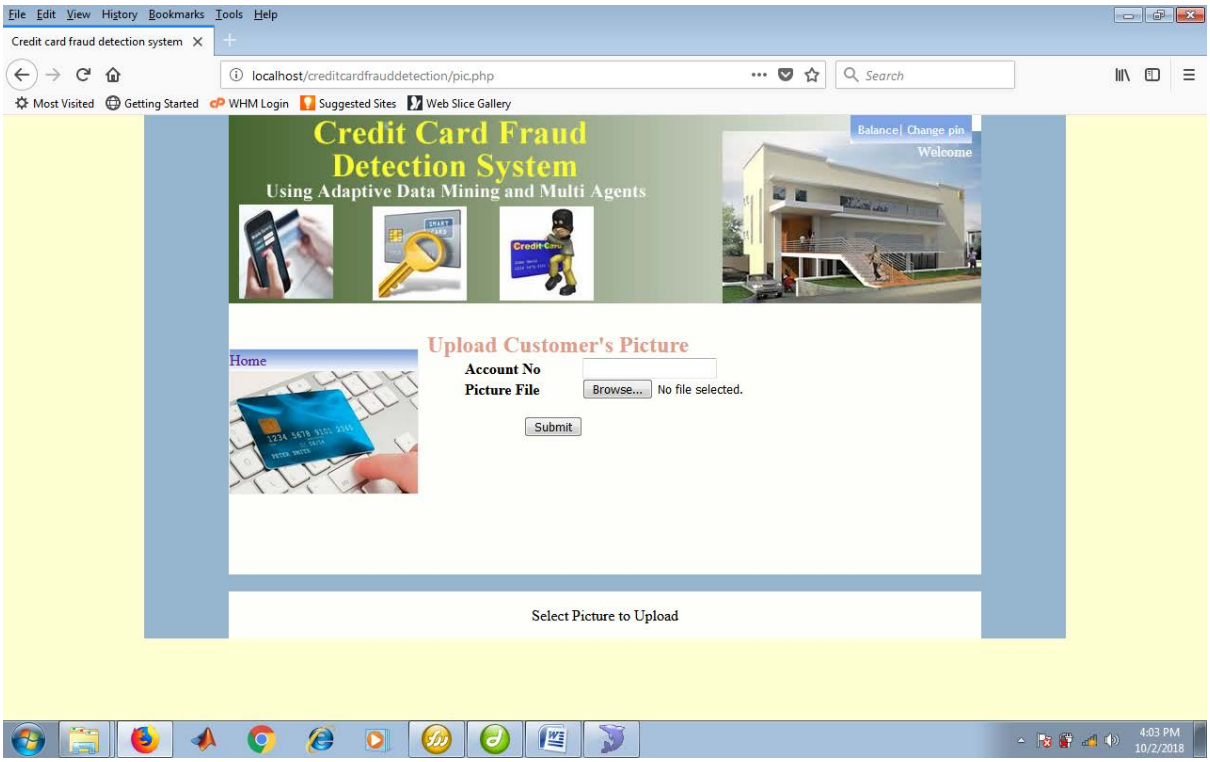
APPENDIX B

SAMPLE OUTPUTS

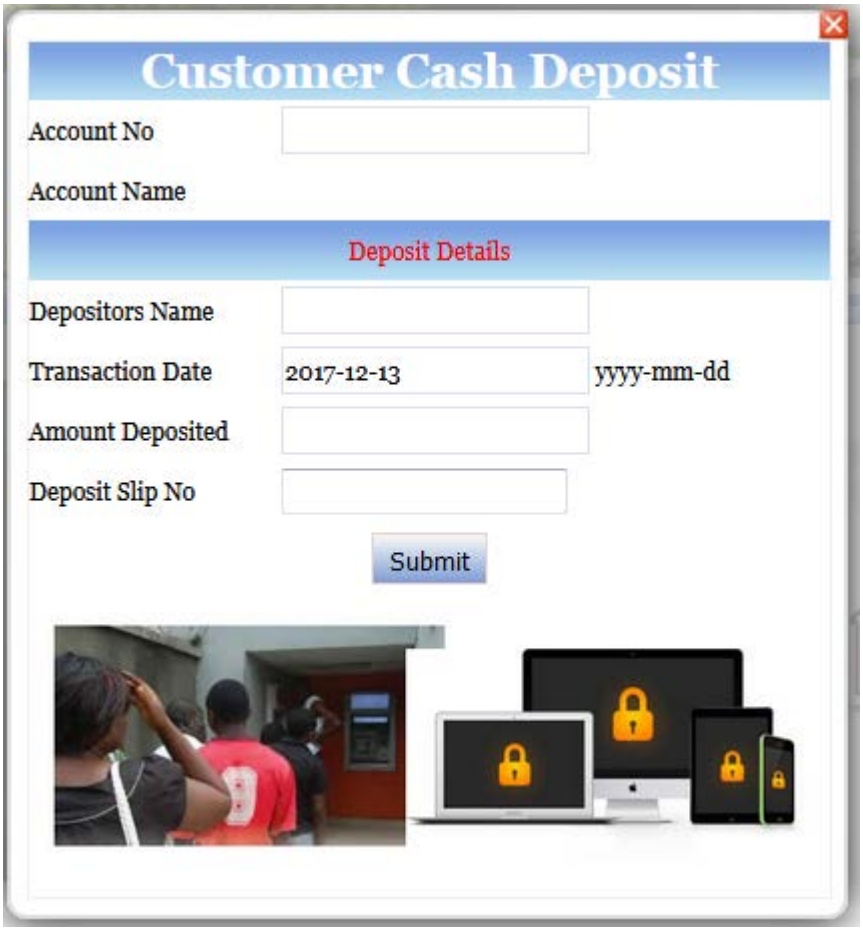
Staff Login Form

Customer Login Form

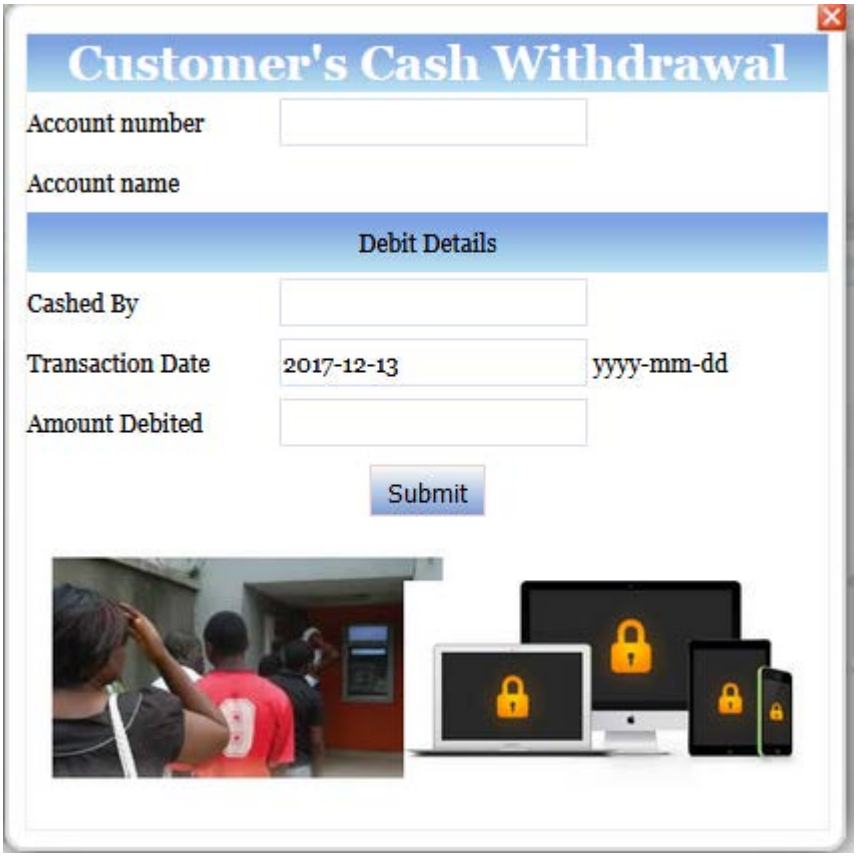
Account Opening Form



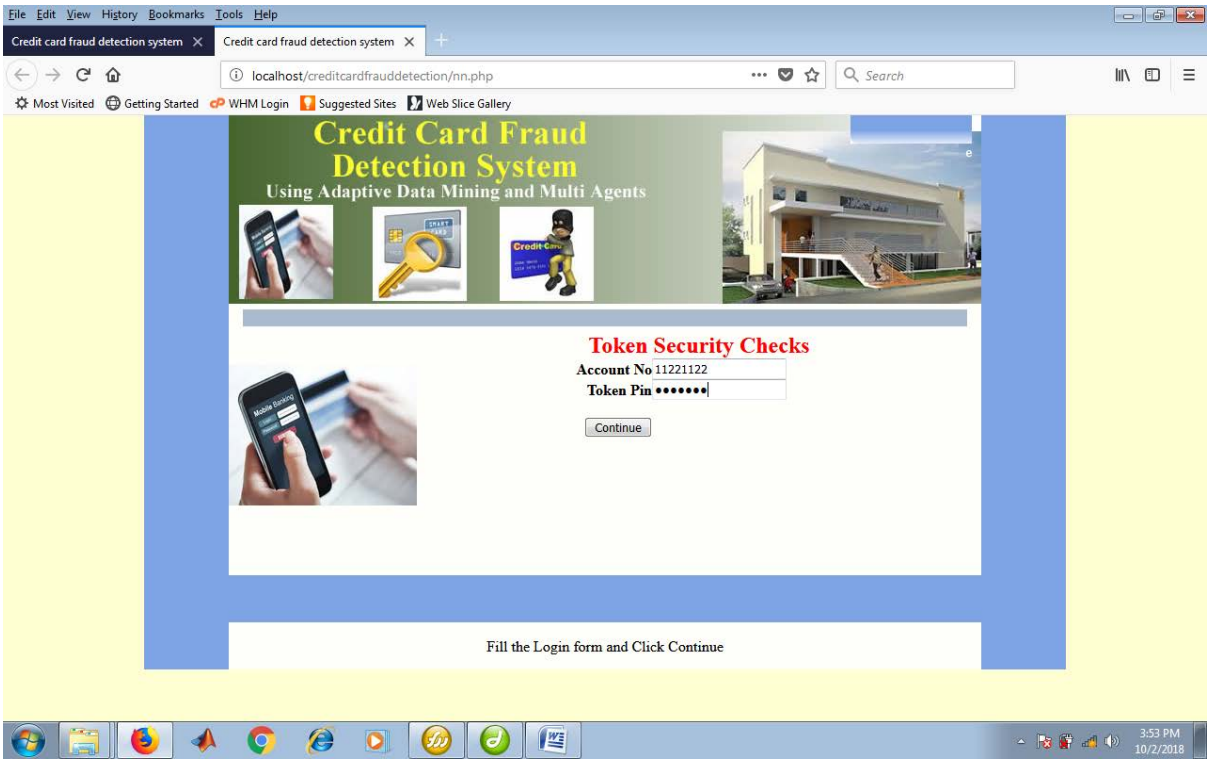
Customer's Picture Upload Form



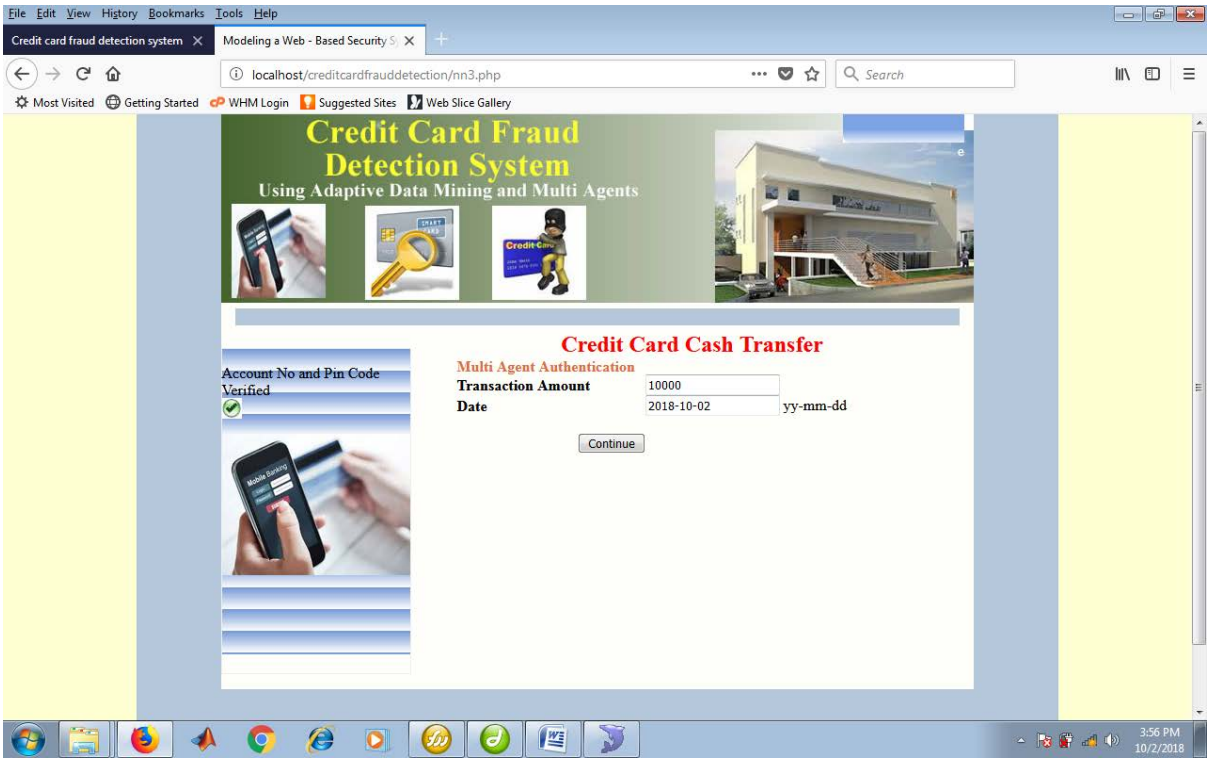
Customer Cash Deposit Form



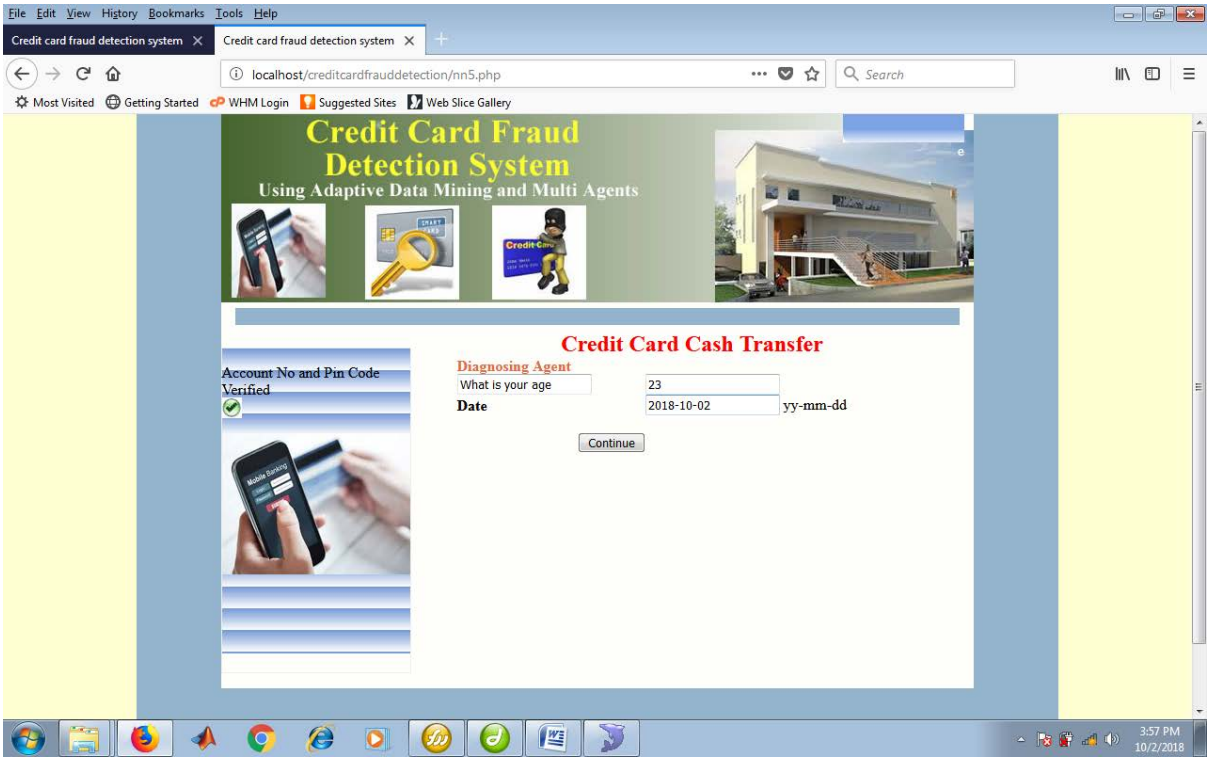
Customer Cash Withdrawal Form



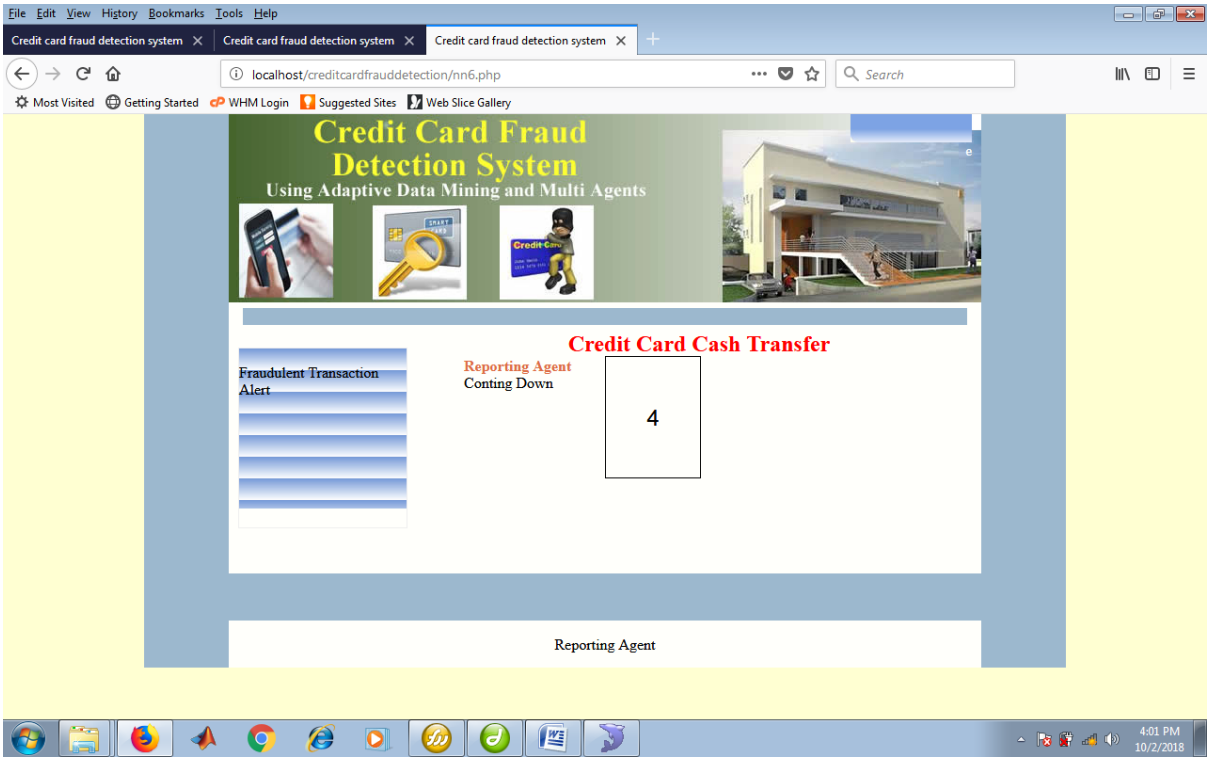
Customer Account number and token verification Form



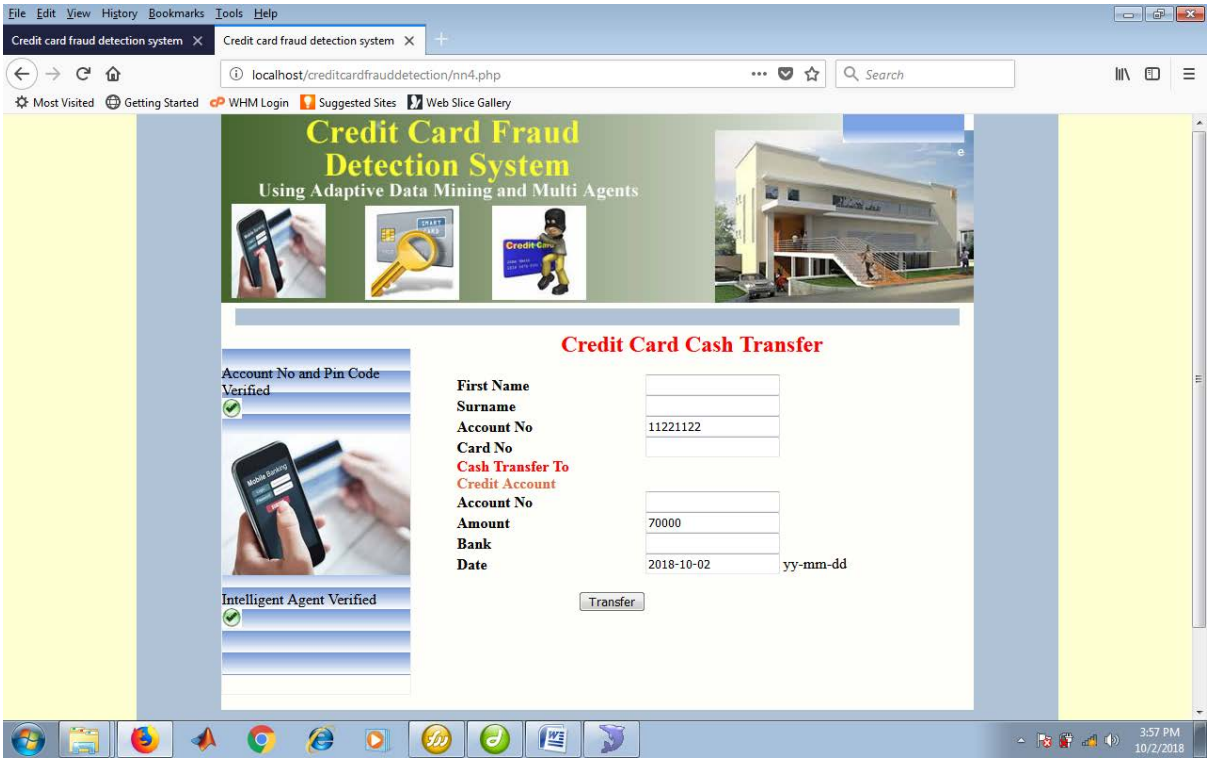
Customer Transaction profiling Form



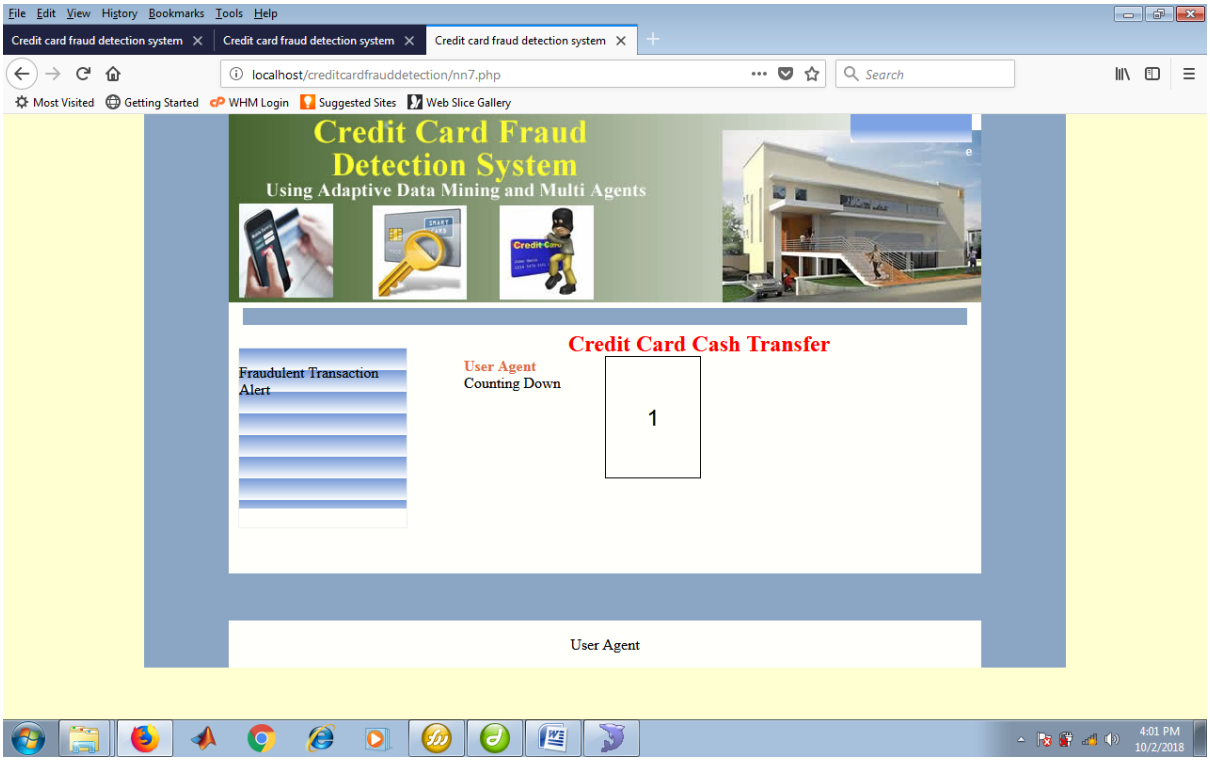
Customer secret question Form



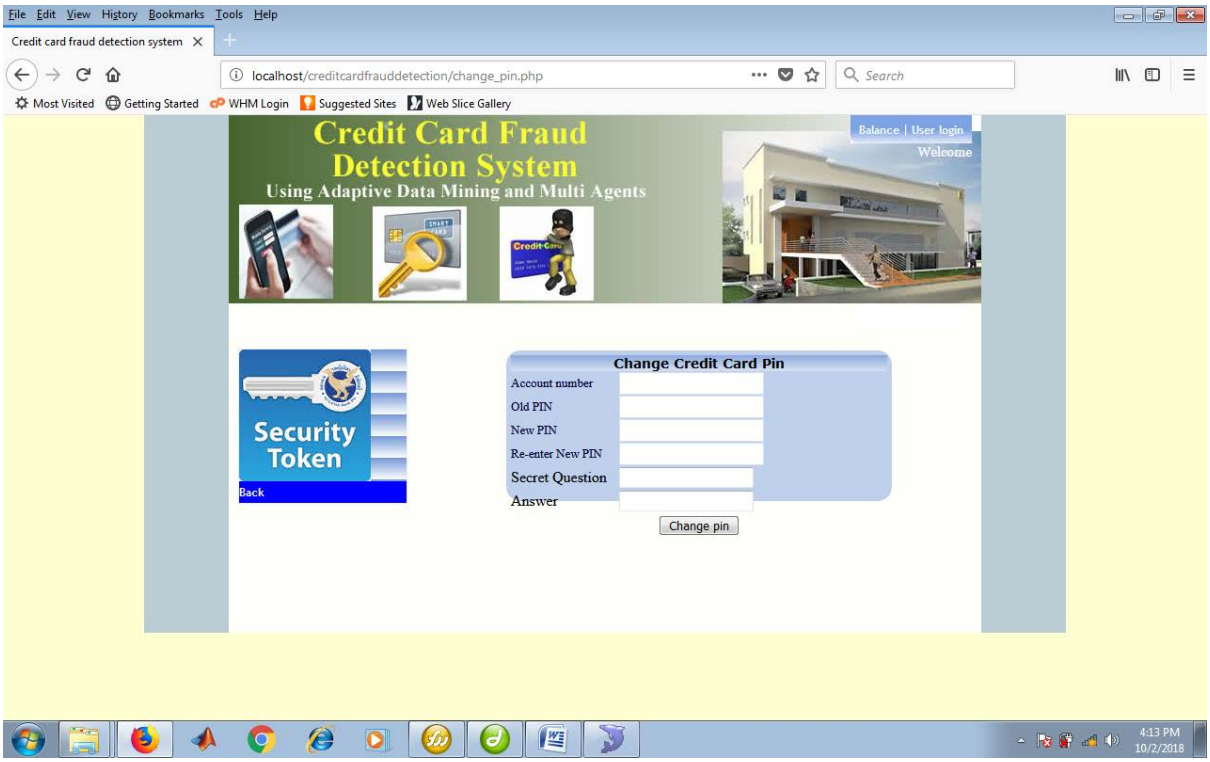
Reporting Agent Form



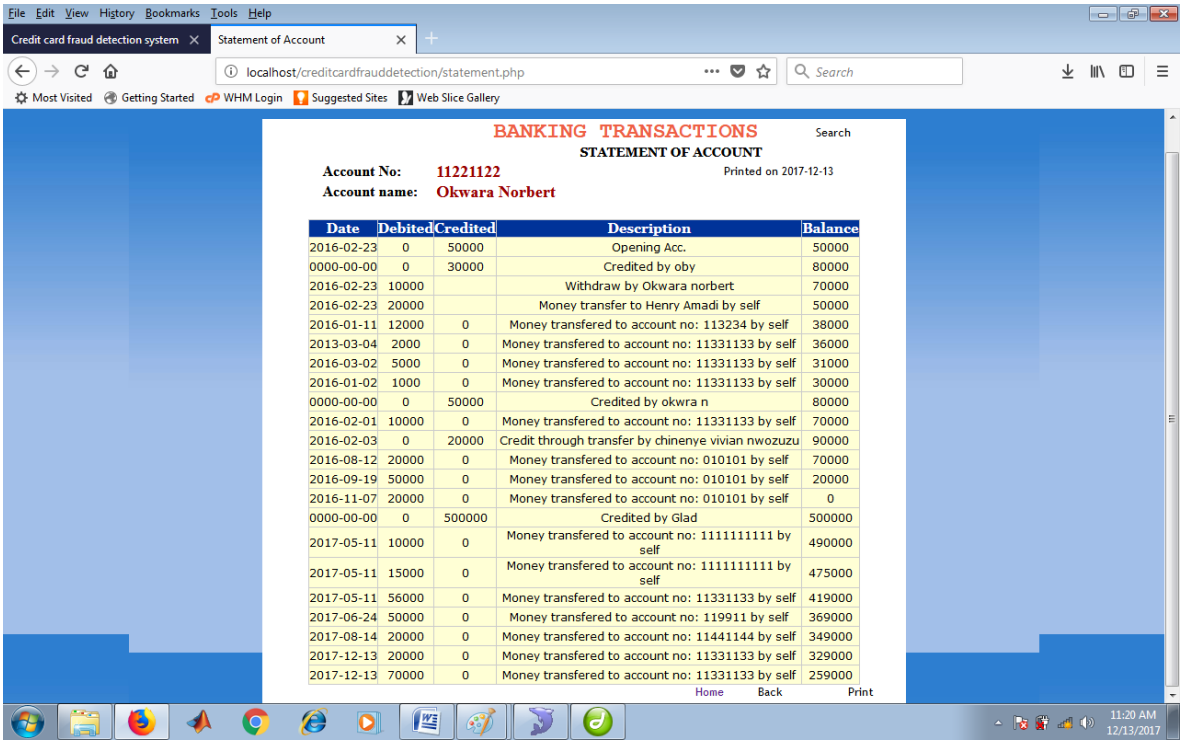
Credit card details verification Form



Credit card transaction agent fraud detection Form



Customer account pin change Form



Date	Debited	Credited	Description	Balance
2016-02-23	0	50000	Opening Acc.	50000
0000-00-00	0	30000	Credited by oby	80000
2016-02-23	10000		Withdraw by Okwara norbert	70000
2016-02-23	20000		Money transfer to Henry Amadi by self	50000
2016-01-11	12000	0	Money transfered to account no: 113234 by self	38000
2013-03-04	2000	0	Money transfered to account no: 11331133 by self	36000
2016-03-02	5000	0	Money transfered to account no: 11331133 by self	31000
2016-01-02	1000	0	Money transfered to account no: 11331133 by self	30000
0000-00-00	0	50000	Credited by okwra n	80000
2016-02-01	10000	0	Money transfered to account no: 11331133 by self	70000
2016-02-03	0	20000	Credit through transfer by chinenye vivian nwozuzu	90000
2016-08-12	20000	0	Money transfered to account no: 010101 by self	70000
2016-09-19	50000	0	Money transfered to account no: 010101 by self	20000
2016-11-07	20000	0	Money transfered to account no: 010101 by self	0
0000-00-00	0	500000	Credited by Glad	500000
2017-05-11	10000	0	Money transfered to account no: 1111111111 by self	490000
2017-05-11	15000	0	Money transfered to account no: 1111111111 by self	475000
2017-05-11	56000	0	Money transfered to account no: 11331133 by self	419000
2017-06-24	50000	0	Money transfered to account no: 119911 by self	369000
2017-08-14	20000	0	Money transfered to account no: 11441144 by self	349000
2017-12-13	20000	0	Money transfered to account no: 11331133 by self	329000
2017-12-13	70000	0	Money transfered to account no: 11331133 by self	259000

Account Statement

Fraud Detection Alert

Date	Time	Amount	Action Taken
2017-05-11	10:40	150000.00	Transaction Blocked
2017-05-11	10:42	160000.00	Transaction Blocked
2017-05-11	10:44	160000.00	Transaction Blocked
2017-06-24	04:22	500000.00	Transaction Blocked
2017-06-24	04:22	500000.00	Transaction Blocked
2017-06-24	04:28	150000.00	Transaction Blocked
2017-06-24	04:28	150000.00	Transaction Blocked
2017-12-13	11:18	150000.00	Transaction Blocked
2017-12-13	11:18	150000.00	Transaction Blocked

Back

Fraud Transaction Alert