Computer Science

E-ISSN No : 2581-6195 | Volume : 1 | Issue : 5 | December 2018

AN ENHANCED MODEL FOR BANK FRAUD DETECTION IN NIGERIAN

Amanze, B.C.[1], Onukwugha, C.G[2]

ABSTRACT

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Conventional method of identification based on possession of pin and password are not all together reliable. This paper aimed at design and develop an enhanced model for bank fraud detection in Nigeria banks using data mining technique and multi- agents that combine evidence from current as well as past behaviour to determine the suspicions level of each incoming transaction. The model was designed using Object-Oriented Analysis and Design Methodology (OOADM), Multi-Agent Methodology and Machine Learning Technique respectively. The model was programmed and implemented using PHP while the database was implemented with MySQL. Test results on the new system using confusion matrix shows a significant positive impact 94% accuracy in credit card fraud detection as against 57% of accuracy by the existing system, and hence a significant improvement on overall operating efficiency. Thus, the new credit card fraud (CCF) detection system using multi-agents is compatible with other detection software but has significantly higher performance efficiency (94%). The model is therefore recommended for use by banks, financial agencies and government agencies.

KEYWORDS: Multi-Agent, Bank Fraud, Machine Learning, Credit Card

INTRODUCTION

Frauds have plagued most financial institutions for a long time. Multi-agents and data mining principles have been used to solve series of real life problems like loan fraud, money laundering, cheque fraud and payment card fraud. With the growth of online business around Nigeria, the number of credit card frauds has also increased drastically. Unfortunately, enough efforts have not been made in the area of applying multi-agents in solving bank fraud problems, especially in area of credit card frauds. This necessitates the need for this study. Fraud is an increasing phenomenon as shown in many surveys carried out by leading international consulting companies [1]. 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 [2]. 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. [3] 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. [3] 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.

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 [4].

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.

[1]Dept. of Computer Science, Faculty of Science Imo State University, Owerri.
[2]Dept. of Computer Science, Federal University of Technology, Owerri.

HOW TO CITE THIS ARTICLE:
Amanze, B.C., Onukwugha, C.G (2018). an Enhanced Model for Bank Fraud Detection in Nigerian , International Educational Journal of Science and Engineering (IEJSE), Vol: 1, Issue: 5, 04-09

Research Paper

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 [5].

b. Loan Fraud: Fraudulent loan applications which are reason 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. Card can also be negotiated by merchant who undertakes duplicate transaction of card.

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

Causes of Bank Fraud

Causes of fraud can be categorized into two, viz : institutional factors and environmental factors [6].

1. **Institutional Factors:** The institutional factors are those that can be traced to internal environment of the organization [6]. 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 would 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, they become frustrated and such frustration could lead to fraud as such employee would attempt to compensate himself in any own way. Among the internal causes of fraud, the Nigerian Deposit Insurance Corporation [7], 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 banks 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 [6]. 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 to commit fraud even though he 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 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.

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 [8]. 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-agent 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 profile 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 [9].

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 [10]. 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 loses 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 issuer 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 [11].

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 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 issuer 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 [12]. 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. Atypical 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.

Multi Agent Concepts

A multi-agent system is a computerized system composed of multiple interacting intelligent agents within an environment. Multi-agent 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 intelligent agent 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.

LITERATURE REVIEW

[13] 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 [14]. 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 [15].

[13] 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 1.

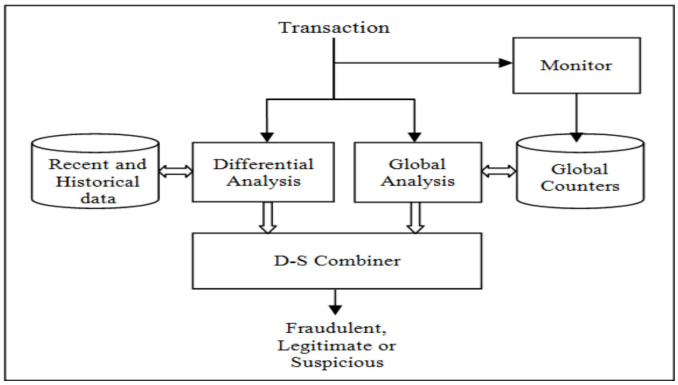

Figure 1: The General Architecture of Online Banking Fraud Detection [13]

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. [16] 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 increases and gets implemented to multi-platforms it makes it easier for a fraudster to commit financial fraud. In their research, the 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 use 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, [16] 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.

METHODOLOGY

This work was done using multi-agent methodology (MAM) to provide an effective means for systematic monitoring of credit card transactions in the banks so as to detect and report any abnormal financial transactions that may signify a high risk fraud. Data mining technique was used to extract and analyze non-trivial patterns from data sets on credit card frauds of various banks. Object-oriented analysis and design methodology (OOADM) was adopted for the analysis and development of the credit card fraud detection system. Confusion matrix was used to evaluate the performance of the system.

Data Flow of the Present System

In Fig. 2, the data flow diagram of the existing system is depicted. The credit card holder supplies username and password, and then the system validates the user identity before proceeding to credit card verification. If the verification are through, the transaction will be completed otherwise access will be denied.

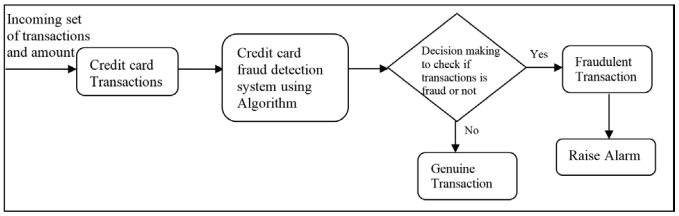

Figure 2: Data flow diagram of the Existing System

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.

Analysis of the New System

This paper 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- agent in data mining algorithm. Fig. 3 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-Agent 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-agent 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 focus 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.

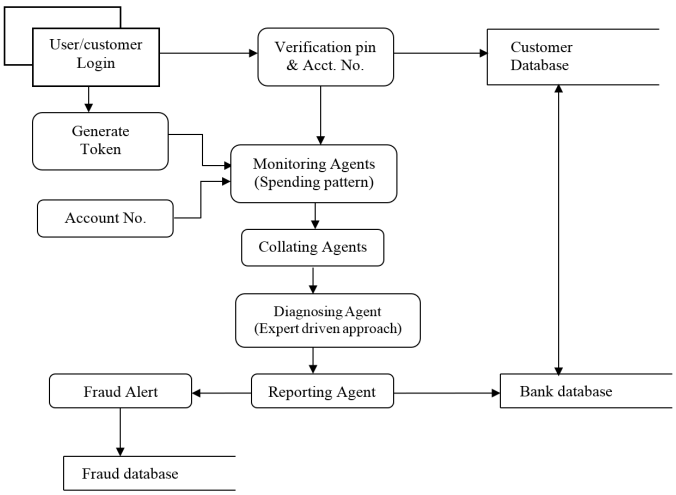

Figure 3: Data Flow Diagram of the New System

Enterprise Architecture of The New System.

The Enterprise Architecture of the New System is shown in Fig.4

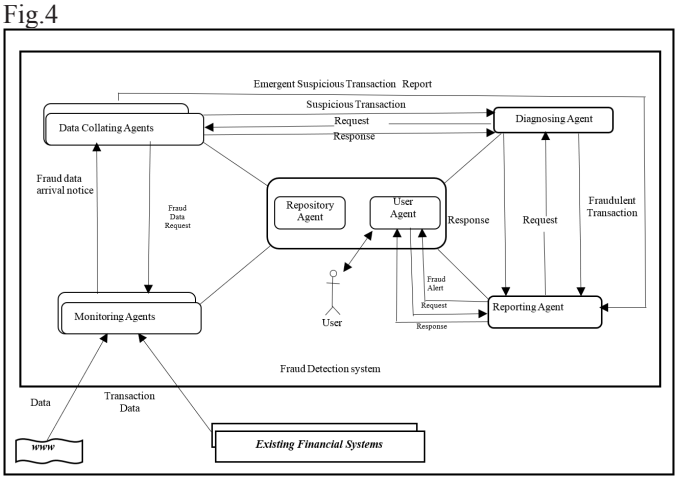

Figure 4: Enterprise Architecture (EA) of the New System

RESULTS AND DISCUSSIONS

An agent based information, that is, bank frauds prediction, and multi-agents data sets were produced; Presentation of the obtained data is in form of SMS notification on the fraudulent attempt were 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 frauds 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.

Summary

The paper developed a new approach of solving bank frauds problems especially in the area of bank fraud. A conceptual framework for a multi-agents system based on credit card fraud (CCF) process was developed. Various classes of multi-agents 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.

REFERENCES

1. NIBSS Annual Report and Statement of Account, 2018.
2. US Legal, (2016).
3. Egu, J. (2010). The Role of Information and communication Technology (ICT) in Fraud Detection in Nigeria Banks.
4. Siklos, & Pierre. (2001). Money, Banking, and Financial Institutions. Canada in the Global Environment. Toronto: McGraw-Hill Ryerson, 40.
5. 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.
6. Nwaze, C. (2008). Quality and Internal Control Challenges in Contemporary Nigeria Bank. Zenith Economic Quarterly, Zenith Bank Plc, 3(2), 21-32
7. Katerina, (2014). Mobile payment in Austria. Is mobile banking paving the way for mobile payments? International Conference on Mobile Web and Information Systems pg. 185-197.
8. Leung & Waisze, (2010).
9. Faweett, T., & Provost, F. (1997). Adaptive Fraud Detection, Data mining and knowledge Discovered. Kluwer Academic Publishers, Boston, Massachusetts, 1-28.
10. Khyrati, C., Jyoti, Y., & Bhawna M. (2012). A Review of Fraud Detection Techniques Credit-Card. International journal of Computer Applications, 45, (1), 39-44.
11. Pozzolo, A.D., Caelen, Y.A., Borgne, Li, Waterschoot S., & Bontempi, G. (2015). Learned lessons in credit card fraud detection from a practitioner perspective. Expert Systems with Applications, 41(10), 4915-4918
12. Rong-Chang Chen; Ming – Li Chiu, Ya-Li Huang & Lin-Ti Chen (2016). Detecting credit and fraud by using Questionnaire – Responded Transaction Model Based on support Vector Machines. Intelligent data Engineering and automated learning 5th International Conference Exeter, UK, August 25-27. 2016. Proceedings.
13. 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.
14. Bolton, R., & Hand, D. (2002). Unsupervised Profiling Methods for Fraud Detection. London.
15. 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.
16. Kovach, S., & Ruggiero, W. V. (2011): Online Banking Fraud Detection Based on Local and Global Behavior ICDS 2011: The Fifth International Conference on Digital Society.
17. Kappelin, F. & 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.