International Journal of Advanced Scientific Research | IJASR
International Journal of Scientific Research in Technology, Applied Sciences & Health Studies | IJSRTASHS
ISSN Print: 2579-1036 | ISSN Online: 2579-1044
Volume 3, Number 1, June, 2018

Credit Card Fraud Detection System in Nigeria Banks Using Adaptive Data Mining and Intelligent Agents: a Review

[1]Amanze, B. C., [2]Inyiama, H. C., & [3]Onyesolu, M. O.
[1]*Department of Computer Science, Faculty of Science, Imo State University, Owerri.*
[2&3] *Dept. of Computer Science, Nnamdi Azikwe University, Awka.*

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. Higher acceptability and convenience of credit card for purchases has not only given personal comfort to customers but also attracted a large number of attackers. As a result, credit card payment systems must be supported by efficient fraud detection capability for minimizing unwanted activities by fraudster's. Most of the well-known algorithms for fraud detection are based on supervised training. Every cardholder has a certain shopping behaviour, which establishes an activity profile for him. Existing fraud detection systems try to capture behavioural patterns as rules which are static. This becomes ineffective when cardholder develops new patterns. This paper aimed at developing credit card fraud detection system for banking industries in Nigeria using adaptive data mining and intelligent agents that could combines evidences from current as well as past behaviour and to determine the suspicious level of each incoming transaction. The statistics of fraud in Nigeria is discussed. In this paper, a system model for credit card fraud is discussed and designed.

Keywords*: Credit card, Nigeria banks, Data mining, Fraud detection system*

Corresponding Author: Amanze, B. C.

Background to the Study

Frauds have plagued telecommunication industries, financial institutions and other organizations for a long time (Jia & Jongwoo, 2005). The type of fraud addressed in this dissertation is called credit card transaction fraud. This fraud cost banks millions of dollars per year. As a result, fraud detection has become an important and urgent task 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 for predicting 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 activities or not.

A well-defined classification model is developed by recognizing the patterns of former fraudulent behaviors. Then the model can be used to predict any suspicious activities 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 drawback 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.

Intelligent agents are computer programs that can act on behalf of a person to do various jobs. Intelligent agents can automate a large portion of the fraud detection process and require little human intervention. Additionally, intelligent 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 intelligent agents than other computer programs for fraud detection. Besides, in a multi-agent system, many intelligent agents can work in parallel and cooperate with each other. This not only accelerates the detection process but also increases the detection accuracy. Moreover, intelligent 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.

Aims and Objectives of the Study

The aim of this paper is to model a credit card fraud detection system for banking industries in Nigerian using adaptive data mining and intelligent agents.

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 intelligent agents to authenticate the credit card transaction.

Scope of the Study

There are a number of financial institutions that grant facilities (credit card) to individuals and corporate bodies, this fact is clearly understood but 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 perform interference on the current data in order to make predictions. The intelligent agents 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 institution which is 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 is aimed at covering detection, monitoring and response of fraudulent activities in e-commerce business. It would also cover the area of real-time alerting system to enable financial companies stop or deactivate financial transaction suspected to be fraud.

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 an intelligent 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 trace the fraud, if they know 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.

Statistics of Fraud in Nigeria

Over the years, technology has played a vital role in the history of Nigeria's financial space. 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. Gone are the days of long queues in banks. 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 negate the acts of these fraudsters. It has been a tough battle but surely, was winning. 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, our collaboration, have contributed to reducing fraud menace in Nigeria's financial space. The Fig.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 with 2015, one also witnessed marginal reduction in attempted fraud value and actual loss is 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 1 shows the summary of fraud report, the fraud volume in 2016 recorded higher than 2015.

Table 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

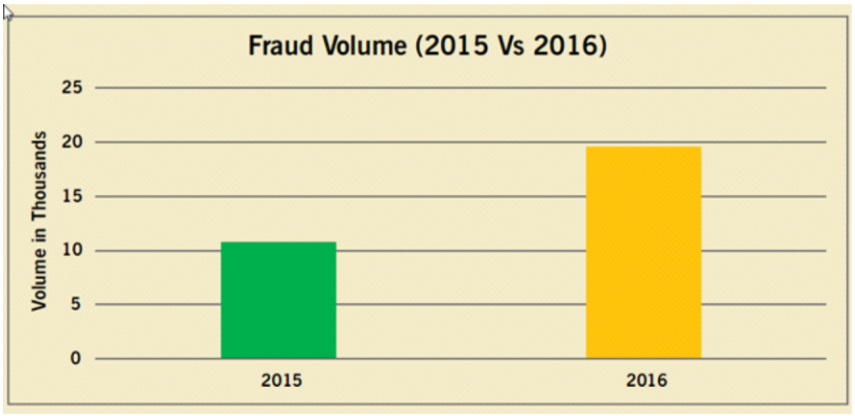


Fig. 1: Comparing Fraud Volume for the years 2015 and 2016 (Neff, 2016)

Fraud per Channels

Table 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: Fraud per Channels (Neff, 2016)

Channel	Fraud Volume	Actual Loss Value
Across Counter	325	511,072,861.29
ATM	9,522	464,514,684.27
Cheque	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 Industry to re-evaluate current strategies and policies. Same with 2015, "across counter" channel recorded the highest actual loss value for the year 2016with approximately N511 million. Although, it is less than what one witnessed 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 position respectively – same with 2015. Fig.2 depicts fraud according to channels in the year 2016, volume and value.

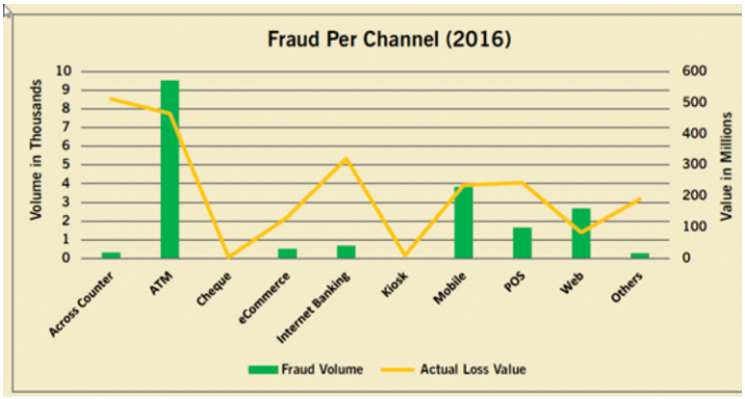


Fig. 2: Fraud according to channels in the year 2016: volume and value (Neff, 2016)

Fraud by Platform

Nigeria Inter Bank Settlement System (NIBSS) categorized various channels stated above into Electronic and Non- Electronic platforms. Tables 3 and 4 shows 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.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.

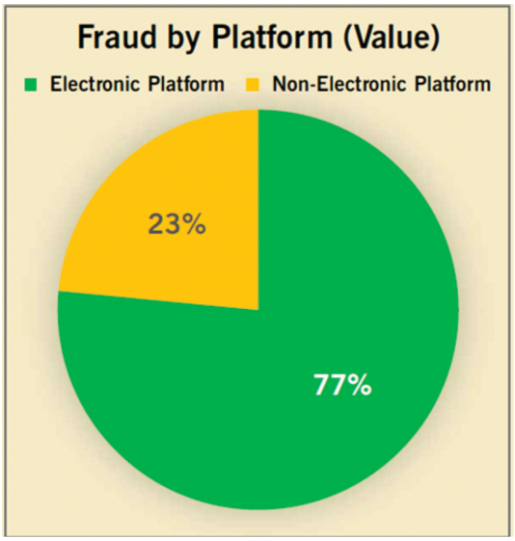


Fig.4: Fraud by Platform (Neff, 2016)

Table 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	19194	1,680,877,279.74

Table 4: Non-Electronic Channel (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

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 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. 5 shows the reported fraud per month both in fraud volume and actual loss value.

Table 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

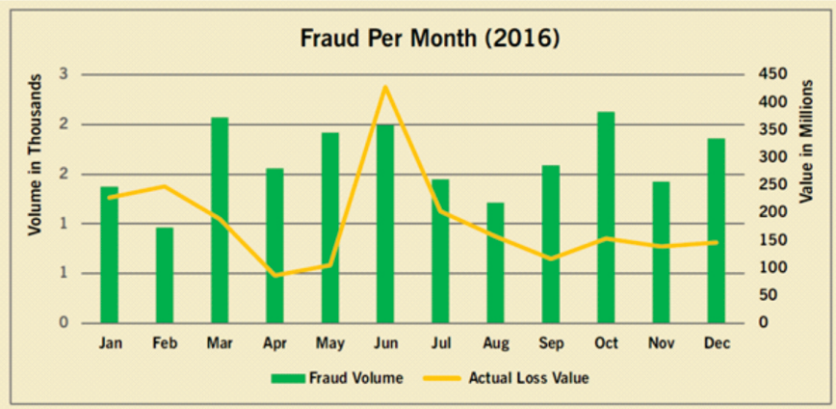


Fig. 5: Reported fraud per month (Neff, 2016)

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.6 shows the reported fraud per quarter and the attempted fraud value and actual loss value attached.

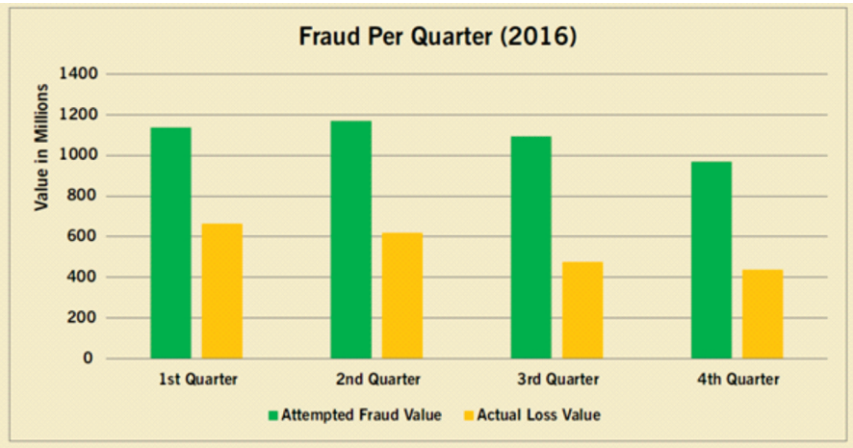
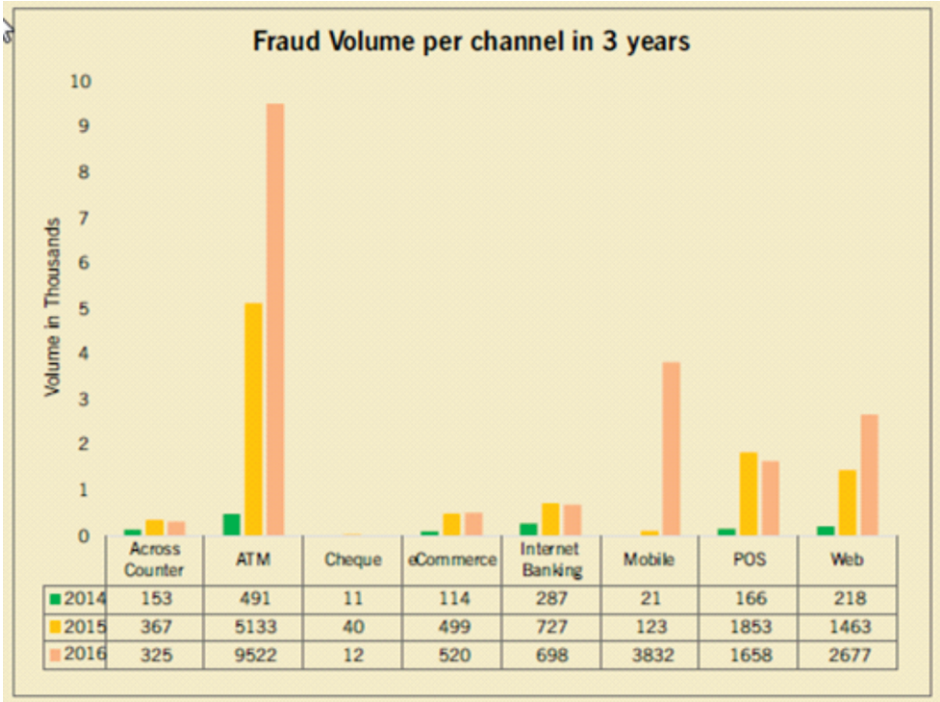


Fig. 6: Reported Fraud per Quarter (Neff, 2016).

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. 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.



	Across Counter	ATM	Cheque	eCommerce	Internet Banking	Mobile	POS	Web
2014	153	491	11	114	287	21	166	218
2015	367	5133	40	499	727	123	1853	1463
2016	325	9522	12	520	698	3832	1658	2677

Fig. 7: Fraud volume per channel in the last 3 years (Neff, 2016).

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 6 and 7 shows 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 to be 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. 8 shows trend in Nigeria over the last three years which recorded increased with over 80% in 2016.

Table 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 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%

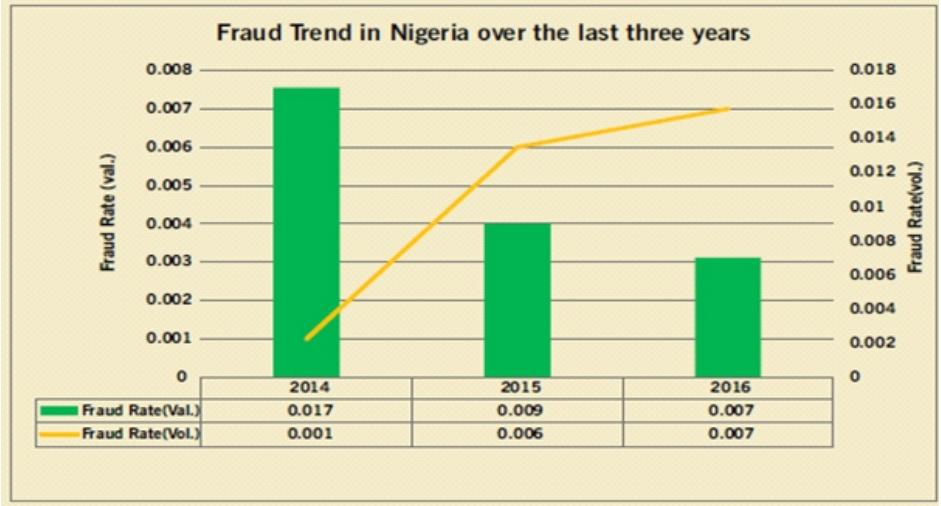


Fig. 8: Fraud Trend in Nigeria over the last three years. (Neff, 2016)

Literature Review

Nabha (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 registered cardholder. When used separately, both these algorithms suffered importation limitations, which include- difficulty in testing because real data is not available in the case of HMM and issues like

scalability and time constraints in case of communal detection. 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 being 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. It is hard to track user's behaviors. All types of users (good users, business, and fraudsters) change their behavior frequently. Finding new or charging patterns is an important as recognizing old patterns.

The main problem is that the existing fraud detection will give the false alarm that means transaction is fraudulent even if the transaction is genuine. Sahil *et al.* (2015) proposed a credit card fraud detection using advanced combination Heuristic and Bayes' Theorem. The authors propose the following steps: step one Luhn's test is used to validate card numbers. Then, two rules i.e. address mismatch and Degree of outlines 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. The overall belief is further weakened in the final step using Bayes' theorem, followed by recombination of the calculated probability with initial belief of fraud using advanced combination heuristic.

Another limitation is that, for evidences with a high degree of conflict, the modeling may not be accurate. Ekrem (2011) proposed a detecting credit card fraud by genetic algorithm and scatter search. In this paper, the author proposed a method to score each transaction and based on these scores the transaction can be classified as fraudulent and legitimate and also combined two well-known methods such as genetic algorithm (GA is a solution procedure that starts with a number of initial solutions which act as the parents of the current generation, then new solutions are generated from these solutions by the cross-over and mutation operator, less fit members of this generations are eliminated, then fitter members are selected as the parents for the next generation.

This procedure is repeated until a pre-specified number of generations have passed, and the best solution found until then is selected). Scatter search (SS) is another evolutionary algorithm which shares some common characteristics with the GA. It operates on a set of solutions, the reference set, by combining these solutions to create new ones, commonly termed as Meta heuristic algorithm to use in such problems where data mining technique does not fit well. The main problem is to detect fraudulent credit card transaction that can be classified with two types: counterfeit fraud which are carried out by organized criminal groups, the other type is illegal use of stolen or lost card and in order to solve

this problem, there is a need of robust solution which is not only based on the behavior of the fraudster but also the behavior of a customer and date mining technique is not directly usable to solve classification problem.

Methodology Adopted

The intelligent agent methodology, adaptive data mining methodology and object oriented analysis and design methodology (OOADM) was adopted in this paper:

i. Intelligent agent methodology will provide an effective means for systematic monitoring of credit card fraud transactions in the bank, to detect and report to manger any abnormal financial transactions that may signify a high risk, fraud, and other financial inconsistencies. Such monitoring tasks involve fraud detection, credit card monitoring, and position or the place the agent is monitoring. However, intelligent agents 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 intelligent agents, 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 methodology will help the bank to identify who uses credit card to commit fraud. 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 techniques, 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 system analysis and application design. 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.

Implications and Conclusion

Adaptive data mining and intelligent agents can play an important role in the credit card fraud detection domain. A conceptual framework for a multi-agent system based on Credit Card Fraud (CCF) process is developed, in which various classes of intelligent agents are proposed to provide a set of functionalities for CCF in electronic transaction environment for banks. 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. Intelligent agents will eventually be the ultimate means to fight against credit card frauds. However, there is still a long way to go before the wide adoption of intelligent agents for credit card fraud detection. The accuracy of fraud detection needs to be improved; the reliability of the agents needs to be ensured by testing the system on a real bank server to check its performance and acceptability.

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 –the design of intelligent agent credit card fraud (CCF) detection model using multi-agent; design of the CCF detection agent architecture and design of the CCF detection alert. An approach is used to develop the credit card fraud detection system that utilizes both adaptive data mining and intelligent agents' approaches to achieve a synergy that better handles the Nigeria credit card fraud situation using multi-agents 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 intelligent agent as a research tool and laid a solid groundwork for intelligent detection methodologies to be used in an operational fraud detection system.

References

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

Delamaire, L., Hussein, A., & John, P. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank Systems, 4*(2), 57-68.

Ekrem, D., & Mehmet, H. (2011). Detecting credit card fraud by genetic algorithms and scatter search. *Expert Systems with applications: An International Journal, 38*(10), 13057-13063.

Hand, D. J. (2010). Fraud detection in telecommunications and banking. *Technimetrics, 52*(1) 34-38.

Joshi, S., & Phoha, V. (2005). Investigating Hidden Markov Models Capabilities in Anomaly Detection. *Proc. 43rd ACM Ann. Southeast Regional Conference*, 1(5), 98-103.

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.

NeFF Pledges Sustained Fight Against e-fraud in 2016.

SahilHak, S., & Varun, P. (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

Singh, M., Perminderpal, S. & Rajan, K. (2014). Fraud detection by monitoring user behavior and activities. *International Conference on Computer and Intelligent Systems,* 6-14.