IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

On the Development of Credit Card Fraud Detection System using Multi-Agents

[1]Amanze B.C., [2]Inyiama H.C, [3]Onyesolu M.O

[1]Dept. of Computer Science, Faculty of Science Imo State University, Owerri
[2] Dept. of Computer Science, Nnamdi Azikwe University, Awka

*Corresponding Author: amanzebethran@yahoo.com

Available online at: www.ijcseonline.org

Accepted: 22/Jun/2018, Published: 30/Jun/2018

Abstract- The paper presents multi-agent techniques for fraud analysis. We present a mathematical model for credit card detection and compare different intelligent agents such as monitoring agents, collating agent, diagnosing agent and reporting agent. We tested agents as against cases of credit card fraud over time at different rates with which customer received fraud alerts, we discovered improvement in detecting a credit card fraud cases using multi-agents system. The credit card authentication techniques is weak and give room to unauthorised users to gain access to customers account and steal their money through online transactions. No single platform for credit card fraud detection + Intelligent Agents +Data Mining. The objective of this paper is 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. The model was therefore recommended for implementation in use by Banks, financial agencies and government agencies for the security and diagnosis of credit card fraud. This shows that the performance of credit card fraud (CCF) detection using multi-agents is in agreement with other detection software, but performs 94% better.

Key words: Multi-agents, credit card fraud, fraudulent transactions, data mining, confusion matrix & ROC curve.

INTRODUCTION

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 has 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 customer/consumers' confidence and ruins brand image. It is indeed the number one enemy of the business world. Merriam Webster dictionary, the term fraud is defined as "the crime of using dishonest methods to take something valuable from a person or a person who pretends to be what he or she is not in order to trick people. In recent times, surveys conducted by leading internal consulting firms indicates that fraud in the financial sector is increasing rapidly 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 [1].

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 [2]. Credit card frauds can be broadly classified into three categories, that is, 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 [2]. 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 make 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, mainly 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.

Development of this intelligent systems using web-based programming with PHP – MySQL and Java Script to implement the credit card fraud detection model which can authenticate credit card transactions using data mining and intelligent agents. Based on the test results, this intelligent agent of credit card can provide mangers with added value information, reduce the uncertainty of the decision outcome and thereby enhance banking service quality.

The purpose of the research is to develop intelligent agents software to detect credit card fraud status. The method used in detection of credit card fraud based is on current behavior as well as past behavior and to determine the suspicious level of each incoming transaction using intelligent agents methodology and data mining methodology. Decisions resulting from the system are demonstrate an alert notification to the key system (customer database and credit card) on any suspicious transactions on the credit process during runtime.

II. RELATED WORK

In [3] 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 3 new features based on the clustering result in order to keep the learning from the clustering results. The main problem is that the framework needs the historic to classify the customer in the commercial and residential class. [4] 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. The detection system performance was not evaluated. [5] 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 perform 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. It does not propose any approach to detect other fraudster behavior such as address mismatch, Internet Protocol (IP) address.

[6] 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. [7] 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. [8] 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. [9] 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.

III. DATA FLOW OF THE PRESENT SYSTEM

In Fig. 1, 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.

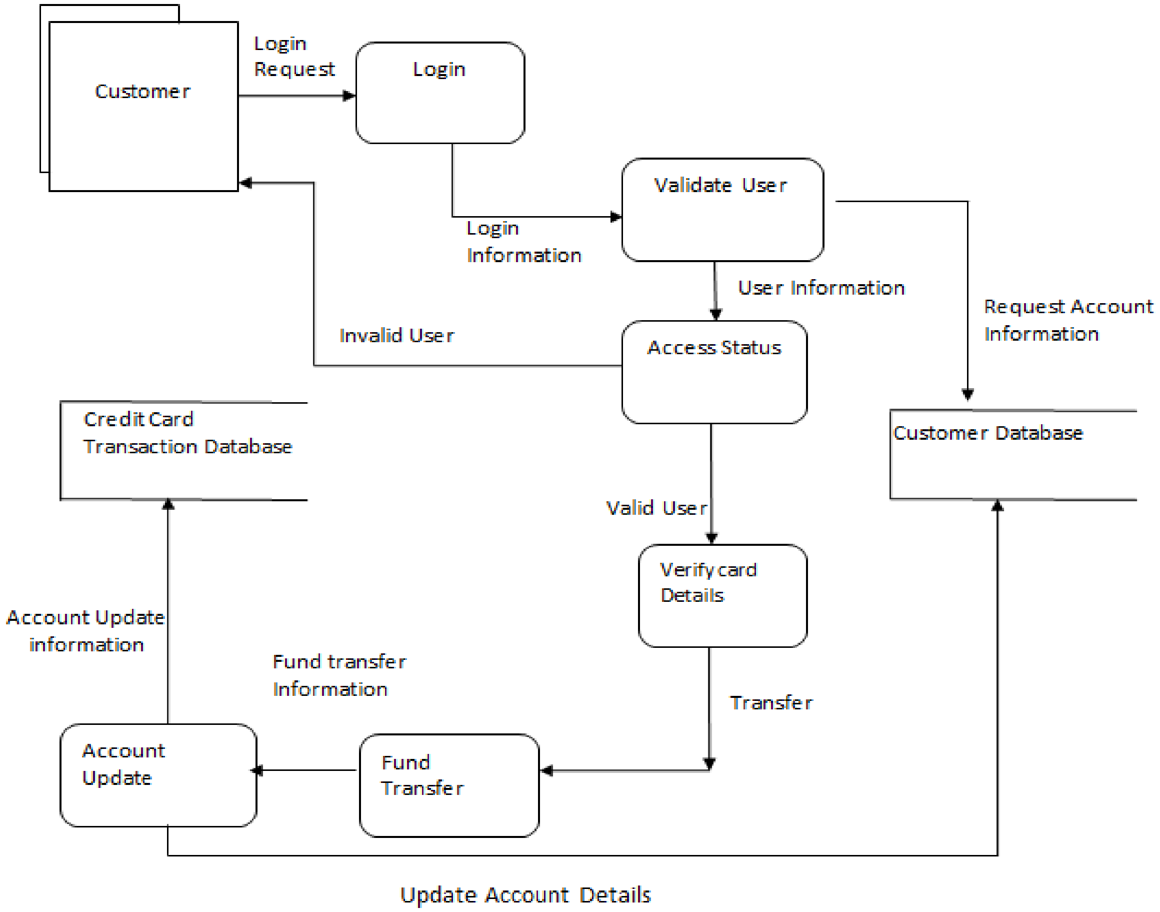

Fig. 1: Data Flow of the Present System Mathematical Model of the Existing System

Parameters and Symbols of the Existing System

Let us assume that one has a population of size N at time t, that is N (t), the customers that come for the services and
Let $\gamma =$ Rate at which people join the C class.
C = Customers (first point of call of the customers)
L = Login

$V_{s.}$ = Validate user

C_D = Customer Database

$V_C = \ Verify\ Card\ Details$

$F_T = Fund\ Transfer$

$A_u = \ Account\ UPdate$

$C_{CT} = Credit\ Card\ Transaction\ Database$

As = Access Status

$\alpha = \ Logic\ Request$

$\beta \ = \ Logic\ Information$

$\lambda \ = Request\ Account\ Information$

$b = Valid\ User$

$\emptyset = Transfer$

$\tau \ = \ Update\ Account\ Details$

$\bar{a} \ = Fund\ Transfer\ Information$

$\bar{b} \ = Invalid\ User$

$\xi = Account\ Update\ Information$

$\rho = User\ Informatiion$

$$\left.\begin{aligned}
\frac{dC}{dt} &= \gamma N + \bar{b}A_S - \alpha C \\
\frac{dL}{dt} &= \alpha C - \beta L \\
\frac{dV_s}{dt} &= \beta L - \lambda V_{s-} \quad {}_P V_s \\
\frac{dA_s}{dt} &= PV_s - bA_s - \bar{b}A_s \\
\frac{dV_c}{dt} &= bA_s - \emptyset V_c \\
\\
\frac{dC_D}{dt} &= \tau A_U + \lambda V_s \\
\frac{dF_T}{dt} &= \emptyset V_{c-\bar{a}F_T} \\
\frac{dA_U}{dt} &= \bar{a}F_T - \tau A_U - \xi A_U \\
\frac{dC_{CT}}{dt} &= \xi A_U
\end{aligned}\right\} \qquad (1)$$

$$N = C + L + V_S + A_S + V_C + C_D + F_T + A_U + C_{CT}$$

$$\therefore \frac{dN}{dt} = \frac{dC}{dt} + \frac{dL}{dt} + \frac{dV_S}{dt} + \frac{dA_S}{dt} + \frac{dV_C}{dt} + \frac{dC_D}{dt} + \frac{dF_T}{dt} + \frac{dA_U}{dt} + \frac{dC_{CT}}{dt} = \gamma N$$

$$\Longrightarrow \frac{dN}{dt} = \gamma N$$

Separating the variables we have

$$\Longrightarrow \frac{dN}{N} = \gamma dt$$

Integrating using the method of separation of variables we have

$$\int \frac{dN}{N} = \int \gamma dt \Longrightarrow \quad InN = \gamma t + c \quad \Longrightarrow \quad N = e^{\gamma t + c} = e^{\gamma t}e^{c}$$

$\therefore N(t) = N_0 e^{\gamma t}$ Where $N_0 = e^{c}$

IV. 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 intelligent agent in data mining algorithm. Fig. 2 shows the data flow diagram of the new system model. The system has three data mining engines: customer/bank database, credit card transaction database and fraud detection database. The customer/bank database has the following: opening of account operation, withdrawal and deposit transaction and credit card transaction. Fraud techniques database will give details of attack attempts on customer's credit card. The credit card database will contain all the previous credit card transactions carried out by the customer. The proposed Credit Card Fraud Intelligent Agent Model (CCFIAM) which is to detect the credit card fraud by analyze the spending patterns on every card and figure out any inconsistency with respect to the usual spending patterns. Intelligent 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 the most recent spending pattern of the transaction.

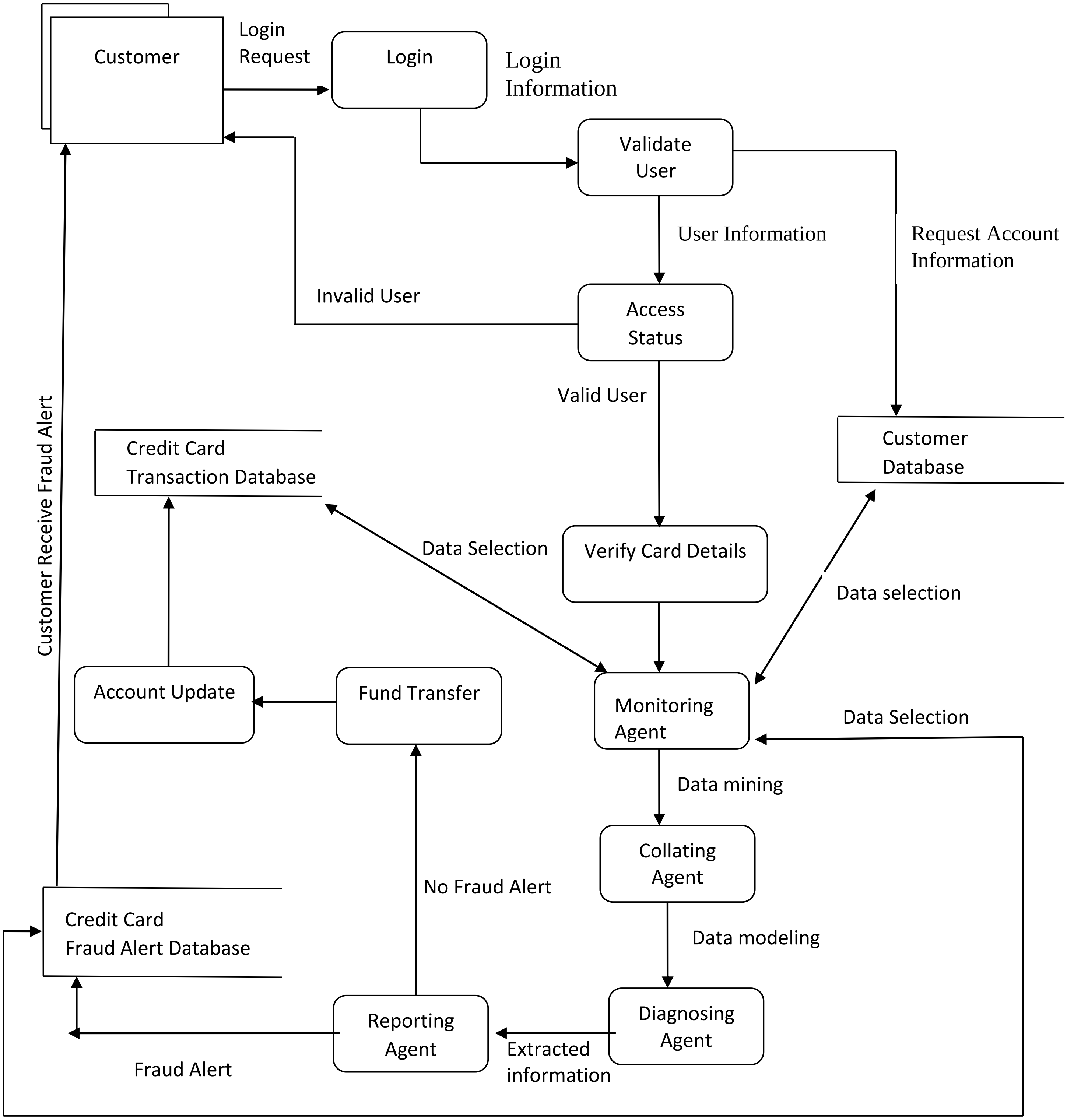

Fig. 2: Data Flow Diagram of the New System Model Mathematical Model of the New System

Parameters and Symbols of the New System

γ = Rate at which people join the C class

C = Customers (first point of call of the customers)

L = Login

V_U = Validate user

C_D = Customer Database

$V_C = \ Verify\ Card\ Details$

$F_T \ = FundTransfer$

$A_u \ = \ Account\ Update$

A_S = Access Status

C_{CF}= Credit Card Fraud Alert Database

$C_{CT} \ = \ Credit\ Card\ Transaction\ Database$

$M_A = Monitoring\ Agent$

$D_{CA} = Data\ Collating\ Agent$

$D_A \ = Diagnosing\ Agent$

$R_A \ = Reporting\ Agent$

$C_{CF} \ = \ Credit\ Card\ Fraud$

$\alpha \ = \ Logic\ Request$

$\beta \ = \ Logic\ Information$

$\lambda \ = Request\ Account\ Information$

$b = Valid\ User$

$\emptyset = Transfer$

$\tau \ = \ Update\ Account\ Details$

$\bar{a} \ = Fund\ Transfer\ Information$

$\bar{b} \ = Invalid\ User$

$\xi$$= Account\ Update\ Information$

$\rho = User\ Informatiion$

t_1 = $\ Data\ Mining$

t_2 = $\ Data\ Modeling$

t_3 = $\ Extracted\ Information$

t_4= $\ Fraud\ Alert$

$\varphi = No\ Fraud\ Aert$

$d_1 = Data\ selecting\ from\ CCT$

$d_2 = Data\ selecting\ from\ CD$

$d_3 = Dataselectingfrom\ CCF$

$\omega = Customer\ Received\ Fraud\ Alert$

g = Card Information

Using the above symbols and parameter one therefore write the model of the new system as follows:

$$\left.\begin{aligned}
\frac{dC}{dt} &= \gamma N + \omega C_{CF} + \bar{b}A_S - \alpha C \\
\frac{dL}{dt} &= \alpha C - \beta L \\
\frac{dV_U}{dt} &= \beta L - \lambda V_{U-} \quad {}_P V_U \\
\frac{dA_s}{dt} &= \quad {}_P V_U - bA_s - \bar{b}A_s \\
\frac{dV_c}{dt} &= bA_s - gV_c \\
\frac{dC_D}{dt} &= \lambda V_U + d_1 M_A - d_1 C_D \\
\frac{dM_A}{dt} &= gV_C + d_1 C_D + d_2 C_{CT} + d_3 C_{CF} - t_1 M_A - d_1 M_A - d_2 M_A - d_3 M_A \\
\frac{dD_{CA}}{dt} &= t_1 M_A - t_2 D_{CA} \\
\frac{dD_A}{dt} &= t_2 D_{CA} - t_3 D_A \\
\frac{dR_A}{dt} &= t_3 D_A - t_4 R_A - \varphi R_A \\
\frac{dC_{CF}}{dt} &= t_4 R_A + d_3 M_A - \omega C_{CF} - d_3 C_{CF} \\
\frac{dF_T}{dt} &= \varphi R_A - \bar{a}F_T \\
\frac{dA_U}{dt} &= \bar{a}F_T - \xi A_U \\
\frac{dC_{CT}}{dt} &= \xi A_U + d_3 M_A - d_2 C_{CT}
\end{aligned}\right\} \qquad (2)$$

$$N = C + L + V_U + A_s + V_C + C_D + D_{CA} + M_A + R_A + D_A + C_{CF} + F_T + A_U + C_{CT}$$

$$\therefore \frac{dN}{dt} = \frac{dC}{dt} + \frac{dL}{dt} + \frac{dV_U}{dt} + \frac{dA_S}{dt} + \frac{dV_C}{dt} + \frac{dC_D}{dt} + \frac{dD_{CA}}{dt} + \frac{dM_A}{dt} + \frac{dR_A}{dt} + \frac{dD_A}{dt} + \frac{dC_{CF}}{dt} + \frac{dF_T}{dt} + \frac{dA_U}{dt} + \frac{dC_{CT}}{dt} = \gamma N$$

$$\Longrightarrow \frac{dN}{dt} = \gamma N$$

Separating the variables we have

$$\Longrightarrow \frac{dN}{N} = \gamma dt$$

Integrating using the method of separation of variables we have

$$\int \frac{dN}{N} = \int \gamma dt \Longrightarrow InN = \gamma t + c \Longrightarrow N = e^{\gamma t + c} = e^{\gamma t} e^{c}$$

$\therefore N(t) = N_0 e^{\gamma t}$ Where $N_0 = e^{c}$

V. MODEL PERFORMANCE

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 intelligent agent 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 intelligent 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 1, contains information about actual and predicted classifications. Performance is evaluated using the data in the matrix. Table 2 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%.

Table 1: Confusion matrix of a model applied to test dataset (Pin) Observed

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

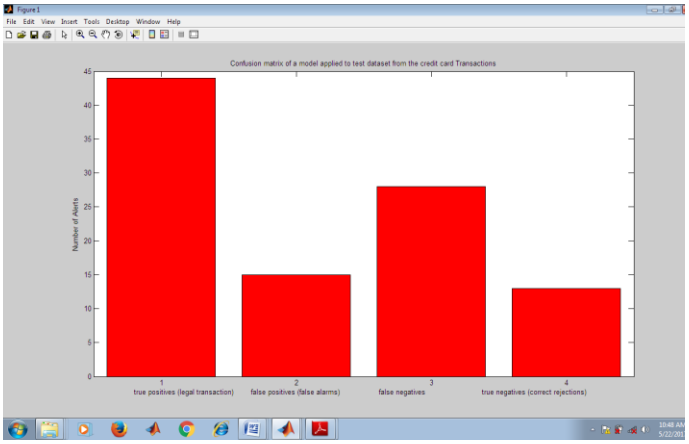

Fig. 3: Confusion matrix of a model applied to test dataset from the credit card Transactions using pin as the only security mechanism

Figure 3 shows the alerts on 100 transactions carried out using credit card. The graph shows that 44 transactions are legal and was predicted correctly. 15 transactions are detected to be fraudulent while it is not 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 3, which show the accuracy of the credit card fraud detection system.

$$AC = \frac{a+d}{a+b+c+d} \quad (3)$$

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 2: Confusion matrix of a model applied to test dataset Observed

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

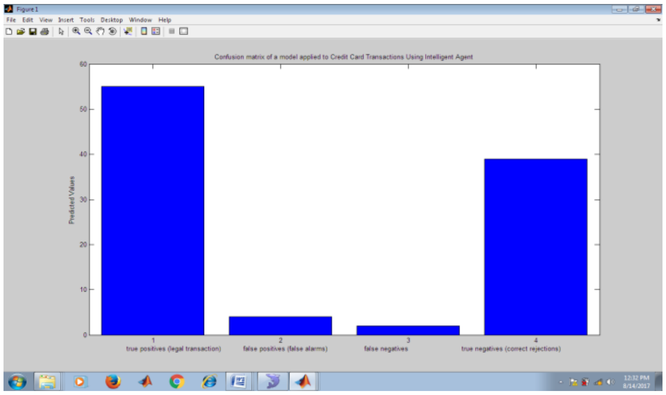

Fig. 4: Confusion matrix of a model applied to test dataset from the credit card Transactions using intelligent agent as the only security mechanism

Figure 4 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, which show the accuracy of the credit card fraud detection system.

$$AC = \frac{a+d}{a+b+c+d} \quad (5)$$

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

VI. RESULTS AND DISCUSSIONS

In this paper, the credit card fraud detection system using intelligent agents and data mining consists of two units namely, the withdrawal and deposit unit. Each of the two units is in turn made up of the following subunits: database interface and intelligent agents. The database interface subunit is test to ensure that the necessary transaction data is import and use. The intelligent agents is done using a multi-agents (machine Learning) where the available data set is randomly partition into a training set and a test set, and the training set will be further partition into subsets: use for elimination of the model (i.e., training the algorithm) and a subset use for evaluation of the performance of the model (i.e., validation). If any of the above test fails, the subunit will be redesigned or the program statements rewritten, followed by a retesting, until all the subunits pass the test. Test data is design and run on the system with the test program. The result of the process is compared with a manually prepared result to determine the efficiency and effectiveness of the new system. The test data for two credit card banking transaction under study, which is withdrawal and deposit, will be used. The software programs were experimented module by module to give an expected result. The Agent Based system for Real time fraud detection is 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. 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 diagnosing agent reports. Credit card fraud detection is based on intelligent agents and adaptive data mining model which is machine learning algorithm, hence not 100% correct. It has detected those transactions as fraud where user belongs to low category and high category payment is made or vice versa. The mechanisms require at least 10 transactions to determine accurately the transaction as fraud or not. The credit card fraud detection system developed in this dissertation provides features for performing some core banking functions like account opening, cash deposit/withdrawal, account balance checking and printing account statement online. But the major achievement in the design is the integration of a highly secured credit card transaction using the adaptive data mining and intelligent agent as the credit card fraud detection technique. The interface is user friendly, secured and improved accuracy in fraud detection. The accessibility of the modules in the system is controlled using three levels of access (staff, admin and credit card holders). Each user has a limited access and cannot go beyond the assigned access to the system. The challenges of credit card fraud detection system using adaptive data mining and intelligent agent 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 intelligent agent while trying to detect credit card fraud. Also, some time the system can generate false alert thereby denying the credit card user the privilege of transaction at that particular moment.

VII. GRAPHS OF THE RESULTS

Figures 5a and 5b showed the cases of credit card fraud over time at different rates with which customer received fraud alerts. For the first scenario when the simulation is run for a period of ten years, it is observed that the credit card fraud increases with decreasing fraud alerts. Almost the same trend is observed when the simulation is run for a period of thirty years. However, over this longer period, it is seen that the cases of credit card fraud rises to an uncontrollable level. This is because the fraud alert is now very small (about 10%), with customers becoming more unaware of impending card frauds. Figure 6 shows the graph of credit card fraud with varying number of monitoring agents. In this scenario, the higher the number of monitoring agents, the lower the cases of credit card fraud.

However, the collating agents have marginal impact on credit card fraud cases, as shown in Figure 7. The higher the collating agents, the lower the credit card fraud cases. Again, the graph of credit card fraud cases, varying the number of diagnosing agents (DA), over time is depicted in Figure 8. From this graph, one notice that as the number of diagnosing agents (DA) increases, there is a drop in the cases of credit card fraud.

Finally the graph of credit card fraud cases varying number of reporting agents, as shown in Figure 9, reveals that credit card fraud cases reduce with increasing number of reporting agents. The more the number of reporting agents, the lower the cases of credit card fraud.

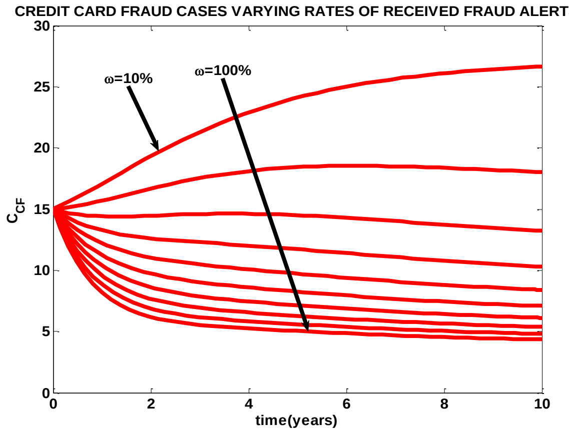

Figure 5a: Cases of Credit Card Fraud over Time at Different Rates with which Customer Received Fraud Alerts

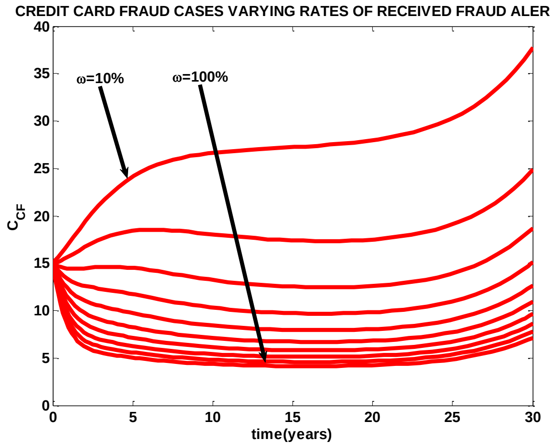

Figure 5b: Cases of Credit Card Fraud over Time at Different Rates with which Customer Received Fraud Alerts

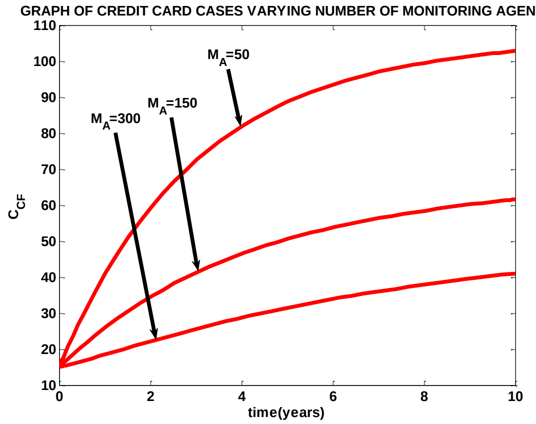

Figure 6: Graph of Credit Card Fraud with Varying Number of Monitoring Agents

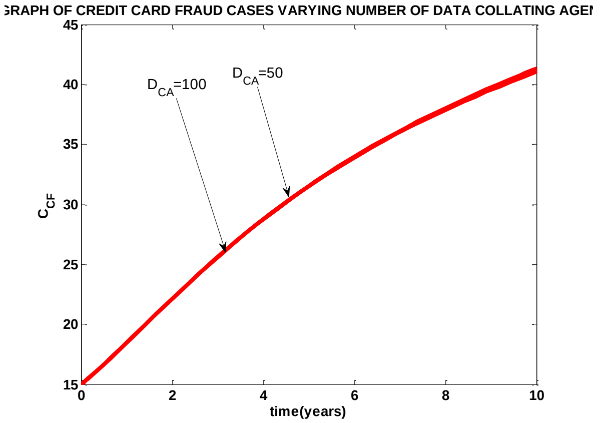

Figure 7: Data Collating Agents with Marginal Impact on Credit Card Fraud Cases

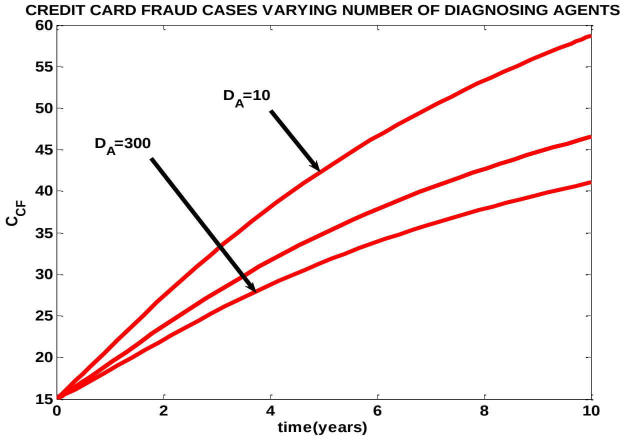

Figure 8: Graph of Credit Card Fraud Cases, Varying with Number of Diagnosing Agents (DA)

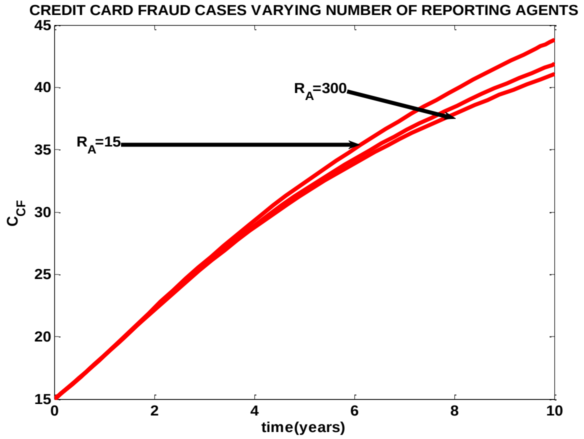

Figure 9: Credit Card Fraud Cases Reduction with Increasing Number of Reporting Agents

VIII. CONCLUSION

Conclusion of Research shows that the software of detecting credit card fraud with intelligent agents method proved able to be used as model of detecting Credit Card Fraud (CCF). This is indicated by an average of 94%.

IX. REFERENCES

[1] Lee, W., Stolfo, S., & Mok, K. (2011). Adaptive Intrusion Detection: a Data mining Approach, *Kulwer Academic Publishers*.

[2] Singh Mandeep, Perminderpal Singh & Rajan Kumar (2014). Fraud detection by monitoring user behavior and activities. *International Conference on Computer and Intelligent Systems, 6-14.*

[3] Farvaresh, H., & Sepehri, M.M (2010). A Data Mining Framework for deleting Subscription Fraud in Telecommunication. Science Direct, Engineering Applications of Artificial intelligence. (24), 182-194.

[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.

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

[6] 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.*

[7] 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.*

[8] 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*

[9] Ekrem, D., & Mehmet Hamdi Ozcelik (2011). Detecting Credit Card fraud by genetic algorithms and scatter search. *Expert Systems with applications: An International Journal, 38(10), 13057-13063.*