International Journal of Trend in Research and Development, Volume 5(3), ISSN: 2394-9333
www.ijtrd.com

Credit Card Fraud Detection System Using Intelligent Agents and Enhanced Security Features

[1]Amanze, B.C., [2]Asogwa, D.C. & Chukwuneke, C.I,
[1]Dept. of Computer Science, Faculty of Science, Imo State University, Owerri, Nigeria
[2]Dept. of Computer Science, Faculty of Science, Nnamdi Azikwe University, Awka, Nigeria

***Abstract*--** Credit card fraud can be detected using intelligent agents during transactions. Intelligent Agents aids to obtain a high fraud transaction coverage combined with low false alarm rate, thus providing a better and convenient way to detect frauds. Using intelligent agent, customers' pattern is analyzed and any deviation from the regular pattern is considered to be a fraudulent transaction. In this paper, the intelligent agent is used to detect the fraud when transaction is in progress. The existing fraud detection techniques are not capable to detect fraud at the time when transaction is in progress. As the usage of credit card has increased the credit card fraud has also increased dramatically. The system will send a token to the customer for more security checks and ask a secret question to the customer, if answer correctly, the customer will proceed for the transaction. If fail, the transaction is a fraudulent transaction and SMS message will send to customer and bank database.

***Keywords*--** *Intelligent Agent Authentication, fraud transaction, credit card, and fraud detection*

I. 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 (Lee *et al.*,2005).

One such aspect of banking where there is high rate of abuse of office and some level of collaboration in perpetrating fraud is in the case of credit card. Timely information on fraudulent activities is strategic to the banking industry. Banks have many and huge databases. Valuable business information can be extracted from these data stores. Credit card fraud detection is the process of classifying those transactions into two classes of legitimate (genuine) and fraudulent transactions (Singh *et al.*, 2014). Credit card frauds can be broadly classified into three categories, 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 (Singh *et al.*, 2014). In everyday life credit cards are used for purchasing goods and services using online transaction or physical card for offline transaction.

In credit or debit card based purchase, the cardholder presents card to a merchant for making payment. To 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.

Credit card frauds are increasing day by day as the use of credit card is increasing (Patel, 2014). Occurrence of credit card fraud has increased dramatically both online and offline. Credit card based purchase can be done in two ways: (i) physical card (ii) virtual card. In physical card purchase, the cardholder presents his card physically to the merchant for making payment. For this type of fraud the attacker has to steal the credit card. In virtual card purchase only the information about the card is stolen or gathered like card number, secure code etc. such purchases are done over the Internet. For this type of fraud the attacker needs only the card details so the only way to detect this type of fraud is to analyze the spending pattern of the card holder. When ones credit card or credit card information is stolen and used to make unauthorized purchases on e-commerce systems on the Internet, one becomes a victim of internet credit card fraud or no card present fraud. This is nothing new and there is nothing unusual about this because identity theft and credit-card fraud are present-day happenings affecting many people and involving substantial monetary losses. Fraud is a million dollar business and it's increasing every year. The PwC global economic crime survey of 2011 suggests that 34% of companies worldwide have reported being victim of fraud in the past year and increasing from 30% as reported in the year 2009. However, in recent years, the

development of new technologies like the Internet has provided further ways in which fraudsters can commit fraud. Fraud is a very skilled crime; therefore a special method of intelligent data analysis to detect and prevent it is necessary. These methods exist in the areas of Knowledge Discovery in Databases, Data Mining, Machine Learning and Statistics. They offer applicable and successful solutions in different areas of fraud crime.

Credit Card Fraud Detection System using Intelligent Agents

Intelligent agent 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.

Literature Review

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

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

Another implementation of ANNs is suggested by Patidar *et al.* (2011). They use the genetic algorithm in order to derive the optimal parameters of ANN. Like many other data mining techniques, ANNs make use of a number of parameters which need to be specified by software developers. Although the values of theses parameters can seriously affect the predicting accuracy of ANN models; a standard practice for specifying these parameters has never been established. The use of genetic algorithm which is suggested by Patidar *et al.* (2011) can help in deciding these optimal parameters. They call their approach as "Genetic Algorithm Neural Network (GANN)" Chen *et al.* (2006) suggest an implementation of SVM which they call "Binary Support Vector System (BSVS)". The approach of Chen *et al.* (2006) is insensitive to skewed distribution of training samples.

An innovative implementation of SVMs for detecting credit card fraud is also suggested by Chen *et al.* (2004) They suggest from the issuing banks to ask their new customers to fill some questionnaires that can help them understand the spending habits of the customers .This is particularly useful since there is no any prior history on the spending behavior of new customers and therefore the detection techniques cannot spot fraudulent transactions at the initial stage. Therefore the answers to the questionnaires can be used in a similar manner to the historical information of each customer. They call their approach as "Questionnaire-Responded Transaction Model" (QRT Model). One of the main problems of data mining techniques arises in situations where the training samples have an imbalanced distribution — also known as skewed distribution. In such a case the misclassification rate is increased whereas the predicting accuracy of the classifier is reduced. Sahin *et al.* (2011) provide three different implementations of decision trees for detecting credit card fraud. These implementations are called C5.0, C&RT and CHAID. Their differences lie in the way in which they construct the tree as well as the pruning algorithm which they use to remove erroneous branches and nodes. According to the experiments made by Sahin *et al.* (2011), the best predicting accuracy was achieved by C5.0 with an average of 92.80%, following by CHAID with 92:22% and finally by C&RT with 91.34%. In their experiments, the three DT implementations outperformed the SVM implementation which achieved an average accuracy of 88.38%.

YU *et al.* (2009) suggest an implementation of outlier detection technique. The similarity metric that they use to detect outliers is called distance sum. This is mathematically explained.

Yamanishi *et al.* (2004) suggest another implementation of outlier detection for detecting credit card fraud. They call their approach as "Smart Sifter" and claim that it can be applied in real time. This means that a new transaction is checked as soon as it arrives before being authorized. This is not the case for most fraud detection systems because real time detection is time consuming. Most of them will check the newly authorized transactions at some time in the future — for example once a day — in batch processing mode. The main disadvantage of this approach is that a fraud is just detected but not prevented. If, for instance, a fraud was committed in a physical shop then the fraudster would take the products and run away before the bank discover this fraud. Therefore somebody — either the legitimate cardholder or merchant or bank — would need to pay the losses of this fraud. Brabazon *et al.* (2010) propose an implementation of AIS for detecting credit card fraud which is committed online only. Although their approach can identify 90% of legitimate transactions; 96% of fraudulent transactions are classified as legitimate and therefore their approach is at least unrealistic

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

Algorithm Used

Given:

Accts: set of all accounts

Rules: set of all fraud rules generated from Accts

Input Phase: user inputs the credit card transaction details

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

Transaction Agent captures the Account Number being posted

Transaction Agent passes the number to intelligent agents

Intelligent agents check on rule set against the Account number received

Training Phase: Cluster creation

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

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

STEP 3: To construct the training sequence for training model

1. /*Initialization*/

2. S = { };

3. for (a ∈ Accts) do Cover[a] = 0;

4. for (r ∈ Rules) do

5. Occur[r] = 0; /*Number of accounts in which r occurs*/

6. AcctsGen[r] = { }; /*Set of accounts generating r */

7. end for

8. Check the previous spending profile

9. for (a ∈ Accts) do

10. Ra = set of rules generated from a;

11. for (r ∈ Ra) do

12. Occur[r] : = Occur[r] + 1;

13. add a to AcctsGen[r];

14. end for; end for

15. if transaction is outside spending profile the send alert to monitoring agent

16. for (a ∈ Accts) do

17. Ra = secret questions;

18. request for user to supply secret question and answer

19. while (cover[a] <Trules) do

20. r := correct from Ra

21. Remove r from Ra

22. if (r ∉ S and Occur[r] ≥ Taccts) then

23. add r to S;

24. for (a2 ∈AcctsGen[r]) do

25. Cover[a2] = Cover[a2] + 1;

26. end for; end if

27. end while; end for

Intelligent agents report back to Transaction agent if any rule is broken

Transaction agent stores the alert received

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

Detection Phase: Fraud detection

STEP 1: To Generate the observation symbol

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

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

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

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

Additional Security Features

Along with using the machine learning algorithm for detection of frauds one has implemented additional features like a token will send to customer for more authentication and secret question is also verified and checked for additional security.

In token detection, the information related to the token of the area in which the user is currently residing during making the transaction is stored in the database. This provides the database with the authentic user of the system and stores it. The information is cross checked every time the user makes a purchase online using the credit card and if any anomaly is detected then fraud detection system gets activated and necessary steps are taken to ensure the user is legitimate. See Fig 3 and Fig 4.

Analysis of the New System

This dissertation focused on credit card application which is used to detect the fraudulent credit card activities on credit transaction. In this peculiar type, the pattern of current fraudulent usage of the credit card has been analyzed with the previous transactions, by using the intelligent agent in data mining algorithm. Fig. 1 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.

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 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 also use data mining 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, they agents runs 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 send 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 the fund transferred will be deducted from the customer's account balance.

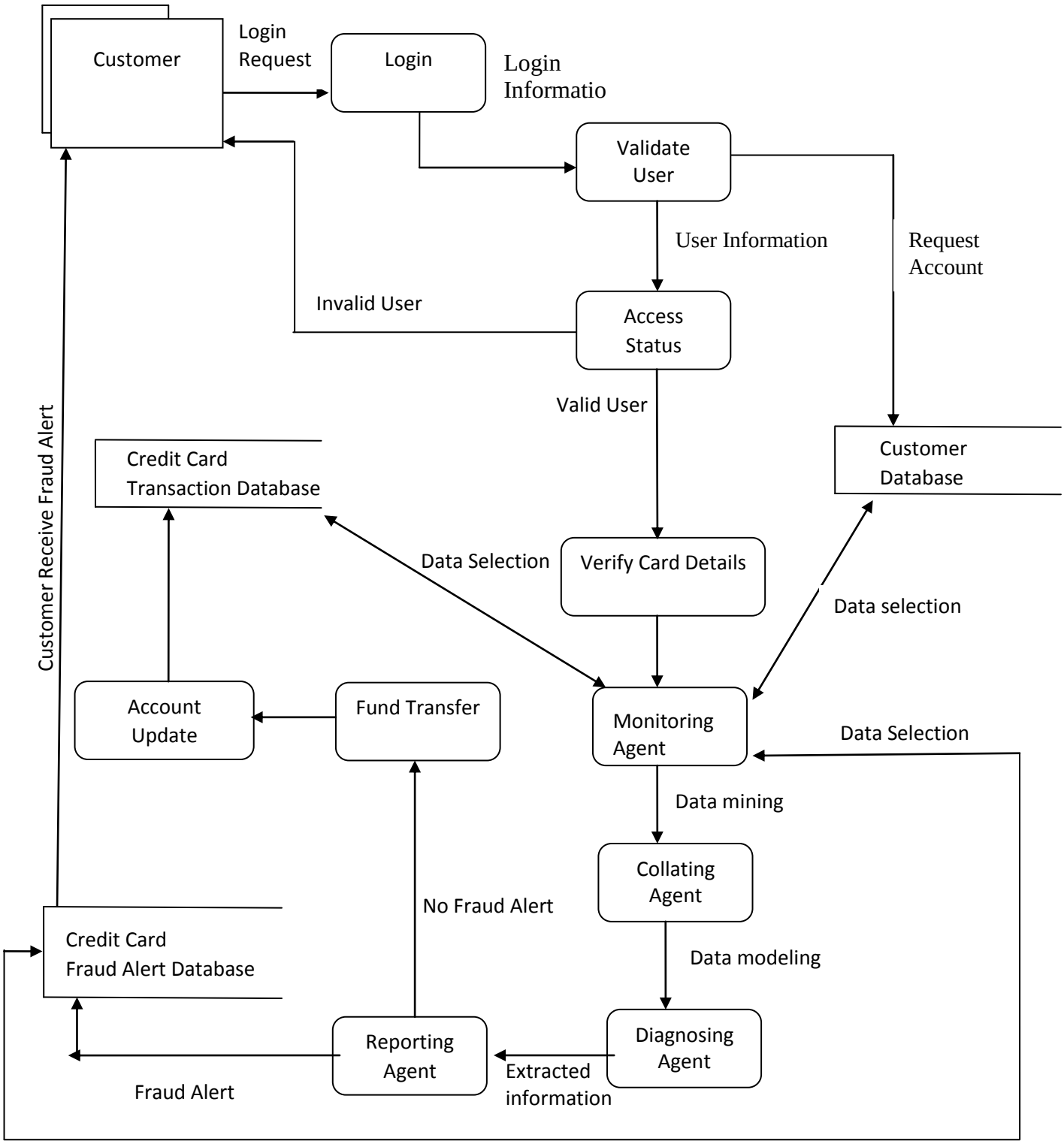

Figure 1: Data Flow Diagram of the New System Model

Advantages of the New System

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

1. The adaptive data mining and intelligent agent's model will introduce a more secured communication channels for credit card transactions thereby preventing loss of money by the customers to credit card fraudsters.

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

Justification of the New System

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

1. The model will maintain the database in which users transaction behaviors and spending patterns are saved.
2. Simple and easy to extract fraudulent activities since fraudsters will not check the transactions of the original card holder.
3. The model will produce a better true positive since it will be the combination of recent credit card fraud techniques and user account transaction database to form an agent.
4. The model raises alarms if unusual transaction is observed at agent stage.
5. The security will be maintained and transaction secured from fraud.
6. The speed of fraud detection is high to compared with existing model (HMM, ANN etc.).Once fraud detection is enhanced in the financial institutions, people's confidence in online transactions will increase and thereby reduce the stress of using fiscal cash for every transaction. This justifies the need for the new system.

High-Level Model of the New System

Fig. 2 shows the high level model of the new system. It shows that we have two active players in the system; the bank staff and the credit card user. Their actions on the system are separated as show in the model.

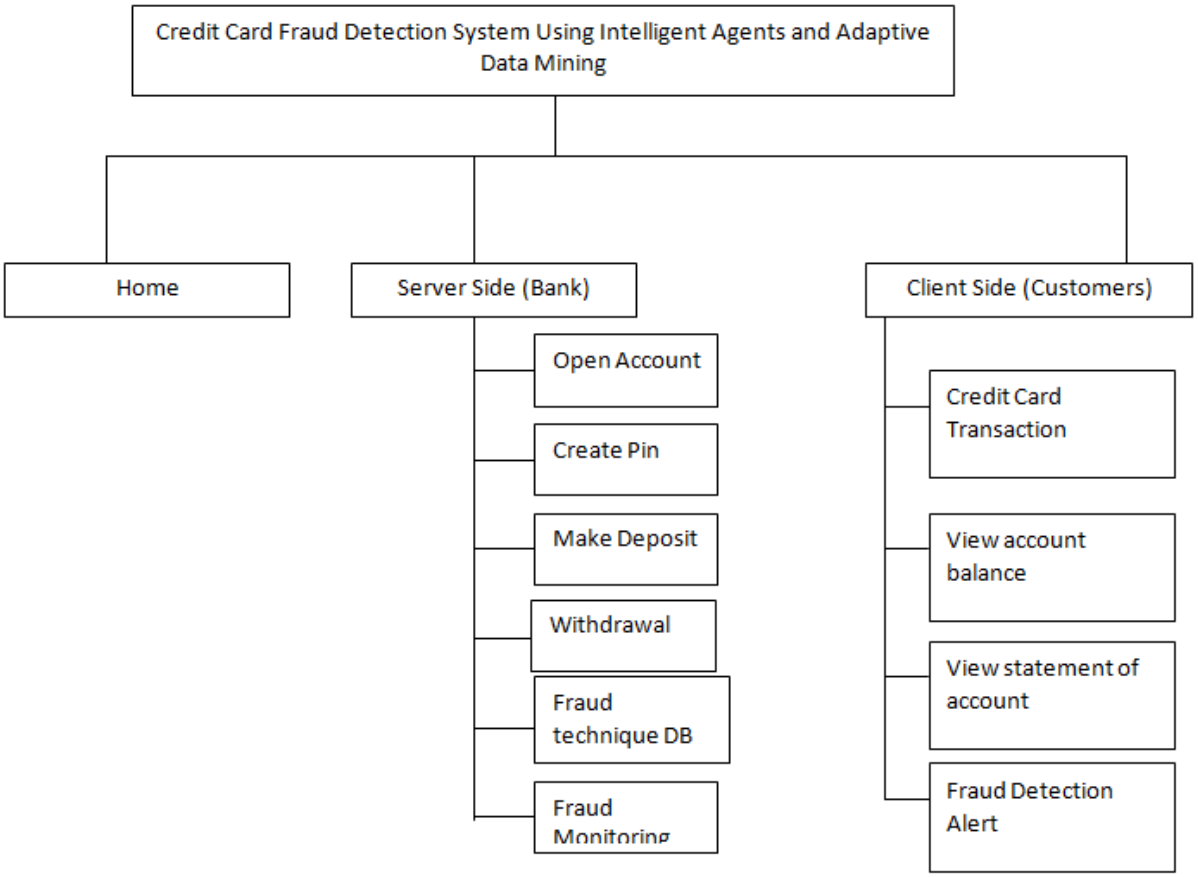

Figure 2: High Level Model of the New System

Application of the design

a. To provide easy and well security to online transactions

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

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

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

Table 1: Expected Result vs Actual Result

Module	Expected Test Result	Actual Test Result
Home Page	Expected to see the page containing links to other modules	The home page displayed platform and contains all the links to the various modules in the credit card fraud detection system
Log In Form	Expected to see the Log In form so that users can log in.	When clicked on log in, a form appeared where you can enter your username and password for admin or account number and account pin for customers.
New Account opening form	When clicked on the system, it is expected to display the form for entering new account opening details	When clicked on the button, the system displays the customer account opening form.
Deposit/withdrawal form	It is expected to allow users to deposit or withdraw money	The form allowed the user to enter the account no, transaction amount, date, and post it to the customer's account
Credit card transaction form	It is expected to allow customer transfer money to another account	The customer was able to transfer money from his/her account to another account
Data Collating agent form	It is expected to use data mining to extract users previous transactions and sent it to diagnosing agent	The data collating agent form was able to use data mining technique to extract the data set for the users credit card and forward it to diagnosing agent
Account Statement	In this module, it is expected to be used to view customers account statement	When you go to this module, the customers statement was displayed
Diagnosing agent form	It is expected to use determine the users spending profile and compare it with the current transaction	The diagnosing agent form was able to determine users spending profile and forward it to reporting agent
Monitoring agent form	It is expected to monitor the transaction and detect fraud where it exist	The monitoring agent was able to use the users spending profile and compare it with the current transaction to determine if it is fraudulent and report to collating agent
Reporting agent form	Expected to generate fraud alert where fraud is suspected	The reporting agent was able to forward an alert to the bank database indicating that the transaction is fraudulent and the account will be blocked

CONCLUSION

It has been discussed in this paper, that how intelligent agents will enable to end false online transaction through credit card. The Fraud Detection System is also accessible for controlling vast volumes of transactions handling. The intelligent agents credit card fraud detection system is not taking much time and in spite of having difficult process to achieve fraud check like the present system and it gives better and fast result. The intelligent agents makes the handling of detection very easy and tries to eliminate the complexity.

We recommended system which is an application of intelligent agents in Anomaly or fraud detection. The diverse steps in credit card transaction handling are represented as the essential method of an intelligent agents. The system implemented takes all the user information and deals with the data carefully to detect online frauds. It has also been described how they can detect whether an inbound transaction is fraudulent or not. Additional security features like token detection and also secret question verification are provided for enhanced security and better detection of fraud transaction. This proposed method can be made more advanced and better version can be developed and enhanced in the future.

Figure 3: Customer Account number and token verification Form

Figure 4: Customer secret question Form

References

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

[2] Sing, 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.

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

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

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

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

[7] Sahin, Y., & Duman, E. (2011). Detecting Credit card fraud by decision trees and support vector machines. Proceedings of the International Multi conference of Engineers and Computer Scientist, (1) 1-6.

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

[9] Yamanishi, K., & Takeuchi, J.I. (2004). Online unsupervised Outlier Detection using finite mixtures with Discounting Algorithms. Data mining and knowledge discovering pp. 275-300.

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

[11] Costa, G., Folino, F., Locane, A., Manco. G., & Ortale R. (2007). Data mining for effective risk analysis in a bank intelligence scenario. Proceedings of the 23rd International Conference on Data Engineering Workshop, IEEE Xplore Press, Istanbul, 904-911.