International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Survey on Credit Card Fraud Detection Techniques

P. Jayant
Electronics & Communication Department
Banasthali University, Rajasthan

Vaishali
Electronics & Communication Department
Banasthali University, Rajasthan

D. Sharma
Amity Institute of Information Technology
Amity University, U.P.

***Abstract* - Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. Since credit card is the most popular mode of payment, the number of fraud cases associated with it is also rising. In this paper, the survey on the present techniques available for detecting fraud in credit card is presented as a review paper. Fraud detection involves identifying fraud as quickly as possible once it has been done. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. The transaction is classified as normal, abnormal or suspicious depending on this initial belief. Once a transaction is found to be suspicious, belief is further strengthened or weakened according to its similarity with fraudulent or genuine transaction history using Bayesian learning.**

***Keywords* - *Credit card, fraud detection, supervised techniques, unsupervised techniques*.**

1. INTRODUCTION

The popularity of online shopping has grown day by day. According to an ACNielsen study conducted in 2005, one-tenth of the world's population is shopping online [1]. Credit card is the most popular mode of payment. As the number of credit card users is rising world-wide, the identity theft is increased and frauds are also increasing.

Credit-card-based purchases can be categorized into two types: 1) physical card purchase and 2) virtual card purchase. In a physical-card purchase, the cardholder personally presents the card to make a payment. While doing a physical card purchase, the attacker needs to steal the credit card and forge the signature in order to make a purchase. In the virtual card purchase, only the card information is required such as card number, expiration date, secure code, etc. Such purchases are normally done on the Internet or over telephone. To commit fraud in these types of purchases, a person simply needs to know he card details [1]. The mode of payment for online purchase is mostly done by credit card. Fraud in credit cards has been increased day by day. The amount of financial losses due to credit card frauds is growing as the usage of the credit cards is common. Security means to use credit card safely and avoid the occurrence of fraud. The purpose of security is to avoid fraudulent usage of credit cards. In Fraud cases issues like lost cards, stolen lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and non-received issue (NRI) fraud are found. For decreasing these frauds, security with credit cards is needed.

The details of credit card should be kept private. To secure credit card privacy, the details should not be leaked. Different ways to steal credit card details are phishing websites, steal/lost credit cards, counterfeit credit cards, theft of card details, intercepted cards etc. For security purpose, the above things should be avoided. The credit card security is needed for the detection of valid and invalid number of transactions. Most fraudulent transactions result from stolen card numbers rather than the actual theft of card. So, keep credit card safely.

A fraud committed over Internet like online credit card frauds becomes more popular because of their nature. In online fraud, the transaction is made remotely and only the card's details are needed. A manual signature, a PIN or a card imprint are not required at the purchase time. In most of the cases the genuine cardholder is not aware that someone else has seen or stolen his/her card information. The simple way to detect this type of fraud is to analyze the spending patterns on every card and to figure out any variation to the "usual" spending patterns.

Fraud detection by analysing the existing data purchase of cardholder is the best way to reduce the rate of successful credit card frauds. Transactions that were made by using payment cards such as credit cards, prepaid cards, debit cards and smart phones are considered as fraud. Credit card fraud can be defined as "Unauthorized account activity by a person for whom the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future" [2].

So, Credit Card Fraud is defined as when an individual uses another individual's credit card while the cardholder and the card issuer are not aware of the fact that the card is being used.

Fraud detection methods are developed to defend criminals from doing such illegal activities. The development of new fraud detection methods is made more difficult due to the limited ideas in fraud detection. As the data sets are not available and also the results are not disclosed to the public. The fraud cases should be detected from the available data sets known as the logged data and user behavior. At present, fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence.

1.1 Types of fraud

The types of frauds considered in this paper are Credit card frauds, Telecommunication frauds, Computer intrusions,

Bankruptcy fraud, Theft fraud/counterfeit fraud, Application fraud, Behavioral fraud.

Credit Card Fraud: Credit card fraud is divided into two types:

Offline fraud: Offline fraud is done by using a stolen physical card at any place**.**

On-line fraud: On-line fraud is committed over internet, phone, online shopping or when the card holder is not present.

Telecommunication Fraud [2] - The use of telecommunication services to commit other forms of fraud. Consumers, businesses and communication service provider are the victims.

Computer Intrusion - Intrusion is defined as the act of entering without warrant or invitation; that means "potential possibility of unauthorized attempt to access Information, Manipulate Information Purposefully. Intruders may be from any environment, an outsider (Or Hacker) and an insider who knows the layout of the system [3].

Bankruptcy Fraud - Bankruptcy fraud means using a credit card while being absent. Bankruptcy fraud is one of the most complicated types of fraud to predict [3].

Theft Fraud/ Counterfeit Fraud [3] - In this section, the focus is on theft and counterfeit fraud, which are related to one other. Theft fraud refers to the other person who is not the owner of the card. As soon as the owner give some feedback and contact the bank, the bank will take measures to check the thief as early as possible. Likewise, counterfeit fraud occurs when the credit card is used remotely; where only the credit card details are needed.

Application Fraud [3] - When any people apply for a credit card with false information then it is termed as application fraud. For detecting application fraud, two different situations have to be classified. When applications come from a same user with the same details, that is called duplicates, and when applications come from different individuals with similar details, that is termed as identity fraudsters. Phua et al [4] describes application fraud as "demonstration of identity crime, occurs when application forms contain possible, and synthetic (identity fraud), or real but also stolen identity information (identity theft)."

Internal Fraud - Banking sector allows their employees to access customer data. The data is the same information needed to access online banking to customer accounts. So the fraud can be done easily by an employee. Instead of this, financial institutions should require a password or PIN for net banking, and the password or PIN should be stored in the format of encrypted [5].

2. INTRODUCTION TO TYPES OF SOLUTIONS FOR THE FRAUD

Frauds and identity theft should be taken personally and the financially as a challenge. The frauds and identity theft can cause a lot of frustration.

How to Deal with credit card fraud? Fraud is considered as unauthorized use of credit card accounts. Usually fraud is discovered when a credit card is lost or stolen, when unfamiliar charges on the billing statement are found, when calls or letters about transactions that have not been made, contacted by the credit card company's fraud department to question about the charge. If the fraud is suspected on the account, then one should contact the credit card company immediately. The credit card company will be able to help in verifying the fraud, remove the charges which have not been used by the card holder or any authorized person, close down the account to prevent more fraudulent transactions and issue a new account number and new card, and transfer old information to the new account.

It's also a good idea to check credit report to be sure there's nothing else that looks suspicious. In most cases, the involvement of law enforcement will be coordinated with the financial institution.

How to Deal with identity theft? Identity theft is a particular type of fraud in which a thief uses the personal information to set up new accounts or get other benefits in the name of cardholder. Though it's not as common as other types of fraud, it can be more challenging and cause more severe problems.

Some signs of identity theft are: cardholder is not receiving the bills or other mail, receives credit card, being denied credit for no apparent reason, getting calls or letters about things that were not transaction by credit cardholder, being served court papers or arrest warrants for things in which there is no involvement of cardholder. Never assume that such unexplained occurrences are just a mistake always look into the details to find out for sure.

3. LITERATURE SURVEY

The fraud detection is a complex task and there is no system that correctly predicts any transaction as fraudulent. The properties for a good fraud detection system are:

1. Should identify the frauds accurately.
2. Should detect the frauds quickly.
3. Should not classify a genuine transaction as fraud.

Outlier detection is a critical task as outliers indicate abnormal running conditions from which significant performance degradation may happen. Techniques used in fraud detection can be divided into two: 1) Supervised techniques where past known legitimate/fraud cases are used to build a model which will produce a suspicion score for the new transactions [6]. 2) Unsupervised are those where there are no prior sets in which the state of the transactions are known to be fraud or legitimate.

3.1 Unsupervised outlier detection technique

An unsupervised outlier detection technique does not make any assumption about the availability of labeled data. This method simply seek those accounts, customer etc, whose behavior is "**unusual" [7]**. Unsupervised methods are useful in applications where there is no prior knowledge about the particular class of observations in a data set. An advantage of using unsupervised methods over supervised methods is that previously occurred undiscovered types of fraud may be detected. There are some techniques which were used now a day they are as follows:

Peer Group Analysis [7] - Peer Group Analysis (PGA) is an unsupervised method for monitoring behavior over time in data mining [8]. The main task of PGA method is to identify peer groups for all the present target observations (objects). The tool detects individual objects that begin to behave in a different manner from objects to which they had previously been similar. Each object is selected as a target object and is compared with all other objects in the database, using either external comparison criteria or internal criteria by summarizing earlier behavior patterns of each object. A peer group of objects most similar to the target object is chosen on the basis of comparisons. The tool

is a part of the data mining process that involves cycling between the detection of objects that behave in anomalous ways and the detailed examination of those objects.

PGA method is used in credit card fraud detection by changing the length of the time windows that is used initially to determine the peer group.

Break Point Analysis [7] - Break Point Analysis is another unsupervised outlier detection tool that is developed for behavioral fraud detection. A break point is an observation or time for detecting anomalous behavior. Break point analysis is operated on the account level by comparing sequences of transactions so that a change in behavior for a particular account is detected. In break point analysis, a fixed length moving window of transactions is present, as a transaction occurs it enters into the window and the oldest transaction from the window is removed.

An advantage of using break point analysis is that the 'balanced' data is not required as the transactions between different accounts are not compared and the anomalous sequences of events that may indicate fraudulent behavior can be identified.

K-Means Clustering technique [5] - K-Means clustering is the most simple and efficient method to cluster the data. Initially, the numbers of cluster K, and Centroid values are obtained. Any random objects as the initial Centroid or the first K objects can also serve as the initial Centroid. This technique is a non hierarchical method; initially it takes the number of objects equal to the final required number of clusters. Iterate until *stable* (= no object move group):

1. Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.
2. Assign each object to the group that has the closest centroid.
3. When all objects have been assigned, recalculate the positions of the K centroids.
4. Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.

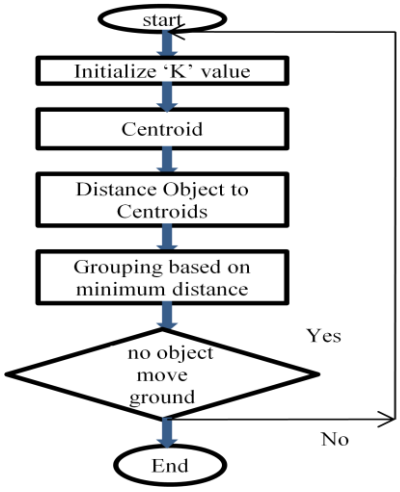

Fig.1. Block diagram of K- means algorithm process [5].

3.2 Supervised outlier detection technique

Supervised outlier detection techniques assume the availability of a data set which has been needed for the normal as well as the outlier class. Supervised method detects fraudulent transactions that can be used to differentiate between those accounts or transactions which are known to be fraudulent and those which are known to be legitimate. Classification techniques such as statistical discriminate analysis and neural networks can be used to discriminate between fraudulent and non-fraudulent transactions to give transactions a suspicion score. Supervised methods are only trained to differentiate between legitimate transactions and previously known fraud [7].

While doing the literature survey on various methods for fraud detection, there are multiple approaches like Gass Algorithm, Bayesian Networks, Hidden Markov Model (HMM), Genetic Algorithm (GA), A Fusion approach using Dempster-Shafer Theory and Bayesian learning, Decision tree, Neural Network (NN), Logistic Regression (LR).

Gass Algorithm [2] – Gass algorithm is a combination of genetic algorithm and scatter search. The basic idea is that the chance of survival for the stronger members of a population is larger than that of the weaker members and as the generations increases the average fitness of the population gets better. The less fit members of the generation are eliminated and the fittest members are selected as the parents for the next generation. This procedure is repeated until the best solution was found.

Bayesian Networks [2] - For fraud detection, two Bayesian networks to describe the behavior of user are constructed. First Bayesian network is constructed to model behavior under the assumption that the user is fraudulent (F) and the second model is constructed under the assumption that the user is a legitimate (NF). The 'fraud net' is set up by using expert knowledge and the 'user net' is set up by using data from non fraudulent users. During operation the user net is adapted by a specific user based on present data. By inserting evidence in the networks and propagating it through the network, the probability less than two is obtained. This shows at what degree the observed user behavior should meet typical fraudulent or non fraudulent behavior.

Bayesian networks also allow the integration of expert knowledge, which is used for initial set up in the models. On the other hand, the user model is retrained in an unsupervised way using data. Thus Bayesian approach incorporates both, expert knowledge and learning.

Hidden Markov Model [2] - A Hidden Markov Model is a double embedded stochastic process which is used to model much more complicated stochastic processes. If an incoming credit card transaction is not accepted by the trained Hidden Markov Model with sufficiently high probability, it is considered to be fraudulent transactions [9]. *Baum Welch* algorithm is used for training purpose and K-means algorithm for clustering.

In HMM, the data is stored in the form of clusters depending on three price value ranges low, medium and high. If the probabilities of initial set of transaction is chosen and then FDS will check whether transaction is genuine or fraudulent. Since HMM maintains a log for transactions it reduces the load of work on employees but simultaneously produces high false alarm as well as high false positive. The initial choice of parameters which affects the performance of the algorithm should be chosen carefully.

Genetic Algorithm [2] - Genetic algorithms, inspired from natural evolution was first introduced by Holland (1975). Genetic algorithms are an evolutionary algorithm which provides better solutions as time progresses. Fraud detection has been usually in domain of Ecommerce data mining [10]. GA is used in data mining mainly for variable selection [11] and is mostly coupled with other DM algorithms. Its combination with other techniques has a very good performance. GA is used in credit card fraud detection for reducing the wrongly classified number of transactions. And it is easily accessible for computer programming language implementations which make it strong in credit card fraud detection.

But this method has high performance and is quite expensive.

A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning [2] - Dempster-Shafer Theory proposes Fraud Detection System using information fusion and Bayesian learning in which the evidences of both the current as well as the past behavior are combined together and depending on certain type shopping behavior establishes an activity profile for every cardholder.

The advantages are high accuracy, processing speed, reduces false alarm, improves detection rate, applicable in E-commerce. There is only one disadvantage of this approach that it is highly expensive. The FDS system consists of four components, namely, rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner. The transaction is classified as suspicious or suspicious depending on its initial stage. Once a transaction is found to be suspicious, belief is strengthened or weakened by comparing fraudulent or genuine transaction.

Decision Tree [2] - Decision trees are statistical data mining technique that uses independent attributes and a dependent attributes which are logically AND in a tree shaped structure. The classification rules extracted from decision trees are IF-THEN expressions and all the tests have to succeed if each rule is to be generated. Decision tree usually separates the complex problem into many simple ones and resolves the sub problems through repeatedly using [11]. Decision trees are predictive decision support tools which create mapping from observations. Decision tree methods are C5.0, C&RT and CHAID. The data mining techniques including decision trees and SVMs to the credit card fraud detection problem is useful in reducing the bank's risk.

Neural Network [2] - Fraud detection methods based on neural network are popular. An artificial neural network [12] consists of an interconnected group of artificial neurons .The principle of neural network is motivated by the functions of the brain especially pattern recognition and associative memory [13]. The neural network identify similar patterns, predicts future values or events based upon the associative memory of the learned patterns. It is applied in classification and clustering. The advantages of neural networks over other techniques are that this model learns from the past and thus, improve results as time passes. They can also extract rules and predict future activity based on the current situation.

The two phases of neural network are training and recognition. Learning in a neural network is called training. The NN training methods are supervised and unsupervised. In supervised training, samples of both fraudulent and non fraudulent records are taken to create models. While unsupervised training simply seeks those transactions, which are more different from the normal one though the unsupervised techniques do not need the previous knowledge of fraudulent and non fraudulent transactions in database. NNs are best for large transaction dataset.

Logistic Regression [2] - The two data mining approaches, are support vector machines and random forests, together with the well known logistic regression, as part of an attempt to detect the credit card fraud. It is well-understood, easy to use, and it is most commonly used for data-mining. Thus it provides a useful baseline for comparing performance of newer methods.

Supervised learning methods for fraud detection face two challenges. They are:

1. The unbalanced class sizes of legitimate and fraudulent transactions, with legitimate transactions far outnumbering fraudulent ones.

2. The second is to develop supervised models for fraud that can arise from potentially undetected fraud transactions, leading to mislabeled cases in the data to be used for building the model.

For the purpose of the above problems, the fraudulent transactions are those specifically identified by the institutional auditors as those that caused an unlawful transfer of funds from the bank sponsoring the credit cards. These transactions were observed to be fraudulent expose. The study is based on real-life data of transactions from an international credit card operation.

4. ANALYSIS OF EXISTING TECHNIQUES

Srivastava et al. [1] has implemented a model to show the sequence of credit card transaction process and presents the experimental results which shows the effectiveness of the system and demonstrate the usefulness of learning the spending profile of cardholders. Comparative studies reveal that the Accuracy of the system is close to 80 percent over a wide variation in the input data. Accuracy represents the fraction of total number of transactions (both genuine and fraudulent) that have been detected correctly. The system is also scalable for handling large volumes of transactions.

Suman and Nutan [2] has presented a survey of current techniques used in credit card fraud detection and telecommunication fraud. In this paper, comprehensive review of different techniques to detect fraud is provided. Various types of frauds in this paper include credit card frauds, telecommunication frauds, and computer intrusions, Bankruptcy fraud, Theft fraud/counterfeit fraud, Application fraud, Behavioral fraud. Gass algorithm, Bayesian networks, Hidden markov model, Genetic algorithm, A fusion approach using dempster-shafer theory and Bayesian learning, Decision tree, Neural network and Logistic Regression techniques are explained to detect credit card fraud. One aim of this paper is to identify the user model that best identifies fraud cases.

Delamaire et al. [3] has identified the different types of credit card fraud such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud and review alternative techniques that include pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms. Also state the problems that have been faced by the banks and credit card companies. The next step in this research program is to focus on the implement of a 'suspicious' scorecard on a real data-set and its evaluation. The main tasks should be to build scoring models to predict fraudulent behavior, taking into account the fields of behavior that should be related to the different types of credit card fraud identified in this paper, and to evaluate the

associated ethical implications. The plan is to take one of the European countries, probably Germany, and then to extend the research to other EU countries.

Phua et al. [4] proposed an innovative fraud detection method, built upon existing fraud detection research and *Minority Report*, to deal with the data mining problem of skewed data distributions. For experiment, Angoss Knowledge Seeker software is used. In this paper, success rates *X* outperformed all the averaged success rates *W* by at least 10% on evaluation sets. When applied on the score set, bagged success rates *Z* performed marginally better than the averaged success rates *Y*. The future work is to make one classifier more appropriate than another.

Esakkiraj and Chidambaram [5] has design a predictive model with sequence of operations in online transaction by using hidden markov model (HMM) and decides whether the user act as a normal user or fraud user. In the trained system, the new transaction is evaluated with transition and observation probability. Depending upon the observation probability, system finds the acceptance probability and decides whether the transaction should be declined or not. Normally existing fraud detection system for online banking will detect the fraudulent transaction after completion of the transaction. This causes the economic loss and makes the bank name as unsecured. The model predicts the fraudulent during the transaction time and prevents the money transfer. As future work, some effective classification algorithms instead of using clustering which can perform well for the prediction.

Sahin and Duman [6] has used seven classification methods using decision tree algorithm and SVM to build fraud detecting model for the improvement of the financial transaction systems in an effective way. This work demonstrates the advantages of applying the data mining techniques including decision trees and SVMs to the credit card fraud detection problem with the real data set. In this study, the performance of classifier models built by using the well-known decision tree methods C5.0, C&RT and CHAID and a number of different SVM methods (SVM with polynomial, sigmoid, linear and RBF kernel functions) are compared. When the performances of the models are compared with respect to accuracy, it is seen that as the number of the training data increases, this over fitting behavior becomes less remarkable and the performances of the SVM based models become comparable to decision tree based models. But the number of frauds caught by SVM models is less than the decision tree models, especially C&RT model. Though C5.0 model is the champion over the other models with respect to accuracy for each sample, C&RT model catches the largest number of frauds. So the C&RT and C5.0 models are choose as the final methods to build the prediction model. As a future work, other data mining algorithms such as different versions of Artificial Neural Networks (ANN) and logistic regression will be used to build new classification models on the same real world dataset and the performance of the new models will be compared with the performance of the models given in this paper.

Bolton and hand [7] has explained the two categories: behavioral fraud and application fraud. But this paper is concerned with detecting behavioral fraud through the analysis of longitudinal data. So two methods for unsupervised fraud detection in credit card are discussed here and have applied them to some real data sets. Peer group analysis which is the new tool for monitoring behavior over time in data mining situations followed by break point analysis were discussed here. It describes an implementation of PGA to detect changes in credit card account spending behavior and illustrates its propensity to detect outliers through a simulation study. An example of credit card spending in 858 accounts over 52 weeks period with the total spending recorded per week is shown and PGA can detect that the spending for these weeks is unusual amongst accounts that have similar spending trends

Ferdousi and Maeda [8] has presented in this paper the problem of finding outliers in time series financial data using Peer Group Analysis (PGA) which is a unsupervised technique for fraud detection. It can be observed that PGA can detect those brokers who suddenly start selling the stock in a different way to other brokers to whom they were previously similar. The experiment is conducted on PGA tool in an unsupervised problem over the stock market data sets with continuous values over regular time intervals. The experimental results were shown through graphical plots that peer group analysis can be useful in detecting observations that deviate from their peers. Also t-statistics is applied to find the deviations effectively. The future work is to integrate some other effective methods with PGA and also apply this strategy on other more applications, such as banking fraud detection.

Mishra et al. [9] has present the necessary theory to detect fraud in credit card *transaction* processing using a Hidden Markov Model and shows how the model is used for the detection of fraud. If an incoming credit card transaction is not accepted by the HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, they try to ensure that genuine transactions are not rejected. Different ranges of transaction amount as the observation symbols has been used whereas the types of items has been considered to be states of the HMM. Also a method for finding the Spending Profile of the Cardholders as well as application of this knowledge in deciding the observation symbols is suggested. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not and if it is found to be fraudulent then how the user is notified instantly regarding the fraud. In the proposed model more than 85% transactions are genuine and very low false alarms are about 8% of the total number of transactions. Comparative studies reveal that accuracy of the system is close to 82% over a wide range of input data.

In this paper, *RamaKalyani and UmaDevi* [10] are proposing a credit card fraud detection system using genetic algorithm. The aim is to develop a method of generating test data and to detect fraudulent transaction by using the genetic algorithm. This algorithm is an optimization technique and evolutionary search based on the principles of genetic and natural selection, heuristic used to solve high complexity computational problems and examines the result based on the principles of this algorithm. This algorithm is applied into bank credit card fraud detection system and the probability of fraud transactions can be predicted soon after credit card transactions by the banks.

Chang et al. [11] proposed a new learning methodology towards developing a novel intrusion detection system (IDS) by back propagation neural networks (BPN) with sample-query and attribute-query. In this paper, combination of data reduction and classification with a query-based learning methodology is used because it is less time consuming. Experiment has showed that the training time of the proposed method is 1447 seconds. However, the training of BPN is over 21746 seconds. The future work is to extend the concept of BPN to develop more learning methods for more real world applications.

Patidar and Sharma [11] has used the neural network along with the genetic algorithm to detect fraudulent transaction. For the

learning purpose of artificial neural Network, supervised learning feed forward back propagation algorithm is used. In this paper, BPN is used for training purpose and then in order to choose those parameter (weight, network type, number of layer, number of node etc.) that play an important role to perform neural as accurately as possible, genetic algorithm is used and using this combined Genetic Algorithm and Neural Network (GANN), detection of the credit card fraud is tried successfully. The future work is to design some system that may control credit card fraud before any real transaction is made.

Subashini and Chitra [13] has build the classifier models i.e. C5.0, CART from five classification methods: decision tree, SVMs using SMO algorithm with kernels of polynomial functions, Logistic regression and Bayes Net for detecting fraud in the banking sector using credit card fraud data set. The legitimate user is denoted by good and the fraud user is denoted by bad. C5.0 using J48, SVM using SMO and Bayes Net has been giving the success rate of 72.4% whereas the Bad to Good classification is more in SVM using SMO because classifying a Bad customer as Good is more worse than the classifying a Good customer as Bad. While the logistic regression method provides a success rate of 73.1% and CART gets the highest success rate 74.1%. Therefore depending on the success rate CART outperforms the other models whereas considering the Bad to Good classification J48 shows better performance. Hence, while classifying the customers different classification methods should be used to make the correct decision about a customer.

Phua et al. [14] has categorizes, compares and explored almost all published technical and review articles in automated fraud detection. The paper defines the professional fraudster, types and subtypes of fraud, the technical nature of data, performance metrics, methods and techniques. After studying the limitations in methods and techniques of fraud detection, the paper shows that this field can be benefited from other related fields such that the unsupervised approaches from counterterrorism work, actual monitoring systems and text mining from law enforcement, and semi supervised and game-theoretic approaches from intrusion and spam detection communities can contribute to future fraud detection research.

Bagheri et al. [15] evaluated the performance of an ensemble of three classifiers, each trained on different data sets. A powerful combination strategy based on the Dempster-Shafer theory is used to combine the three classifiers trained on different sources. The classification results of the individual classifiers were compared with those obtained from fusing the classifiers by the Dempster-Shafer combination method. By using the DS fusion method, the classification performance was significantly improved compared with single classifiers trained by a specific set of features.

Maes et al. [16] has discussed the credit card fraud, its detection and the problems related to credit card fraud. They briefly explained the two machine learning techniques: Artificial Neural Network (ANN) and Bayesian Belief Network (BBN) and shows their significant results on the real world financial data. ANN use backpropogation of error signal or in short backprop. On the basis of the experiments conducted, the results of BBN and ANN were compared. It shows that BBN detects 8% more of the fraudulent transaction than the ANN. BBN shows better result than ANN and the training period is shorter about 20 minutes while ANN takes several hours. But the ANN detects the fraud much faster than the BBN.

5. CONCLUSION AND FUTURE WORK

Credit card fraud has become more and more rampant in recent years. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. In Fraud detection, identifying Fraud as quickly as possible once it has been done through fraud detection techniques, is now becoming easier and faster. The techniques which were studied here, through which credit card fraud can be detected quickly and fast and the crime can be stopped.

The Future work is to design an improved technique which will be much better than the available techniques.

6. ACKNOWLEDGMENT

We would like to take opportunity to thank to Dr. Ashok K. Chauhan, Founder President, Amity University to provide necessary support and infrastructure to carry out the research work. We would like to thank Mr. Aditya Shastri, Vice chancellor, Banasthali University who has rendered their continuous help and support to us.

7. REFERENCES

[1] A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, **"**Credit card fraud detection using hidden markov model"**,** IEEE transactions on dependable and secure computing, vol. 5, no. 1, january-march 2008.

[2] Suman and Nutan **"**Review paper on credit card fraud detection", International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[3] L. Delamaire, H. Abdou and J. Poinon, "Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[4] Phua, D. Alahakoon and V. Lee, "Minority report in fraud detection: classification of skewed data," ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[5] S. Esakkiraj and S. Chidambaram, "A predictive approach for fraud detection using hidden markov model" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 C.

[6] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines", International Multiconference of Engineers and computer scientists March, 2011

[7] R.J. Bolton and D.J. Hand **"**Unsupervised profiling methods for fraud detection", Department of Mathematics Imperial College London {r.bolton, d.j.hand}@ic.ac.uk

[8] Z. Ferdousi and A. Maeda **"**Unsupervised outlier detection in time series data"**,** Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW'06) © 2006 IEEE.

[9] J.S. Mishra, S. Panda, and A. Kumar Mishra, "A novel approach for credit card fraud detection targeting the Indian market" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, May 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org

[10] K. Rama Kalyani and D. Uma Devi**,** "Fraud detection of credit card payment system by genetic algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 7, July-2012.

[11]Ray-I Chang, Liang-Bin Lai, Wen-De Su, Jen-Chieh Wang and Jen Shiang Kouh "Intrusion detection by back propagation neural networks with sample-query and attribute-query", Research India Publications; (2006). (6-10).

[12] R. Patidar and L. Sharma ,**"**Credit card fraud detection using neural network**"** NCAI2011, 13-14 May 2011, Jaipur, India International Journal of Soft Computing and Engineering

(IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011.

[13] B. Subashini and Dr. K. Chitra "Enhanced system for revealing fraudulence in credit card approval", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 8, August – 2013 ISSN: 2278-0181.

[14] L. Phua, V. lee, K. Smith and R. Gayler, "A comprehensive survey of data mining-based fraud detection research", School of Business Systems, Faculty of Information Technology, Monash University, Clayton campus, Wellington Road, Clayton, Victoria 3800, Australia.

[15] M. A. bagheri, Q. GAO and S. Escalera "Logo recognition based on the dempster-shafer fusion of multiple classifiers", Advances in Artificial Intelligence, Lecture Notes in Computer Science Volume 7884, 2013, pp 1-12.

[16] Maes, S., Tuyls, K., Vanschoenwinkel, B. & Manderick, B. (2002), "Credit card fraud detection using bayesian and neural networks", Proc. of the 1st International NAISO Congress on Neuro Fuzzy Technologies.