Applications of Data Mining Techniques for Fraud Detection in Credit-Debit Card Transactions.

Mrs. Poonam M. Deshpande[1] Prof. Abul Hasan Siddiqi[2] Dr. Khursheed Alam[3] Mr. Khinal Parmar [4]
[1,4]Assistant Professor
[1,4]Department of Humanities and Applied Sciences [2,3]Department of Mathematics
[1]Atharva College of Engineering, Mumbai University,Mumbai, India [2,3]School of Basic Sciences & Research, Sharda University, Greater Noida, Uttar Pradesh 201306, India [4]Mukesh Patel School of Technology Management & Engineering, Vile Parle(W), Mumbai-400056, India

Abstract— Although the term FRAUD has varied definition and numerous fields to perpetrate, the major setback due to fraud is in the Credit/Debit Card Not Present (CNP) transaction like internet purchase, mail transactions (MT), telephonic transactions (TT) etc. The card fraud losses are in Billions of dollars and on the rise. The fraudsters always find novel ways to commit frauds and they know how to go around the system. Most of the times the fraud detection is done after the fraud are already committed and many of the frauds go unnoticed. Therefore credit card fraud detection methods need constant innovation [1] and all the financial institutions are required to have some fraud detection models or techniques in place to deal with such a scenario. Data Mining is basically a tool for pattern discovery, outlier or anomaly detection. It works well in detecting different types of frauds. This paper takes a review of various fraud detection techniques based on Data Mining like Neural Network, Support Vector Machines, K-nearest Neighbor, Artificial Immune System, Peer group analysis [2] etc.. We also give suggestions for a new technique which can be implemented and which will seize the essence of the existing techniques and may be combine few of them to give superior fraud detection tool.

Key words: Data Mining, Credit Card Fraud, Peer Group Analysis, Pattern discovery, Behavioral Data, Neural Network

I. INTRODUCTION

With the advancement in technology the online shopping is on the rise and e-commerce is booming. The vastly available products all over the world can be viewed and purchased online through various e-commerce websites, not to forget the attractive sales tactics like discounts and many other offers. A customer can make payment to the company in the US even though the transaction is made from some other country. In just few clicks customers can compare multiple products from multiple retailers making it easy for selecting the best product at cheaper price. Therefore the use of plastic money that is credit/debit card is evitable. There are two types of transactions for credit/debit cards first is Card Present (CP) that is when the customer makes a payment physically with a card and second is Card Not Present (CNP) where the payment is done virtually where the physical card is not present like for telephonic and online transactions. Such a scenario gives rise to fraud in credit/debit card transactions mainly which are of CNP type as the fraudster needs the information of the card and then he is all armed to commit fraud.

Fraud detection is a problem of novelty detection. With the extensive availability of unmanned consumer communication channels (e.g., internet, mobile banking, telephone banking etc.), the challenge of controlling fraud has increased substantially [3].

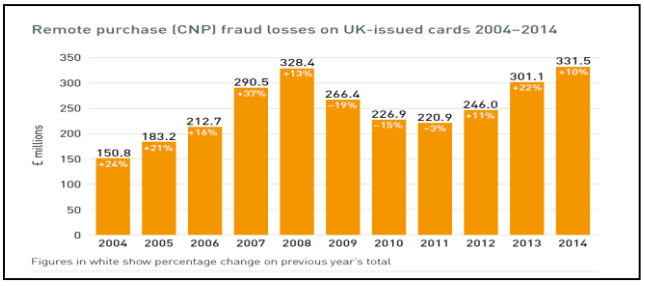

Fig. 1: (Source, Financial Fraud Action, UK, 2015)

In the year 2014 the overall impact of card fraud in India was41% and the impact for last five years record shows 32%., whereas in the UK the overall impact is of 28% and25% for the last five years [4].Intelligence suggests criminals are targeting business accounts which typically allow higher value fraudulent transactions. Losses due to CNP (those made online, over the telephone or by mail order) rose to £174.5 million in the first six months of 2014, up 23 per cent from £142.0 million in the same period in 2013. Within this total, the e-commerce fraud loss is

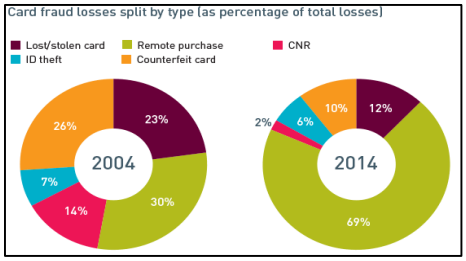

Fig. 2: (Source, Financial Fraud Action, UK, 2015)

Estimated to be £110.0 million, up 23 per cent from an estimated £89.5 million in the first half of 2013 [3]. The ACI worldwide report [8] mentioned in their report that the online retail card fraud that is CNP fraud rose by 30% in 2015 as compared to 2014. They also mentioned that the trend in card fraud is the lower spend on transaction but higher frequency of transactions. One more principle finding in their report was that the 1 out of 86 transactions are fraudulent in 2015 as compared to 1 out of 114 is fraudulent in 2014.

In the report presented by DELEGO for RSA, U.S [6], it is mentioned that the CNP fraud losses in 2014 were US $2.9 billion and they will exceed US$6.4 billion by 2018.

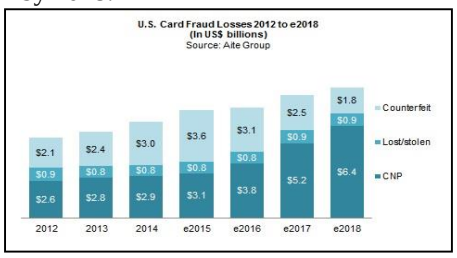

Fig. 3: (Source, Aite Group, US 2015)

Every year we can see the increase in the number of fraud as well as number of types of fraud. The trends in fraudulent

Fig. 4: (Source, Aite Group, US 2015)

behavior often Change, making it difficult to catch these fraudsters. [3]Sanjeeva Murthy Executive Vice President – Compliance of Kotak Bank commented that "The fraudster is always ahead of the controls or risk mitigants which will be put in place by the Banks. However, Banks have to be agile and think ahead of the fraudsters and put in place control measures quickly. The cat and mouse game has been going on in the past and will continue to be in future, but Banks have to devise ways to be ahead" [7].

All the above discussion is about how much and how fraud has impacted the worldwide economy but the question is how to deal with this situation and detect the fraud and stop or cap the losses due to card fraud. Over the years researchers have developed variety of credit/ debit card fraud detection techniques. In this paper we take a look at few of these methods and compare them for their pros and cons and we will also try to propose a new hybrid Model for Credit Card Fraud detection system which will capture the essence of these existing Methods and will try to combine 2 or more of them for building a superior Fraud Detection Model.

II. WHAT IS FRAUD

The Concise Oxford Dictionary defines fraud as "criminal deception; the use of false representations to gain an unjust advantage." Fraud is as old as humanity itself and can take an unlimited variety of different forms. However, in recent years, the development of new technologies (which have made it easier for us to communicate and helped in increasing our spending power) has also provided yet further ways in which criminals may commit fraud. Traditional forms of fraudulent behavior such as money laundering have become easier to perpetrate and have been joined by new kinds of fraud such as mobile telecommunications fraud and computer intrusion. We begin by distinguishing between fraud prevention and fraud detection. Fraud prevention describes measures to stop fraud from occurring in the first place [21] and fraud detection comes into picture where fraud prevention fails. Fraudsters normally work individually or in group. The trend in fraudulent activity can change depending upon the situation as we see the number of frauds rising during recession or during festive seasons etc. Fraud occurs in all aspects of human life, but the motivation may not be always the same. Here we can think of motivation behind fraud as money and/or power. If motivation is money then it can lead to different types of fraud such as banking fraud, telecommunications fraud, insurance fraud, health care fraud etc. whereas if motivation is power then it can cultivate scientific fraud, terrorism fraud etc.

III. DATA MINING TECHNIQUES

Data mining techniques are nothing but pattern discovery techniques. Every data set has a history of behavior and if any data element diverts from that behavior then we need to check what caused this diversion. The diversion caused maybe because of natural causes and may be legitimate but there is a chance that the change is due to fraudulent activity, such a data element is called as an outlier. One of the commonly used fraud detection technique is outlier detection. Outliers are members of data set that are not consistent with the remaining members of the dataset [10] or deviate so much from other observations so as to arouse suspicion that they were generated by a different mechanism [11]. Outlier detection can be done by techniques like neural network, self-organizing maps, Peer Group Analysis and Break Point Analysis etc. In particular, neural networks, a supervised learning technique received much attention [12]. Researchers who have used neural networks for credit card fraud detection include Ghosh and Raillery [13], Dorronsoro [14] and Brause [15]. Above mentioned fraud detection methods were all supervised classification techniques. Unsupervised fraud detection techniques for credit card fraud detection were discussed in detail by Bolton and Hand [16] with the introduction of Peer Group Analysis (PGA) and Break Point Analysis. Unsupervised Profiling method for fraud detection for credit card fraud detection was used by Boltan, R and Hand, D [17]. Ekrem, D. and Hamdi, O. developed a new and faster fraud detection system for Credit card fraud using genetic algorithm and scatter search [18]. They also claimed to have minimized the False Positive rate (FPR). FPR is nothing but the ration of the false alarms to the true alarms raised by the fraud detection system. Neda, S. and Mohamaad, K. used the Artificial Immune system (AIRS) based Fraud Detection system (AFDM) [19] which runs AIRS and Cloud Computing on a parallel level to achieve the desired time related target. There are many supervised methods for fraud detection, but they are all complex so to simplify this Nadar, M. and Ekrem, D. [20] used Modified Fisher Discriminant system for the first time which uses linear Discriminant function. Masoumeh, Z. and Pourya, S. Developed the fraud detection system using 'Bagging Ensemble Classifier' and the technique was proposed by Leo Breimen [22] which works on the decision tree method and the authors claim that this method is much faster and efficient and it can handle data which is unbalanced, large and has thousands of features. Vlasselaer, V. et al introduced APATE (Anomaly Prevention using Advanced Transaction Exploration) system which used network based extensions [23]. There are numerous materials available online for fraud detection techniques or classification techniques but basically they are of two types Supervised Classification and unsupervised Classification.

A. Supervised Methods

Statistical fraud detection methods may be 'supervised' or 'unsupervised'. In supervised methods, models are trained to differentiate between fraudulent and non-fraudulent behavior, so that new observations can be assigned to classes so as to optimize some measure of classification performance. Of course, this requires one to be confident about the true classes of the original data used to build the models; hesitation is introduced when genuine transactions are mistakenly reported as fraud or when fraudulent observations are not identified as such [16]. Supervised methods require that we have examples of both classes, and they can only be used to detect frauds of a type that have previously occurred. These methods also endure the problem of unbalanced class sizes: in fraud detection problems, the legitimate transactions generally far outnumber the fraudulent ones and this imbalance can cause misspecification of models. Brause et al [15] say that, in their database of credit card transactions, 'the probability of fraud is very low (0.2%) and has been lowered in a pre-processing step by a conventional fraud detecting system down to 0.1%.All though there are many sophisticated techniques in supervised classification for fraud detection, but we will discuss techniques which are very popular in the class of supervised methods, they are Neural Networks and Bayesian Networks. One more method that has caught my attention is Trend offset analysis, as it is simple to understand and its practicability towards the application to the specific problem of fraud detection we are covering in this project. Let us explore these fraud detection techniques based on supervised classification.

1) Trend offset analysis [12]

Fraud detection in a debit card data can be done using Trend Offset Analysis (TOA) [12] focuses on identifying pattern changes at an individual account level. Bolton and Hand have proposed a similar technique, Break Point Analysis that focuses on identifying pattern changes for individual accounts but it utilizes an unsupervised learning technique. TOA is a supervised learning technique. We have to assign a signature to each account based on most recent history of transaction behavior. Any significant deviation in current behavior from the assigned signature is used for outlier detection. In other words, we can identify the spending behavior of a particular account, and tag it as a local outlier if it is anomalous to the previously identified spending behavior of the same account (not necessarily anomalous to the entire population of transactions). Trend offset analysis primarily follows three basic steps as shown in Figure 5

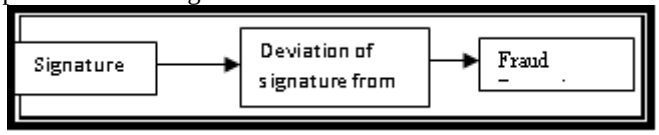

Fig. 5: Flow chart for Trend Offset Analysis.

In TOA, a fixed length-moving window of transactions is considered for identifying spending behavior. The characteristic spending behavior of each account is termed as a Signature. Current behavior is compared to this signature to tag local outliers. In moving window, the transactions are accounted as they enter into the window and the oldest transactions in the window are removed. If each transaction have characteristics denoted by [T1, T2…TJ] A, T for an account A at time T then the signature [S1, S2…SK] A of account A is calculated as mean, median, minimum, maximum and standard deviation over all transactions [T1,T2…TJ] A, T. If D0 denotes current day, D1 denote previous day and D30 denotes 30 days prior to current

day then D1 to D30 are a part of the window W while transactions on D0 are compared to the signature calculated over the time period W. Figure 6 shows Deviation of an account from Signature.

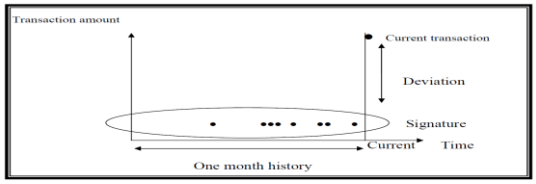

Fig. 6: Pictorial representation of Trend Offset Analysis

Figure 6, is an illustration of the deviation of current transaction from the signature of the account based on transaction amount. The most distinctive characteristic of TOA lies in its focus on personalized patterns, i.e. at account level, rather than on global trends. In the traditional approach to capture fraud, fraudulent patterns as compared to the entire population are considered (Global outlier detection models). For example, number of transactions in a specified time frame, dollar amount of transaction, channel by which the transaction is occurring are a few examples of traditionally used variables to detect fraud patterns. TOA relies on identifying deviations in the current values of these variables from their historically observed values. Exact variables and the type of deviation (deviation from minimum, maximum, mean), that predicts fraud behavior better is dependent on the portfolio under study [12].

2) Neural Network [12]

There are many types of Artificial Neural Networks (ANN) but the most common type is the feed-forward Perceptron illustrated here in figure 3. This network consists of three layers of nodes. 1. The input layer 2. The hidden layer 3.The output layer. Data is passed forward through the network as illustrated by the black connecting lines. A transaction presented to the input will result in a score at the output, which can be used to tag the corresponding transaction as suspicious fraudulent or legitimate. The curved line in the boxes of hidden layer is a non-linear function (e.g. Sigmoid function which is given by $f(x) = 1/(1 + e^{-ßx})$). The training of an ANN consists of adjusting the connection weights associated with each of the connection lines so that the errors are minimized in the output from the network when presented with inputs from the training data. Training a neural network is a form of optimization and can be a very slow process on complex highly nonlinear data. Apart from the complexity in training neural networks they have several other draw backs. The nature of the training process does not allow incremental learning so whenever the network needs to be re-trained it is necessary to pass the full training set through the network. When a neural network produces a score it is very difficult to understand why it produced the result it did. This is in contrast to most other methods. On the other hand Neural Networks can be very good at dealing with highly skewed data like card fraud data and once trained are very fast.

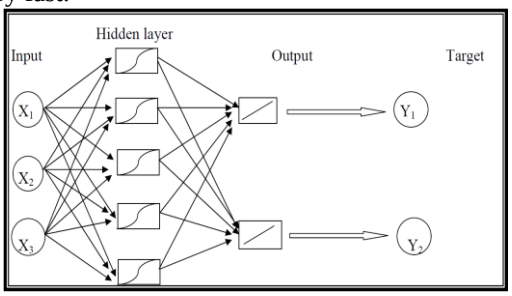

Fig. 7: Artificial Neural Network

3) Bayesian Networks: [24]

According to Kilo [24] the purpose of any fraud detection system is to produce a score that reflects the probability that a particular transaction is fraudulent given some set of evidence. In other words he says that we want to find the probability of fraud given the evidence. However, by profiling the historic (training) data this will only tell us the probability of the evidence given it is fraud. Bayes tells us how to use these so called a priori probabilities to compute the desired posterior probability. The simple form of Bayes is just an expression of conditional probability

$$P(F \mid \text{evidence}) = \frac{P(\text{evidence} \mid F)\, P(F)}{P(\text{evidence}\mid)}$$

Profiling variables is a standard statistical approach. If we profiled rate-of-spend for instance in both the legal (untagged) data and the fraud (tagged) data we would get frequency distributions that look like those illustrated in figure 4. The fraud distribution is greatly exaggerated just to illustrate. This is an example of a very good differentiator of fraud as the two distributions are well separated. In general, this is not the case [24]

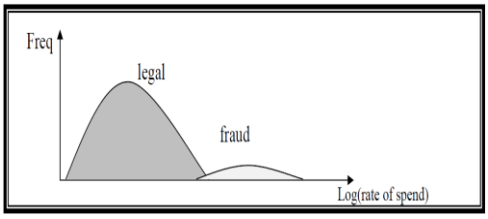

Fig. 5: Frequency distributions of legal and fraud transactions

From these two distributions one can compute the probability of fraud as follows. Now let V be the set of values for a derived variables and v $\subset$ V. Also let S, be the set of states for the systems $\subset$S = (fraud, legal). The system can only be in one of the states. In this particular case there are only two possible states and therefore we can write P(fraud) + P(legal) =1. In general we seek, P(s = fraud | v) and from Bayes we have

$$P(\text{fraud} \mid v) = \frac{P(v \mid \text{fraud})\, P(\text{fraud})}{P(v)} \qquad (1)$$

This then leads to the following. As

$$P(\text{fraud} \cap v) = P(\text{fraud} \mid v)\, P(v) \text{ and}$$
$$P(\text{legal} \cap v) = P(\text{legal} \mid v) P(v) .$$

We can therefore write,

$$P(\text{fraud} \cap v) + P(\text{legal} \cap v) = [P(\text{fraud} \mid v) + P(\text{legal} \mid v)]P(v) = P(v) \text{ and then using}$$
$$P(\text{fraud} \cap v) = P(\text{fraud} \mid v)P(v) \text{ ,etc we have}$$
$$P(v \mid \text{fraud})P(\text{fraud}) + P(v \mid \text{legal})P(\text{legal}) = P(v)$$

So we can write (1) as:

$$P(\text{fraud} \mid v) = \frac{P(v \mid \text{fraud})\, P(\text{fraud})}{P(v \mid \text{fraud})\, P(\text{fraud}) + P(v \mid \text{legal})\, P(\text{legal})}$$

$$P(fraud \mid v) = \frac{1}{1 + \frac{P(v \mid legal)\, P(legal)}{P(v \mid fraud)\, P(fraud)}}$$

B. Unsupervised Methods

In contrast to supervised methods, unsupervised methods simply seek those accounts, customers, etc. whose behavior is 'unusual' [25]. Unsupervised methods are useful in applications where there is no prior knowledge as to the particular class of observations in a data set. A baseline model can be constructed to represents normal behavior and then attempt to detect observations that show greatest departure from this norm. These can then be examined more closely. Again in this case also outliers are a basic form of nonstandard observation that can be used for fraud detection.

An example of application of unsupervised methods to the banking industry is so-called 'behavioral models' which aim to distinguish the legitimate transaction behavior of each individual account over a period of time. For example, customer XYZ only uses his credit card for retail purchases at supermarkets and high street shops, whilst customer PQR tends to use his card for online purchases, especially at bookmakers. If, at some future time, online transactions start to appear on customer XYZ's account, this change in behavior may be indicative of fraud. Likewise, if an unusual proportion of high street purchases are made on customer PQR's account, this might also be considered suspicious, as it is not characteristic of that customer's previous behavior. Behavioral models only consider the previous history of each account but do not attempt to identify global patterns of fraudulent behavior; they only try to detect changes in behavior. The problem is that a change in behavior may not be due to fraud [26].

As mentioned above, the stress on fraud detection methodology is with supervised techniques. In particular, neural networks have proved popular [25]. Perhaps, given the attention they have received. However, unsupervised credit/debit card fraud detection have not received attention in the literature.

The most popular unsupervised method used in data mining is clustering. This technique is used to find natural groupings of observations in the data and is especially useful in market segmentation. However, cluster analysis can suffer from a bad choice of metric (the way one scale, transform and combine variables to measure the 'distance' between observations); for example, it can be difficult to combine categorical and continuous variables in a good clustering metric. Observations may cluster differently on some subsets of variables than they do on others so that we may have more than one valid clustering in a data set. Let us explore two fraud detection technique based on unsupervised clustering technique.

1) Peer- group Analysis:

Peer group analysis is a new tool for monitoring behavior [16] over time in data mining situations. In particular, this tool detects individual objects that begin to act in a way discrete 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 summarizing earlier behavior patterns of each object. Based on this comparison, a peer group of objects most similar to the target object is chosen. The behavior of the peer group is then summarized at each subsequent time point, and the behavior of the target object compared with the summary of its peer group. Those target objects exhibiting behavior on the majority, different from their peer group summary behavior are flagged as suspicious and are sent for further investigation. The tool is intended to be part of the data mining process, involving cycling between the detection of objects that behave in anomalous ways and the detailed examination of those objects. Several aspects of peer group analysis can be tuned to the particular application, including the size of the peer group, the width of the moving behavior window being used, the way the peer group is summarized, and the measures of difference between the target object and its peer group summary.

The distinctive feature of Peer Group Analysis (PGA) lies in its focus on local patterns rather than global models [16] a sequence may not evolve unusually when compared with the whole population of sequences but may display unusual properties when compared with its peer group. That is, it may begin to deviate in behavior from objects to which it has previously been similar.

2) Transaction Aggregation Method.

Two class supervised methods are based on modeling both the distribution of past legitimate transactions, and the distribution of past fraudulent transactions. If the behavior of fraudsters changes over time, this will mean that the models are inevitably outdated. In contrast, the one-class classifier is attempting to portray only legitimate transactions; it is not being tuned explicitly to known types of fraud. Since one might expect the behavior of legitimate transactions to evolve more slowly, it is possible that the one-class approach will be superior. Although, given that neither behavioral models nor transaction-level classification is infallible strategy for detecting fraud, an obvious extension to transaction-level classification is to aggregate information over a succession of transactions, or a period of time. It is hoped that using transaction information accumulated over time will result in better fraud discrimination than one can obtain at the level of isolated transactions [27]. So, a sequence of suspicious-looking transactions provides more evidence of fraud than a single suspicious transaction. For example, we may simply count the number of transactions at a particular type of merchant, or take the sum of the value of all online transactions over the past week or day. Also, in the transition from transaction classification to account level aggregates, a lot of information is being discarded, especially concerning the order of transactions. In addition, we no longer have a transaction-level fraud / non-fraud signal. Instead, we have a label which tells us only that there is some fraud among a set of transactions, some of which are also likely to be genuine. The contribution of a single fraud transaction is watered down when aggregation is used. However, if the aggregated data records are updated continuously (with every transaction) then it is still possible to identify fraud as soon as it happens. One of the main problems of using any fraud detection algorithm or system is at what instance an alarm should be raised. Information about the status of each account is continually being updated as new transactions occur. This new information should allow better discrimination between fraudulent and non-fraudulent behavior. Thus, as information from transactions accumulates, the system should become more confident in its diagnosis of the "status" of the account. However, the insignificant value of new information may diminish as time passes. For example, aggregating 1001 transactions is not likely to be much more useful than aggregating 1000. Worse still, as time passes, an account in a fraud state (i.e. one which has been compromised and is subject to fraudulent activity) is potentially incurring costs in the form of fraudulent transactions. Clearly, it is better to raise an alarm as early as possible in order to limit these losses. On the other hand, if one raises an early alarm, using comparatively modest information, confidence is likely to be low and there will be a high false alarm rate, which also leads to higher costs and may also result in many frauds going undetected [26]. The debit card fraud detection is approached with a one class classification [26]. The idea is to monitor each account separately and using aggregation over a sequence of transactions, construct a baseline model that represents the normal aggregated behavior of an account. This model is deployed to detect and flag accounts that have "status" with the highest suspicious score. Important steps in the approach include: judicious selection of features and pre-processing of debit card transaction data; construction of the model of the legitimate aggregated behavior for each account; and the specification of the alert threshold, such that any aggregated sequence of transaction lying beyond this will be regarded as abnormal and the account 'status' as fraudulent [26].

IV. FUTURE WORK

In this paper we discussed various data mining techniques for credit card fraud detection. After the discussion of the above mentioned methods and techniques we have narrowed down to few methods like Neural Networks [24] Transaction Aggregation method [26], Artificial Immune system (AIRS) based Fraud Detection system (AFDM) [19], Bagging Ensemble Classifier technique [22], which has grabbed our attention and the future work will be on the lines of these techniques. The Model will catch the essence of the few or all these. Which will not only detect the novel fraud much faster but combined with the supervised methods like Neural Network, it will also tackle the known frauds.

REFERENCES

[1] Bhattacharyya, S., Jha, S., Kurian Tharakunnel, J. Westland, C.,Data mining for credit card fraud: A comparative study, Decision Support Systems, Vol-50, 602–613, (2011)
[2] Richard J. Bolton and David J. Hand, Peer Group Analysis – Local Anomaly Detection in Longitudinal Data.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.25.4115&rep=rep1&type=pdf , (2007)
[3] Deshpande Poonam. 'Fraud detection in Debit card transactions' presented in the International conference on Cost Benefit Analysis at Thakur college of Science and Commerce, Mumbai, India, 2015,
[4] Cardhub, 2015, http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/
[5] UK Cards Association, (2015), file:///C:/Users/Poonam%20Deshpande/Downloads/Downloads-7-2979-4084-fraud-the-facts-pageturner%20(2).pdf
[6] Aite, (2015),http://aitegroup.com/
[7] India Banking Fraud Survey Edition II April (2015), www.deloitte.com/in
[8] ACI Worldwide Card Fraud Report, http://www.aciworldwide.com/news-and-events/press-releases/online-retail-fraud-attempts-increased-by-30-in-past-year.aspx, (2015).
[9] E Commerce Fraud: Facts and Tips, DELEGO, http://www.delegosoftware.com/blog/ecommerce-fraud-facts-and-tips/ , 2015.
[10] Barnett, V. and Lewis, T. Outliers in Statistical data. Wiley, New York, (1994).
[11] Hodge V., Austin J., A Survey of Outlier Detection Methodologies. users.rsise.anu.edu.au/~kzhang/.../SurveyOutlierDetectionfulltext.pdf
[12] Kancherla R., Venkata R., Verma A., Behavioral Fraud Mitigation through Trend Offsets, Genpact India, (2008).

[13] Ghosh, S. and Reilly D. L., Credit Card Fraud Detection with a Neural-Network. Proceedings of the 27th Annual Hawaii International Conference on System Science. Volume 3: Information Systems: DSS/Knowledge-Based Systems, J. F. Nunamaker and R. H. Sprague, Eds., Los Alamitos, CA, USA, (1994).
[14] Neural Fraud Detection in Credit Card Operations Dorronsoro (1997)
[15] Brause, R. Langsdorf, T. ,Hepp, M., Neural Data Mining for Credit Card Fraud Detection, http://www-staff.cs.uni-frankfurt.de/papers/ICTAI99.pdf, (1999)
[16] Bolton R.J. and Hand D.J., Peer Group Analysis. Technical Report, Department of Mathematics, Imperial College, London, (2001).
[17] Foo Chi Hui , Chowdary, V., Norazman, M. , Safurah, H., Implementing Peer Group Analysis within a Track and Trace System to Detect Potential Fraud(s), Information Communication and Technology, MIMOS Berhad, Vol. 3, No. 1, March 2014
[18] Ekrem, D., Hamdi, O., Detecting credit card fraud by genetic algorithm and scatter search, ELESVIER Expert Systems with Applications, Vol-38, 13057-13063, (2011).
[19] Neda, S. and Mohamaad, K., A novel model for credit card fraud detection using Artificial Immune Systems, ELSEVIER Applied Soft Computing Journal, Vol. 24, 40–49, (2004)
[20] Nadar, M. and Ekrem, D., Detecting credit card fraud by Modified Fisher Discriminant Analysis, ELESVIER Expert Systems with Applications, Vol-42, 2510-2516, (2015).
[21] Bolton, R., Hand, D., Unsupervised Profiling Methods for Fraud Detection, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.5743&rep=rep1&type=pdf, (2001)
[22] Masoumeh, Z. and Pourya, S., Application of Credit card Fraud Detection Procedia Computer Science 48 679 – 685, (2015)
[23] Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T. , Akoglu, L., Snoeck, M., Baesens, B., A novel approach for automated credit card transaction fraud detection using network-based extensions, ELESVIER Decision Support System, Vol -75, 38-48, (2015).
[24] Kilo O., Review of Techniques, (2006) www.oscarkilo.net/whitepapers/DETECT-TechniquesReview.pdf
[25] Bolton, R. J. and Hand, D. J. (2002).Statistical fraud detection: A review. Statistical Science, 17(3), 235–255.
[26] Krivko M., Debit card fraud detection models. M.Sc. Thesis (University of Leicester, 2008).
[27] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D. and Adams, N. Transaction aggregation as a strategy for credit card fraud detection. Data-Mining and Knowledge Discovery. Springer Netherlands. (2008).