Banking Fraud Analysis and Decision Support System

AyeshaAzeema. Maniyar*
Department of Computer Science
KLS Gogte Institute of Technology
Belagavi, Karnataka, India

Chaitra. L. Mugali
Department of Computer Science
KLS Gogte Institute of Technology
Belagavi, Karnataka, India

Padma. Dandannavar
Department of Computer Science
KLS Gogte Institute of Technology
Belagavi, Karnataka, India

Affiliated to Visveswaraya Technological University, Belagavi

Abstract— ***Banking fraud analysis and decision support system is an effective semi-supervised approach to financial fraud and anomaly detection, using this decision support system is developed. This approach is split into two stages of development including the training phase and the runtime. During the training phase, it creates a profile for each user on the basis of its prior transactions. The training phase takes as input a series of transactions. It differentiates each user using a local, global and temporal profile. Local profiling aims at generating histograms by considering the list of transactions performed by each user. The global profiling aims at forming clusters for each user based on its prior transactions with correlated spending patterns. Temporal profiling is based on the prior transactions and it calculates the anomaly score for each user transaction. During runtime, it sorts the unlooked transactions that differ from the learned profiles. Moreover, it helps the analyst with a reason for analyzing the outcomes by aiding in his/her decision making activities.***

Keywords— ***Banking, Fraud, Bank Fraud, Fraud Detection, Anomaly Detection.***

I. Introduction

With the development of varied communication techniques, online payment transactions as well as e-commerce is spreading day by day. Moreover, the financial frauds associated with these transactions are also increasing which subsequently results in substantial financial losses every year globally. Credit card fraud is practiced most frequently amongst the varied financial frauds due to its acceptance and widespread usage as it offers more convenience to its users. Financial institutions such as banks require more sophisticated techniques for detecting fraud. Financial frauds are often very hard to detect and analyze as the fraudulent behavior is changing, dispersed in distinct user profiles, and spread across huge imbalanced real world datasets (e.g. customer spending profiles, web logs, transaction logs). Furthermore, customers rarely review their online banking history and hence are not able to disclose the fraudulent transactions at the right time. Accordingly, due to the wide usage of credit cards as a mode of payment for procuring goods and services, there comes a need to determine whether the transactions made through the use of a credit card is a valid transaction done by card holder or it is a fraudulent transaction done by the fraudster. In traditional approaches, it can be figured out whether the transaction carried out is a valid transaction or a fraudulent transaction once the billing has been done. This leads to substantial financial losses. Thus, it is necessary to determine the fraudulent transactions prior to performing the billing actions.

Although fraud detection has a very long history, not much research has happened in this area. The cause is that the real world data is very hard to obtain since the financial institutions are not ready to disclose their sensitive customer transaction data due to the privacy restrictions implied by most of the financial institutions which also restricts the researchers to perform the experiments and get the outcomes. Moreover, the authorities of the financial institutions change the field names so that the researchers don’t get to know about the actual fields. Due to these confidential aspects of the real world dataset, fraud detection models have not been developed and described in the academic literature and very fewer models are implemented in the actual detection systems. Still there exist some of the successful applications that use different data mining techniques including self organized maps, neural networks, artificial immune system, hidden markov models, fuzzy logic systems, conditional weighted transaction aggregation, frequent itemset mining, cryptographic algorithms, and outlier detection techniques in fraud detection.

II. ORGANIZATION OF THE PAPER

This paper presents the techniques available for credit card fraud detection. Section III discusses about the related work carried throughout by various researchers. Section IV introduces the proposed methodology for the detection of credit card fraud. Section V discusses about the outcomes of the system. Section VI closes out with the recommendations for future research.

III. RELATED WORK

Fraud detection techniques containing transaction data are mainly split under two categories. The first category involves methods for identifying outliers in transaction data. These methods generally make use of clustering algorithms to aggregate transactions and recognize outlier transactions from the noted clusters. Predefined rules are commonly applied to arrange the transactions as either being fraudulent or legitimate.

The second category of techniques classifies individual transactions using models skilled by classifiers for instance artificial neural networks and support vector machines. This section presents few of these techniques that are applicable to credit card fraud detection [1].

A. Conditional Weighted Transaction Aggregation

Wee-Young Lim et al. [1], have proposed a conditional weighted transaction aggregation method which takes the advantage of supervised machine learning techniques to figure out the fraudulent credit card transactions. This work aids in presenting an enhanced aggregation based method that involves the generation of weights for all the previous transactions in an aggregated period. It also demonstrates that aggregation based approaches perform better than transaction based methods. This is due to the ability of aggregation based methods to include additional information from the preceding transactions. The major improvement of this work is an enhanced aggregation based method that adds weights for all the prior transactions in an aggregated period. The experimental results demonstrate that the time gap weighting strengthens the importance of recent transactions over the older transactions, thereby enhancing credit card fraud detection.

It addresses the drawbacks of the transaction aggregation strategy described by Whitrow et al. [2] by applying aggregation strategy in a weighted manner. In particular, this method manipulates the weight of a preceding transaction based on its distance from the current transaction. The conditional weighted transaction aggregation approach illustrated in this paper treats this issue by considering the advantage of supervised machine learning techniques to capture fraudulent transactions. Whitrow et al. [2] have proposed a transaction aggregation strategy that only aggregates transactions of the previous few days to boost fraud detection performance. However, the major drawback is that it treats all the earlier transactions as equal, avoiding the continuous nature of the credit card transactions.

B. Self Organized Maps

Mitali Bansal and Suman [3], have proposed a real time credit card fraud detection model and conferred a new and innovative approach to detect the credit card fraud by applying Self Organized Maps (SOM). SOM offers better outcomes in case of identifying credit card fraud. This approach uses the normalization and clustering mechanism of SOM for the detection of credit card fraud. This aids in discovering hidden patterns from the transactions which cannot be identified using the various traditional approaches. SOM helps in determining anomalies in varied credit card fraud cases and the concept of normalization aids in normalizing the values present in other fraud cases. This work is based on an unsupervised approach which helps the financial institutions to handle frauds and also assists to abstain the occurrence of fraud as early as possible. Clustering assists to detect anomalous data by forming clusters leading towards the differentiation of legitimate and fraudulent transactions. This work also employs a multilayered approach which performs well in the identification of credit card fraud.

Dominik Olszewski et al. [4], have proposed a fraud detection approach based on the user accounts visualization and classification threshold-type detection. This approach uses Self-Organizing Map (SOM) as the visualization technique. Since the original form of SOM technique visualizes only the vectors, the user accounts correspond to the matrices storing a group of records returning the continuous activities of a user. The major contribution of this work is the matrices visualization applied on the SOM grid. Furthermore, they have also proposed an approach of the classification threshold setting on the basis of the SOM Umatrix. The performance evaluation was carried out on a real world data set in the telecommunications fraud algorithms for credit scoring in credit card transactions. It is observed that Naive Bayes classifier achieves the best accuracy detection field which presents the advantages and effectiveness of the proposed approach.

C. Frequent Itemset Mining

K. R. Seeja and Masoumeh Zareapoor [5], have implemented an intelligent model based on credit card fraud detection for discovering frauds occurring in a highly unbalanced and anonymized credit card transaction datasets. This work is based on frequent itemset mining which handles the class imbalance problem by considering legitimate as well as fraudulent patterns for each user. A matching algorithm is also proposed to identify to which pattern (legal or fraud) the current transaction of a particular user belongs to and a decision is taken accordingly. Here, each attribute is given equal preference to find the patterns. This approach maintains two separate pattern databases for both legal user and fraudulent behaviors. It periodically updates both the databases to reflect to the behavioral changes that occur over time. Performance evaluation has been carried out on an anonymized dataset and it is noticed that the proposed model has a very high fraud detection rate and very less false alarm rate. This approach performs well independent of the attribute values and it also has the ability to look over class imbalance problems.

D. Data Mining Techniques

John Akhilomen [6], presents an application based on data mining that has been designed as a subsystem and can be applicable to most of the financial institutions to detect credit card fraud. This application accepts input formatted on a particular pattern and testes it with the credit card holder’s pattern and then it classifies a real time transaction as either being a legitimate, suspicious or an illegitimate transaction.

This approach makes use of an “anomaly detection algorithm” based on “neural networks” to discover fraud in the transactions happening in real time and it does not introduces any flaws due to its trained classifier which assigns each real time transaction as either being a legitimate, suspicious or a fraudulent transaction.

R. Roselin and C. Hanupriya [7], have proposed a customer behavior analysis system for credit card proposer’s and a comparative analysis has been performed between the classification and clustering algorithms. Several classification algorithms including Naive Bayes, Jripper, ID3 and J48 are applied on the credit card dataset. The clustering techniques such as simple k-means and FarthestFirst have been compared. A comparative study has been achieved between the classification and clustering algorithms using classification accuracy. Amongst the four classification algorithms J48 has proven to have good accuracy of 96% when compared to other algorithms. Accordingly, clustering algorithms concluded that FarthestFirst produces 78% of accuracy whereas simple kmeans gives an accuracy of 77%.

Evaristus Didik Madyatmadja and Mediana Aryuni [8], have proposed a data mining model which employs classification methods such as Naive Bayes and ID3 of 82% above ID3 which has an accuracy of 76%. Addition to this, the proposed data mining model aids in improving the performance and guides the analyst’s job.

E. Hidden Markov Model

Bilonikar Priya et al. [9], have implemented Hidden Markov Model (HMM) in the domain of credit card fraud detection. This work uses a HMM to model the sequence of real time transactions in a credit card fraud detection system. Further, they have incorporated a RFID device to display the transactions occurring over time. It observes the behavior of the customers by presenting a high security questions page. In case the credit card is stolen, it provides the user with a fresh new account including its username and password. For security reasons, it provides the user with a onetime password along with the facility to block the credit card as soon as the user realizes that the credit card is lost. It also makes sure that it does not rejects the genuine transactions by making use of the onetime password generated by the server and sent to the personal communication address of the customer (mobile phone).

Ashphak P. Khan et al. [10], have applied HMM in credit card fraud detection. This proposed approach divides the transaction amount into three major groups including high, medium, and low transaction amounts. Each group requires different ranges of transaction amount and is shown using aberration symbols. The stochastic process of a HMM is used to represent the varied steps in a credit card transaction processing system. Further, a method has been suggested to identify the spending habits of each of the customer. This approach is scalable for managing large volumes of transactional data.

F. Multiple Cryptographic Algorithms

Ms. Pratiksha L. Meshram and Prof. Tarun Yenganti [11], have proposed a system that aims at finding the specific user for real time transactions. In case of credit and ATM cards, for determining the original identity of a user it uses the user’s security pin number as well as it asks for the secret question. To provide multiple layers of security for covering the pin number, DES, 3-DES algorithms are used to implement the cryptographic algorithm. Additionally, any remote user can submit a file from any source to destination by providing the proper path and can save a copy at its own destination. This transferring process is fully secured as cryptographic algorithms have been applied.

G. *Outlier Detection Techniques*

Ms. Amruta D. Pawar et al. [12], have proposed an outlier detection technique that is applicable on credit card fraud detection and is suitable for online applications where large volumes of data are generated. This approach also works conveniently for applications where there is a constraint on memory and computation efforts. Accordingly, one such unsupervised technique known as the “Principal Component Analysis (PCA)” have been used to detect an outlier. “Principal Component Analysis (PCA)” is an unsupervised method used for dimension reduction. The major aim of this work is to look over the credit card fraud detection system using a novel outlier detection system. Performance evaluation has been carried out considering 20 attributes which will be further reduced after applying PCA. After obtaining the reduced attribute set, PCA technique will subsequently detect frauds with less memory and computation requirements. It is possible to identify only the attributes of interest which contain major information. In case, if there exists a fraudulent transaction then this particular transaction will be dumped into a database. This aids in the fraud detection to perform faster.

Michele Carminati et al. [13], have proposed a semi-supervised banking fraud analysis and decision support system. This approach is split into two stages of development including the training phase and the runtime. During the training phase, it creates a profile for each user on the basis of its prior transactions. The training phase takes as input a series of transactions. It differentiates each user by using a local, global and a temporal profile. Local profiling illustrates foregoing user behavior to measure the anomaly of each new transaction by using “a novel algorithm that uses the Histogram Based Outlier Score (HBOS)”. The global profiling clusters users based on their transaction features by means of “an iterative version of Density-Based Spatial Clustering of Applications with Noise (DBSCAN)”. For this, it uses “Cluster-Based Local Outlier Factor (CBLOF)”. Whereas, temporal profiling is based on the prior transactions and it calculates the anomaly score at runtime by employing thresholds.

According to the model built, each profile generates varied statistical features from the transaction attributes. At runtime, it sorts the unlooked transactions that differ from the learned profiles. In this approach, first each transaction's anomaly with respect to the user's profile history is measured. Then, it finds the global clusters of the user's with correlated spending patterns. It uses a temporal threshold system that quantifies the anomaly of the current spending pattern of each user with respect to his/her prior spending patterns. It aids in analyzing the frauds and anomalies by performing the analysis of bank transfer logs. This approach gives the analyst's a ranked series of abnormal transactions along with each user's anomaly score. The anomaly score measures the possibility of a transaction as a fraud with respect to the profiles learned. Accordingly, a general framework for semisupervised outlier detection is developed. It employs a mixture of distinct models to discover frauds of different types. In this approach, the major aim is gathering and correctly establishing information that helps to analyze the abnormal behavior. This approach was deployed on a real world data from a leading Italian bank to analyze frauds and it produced good results by discovering about 98% detection rate. Hence, it can be deployed in any real time banking environment.

IV. APPROACH

This work aims at developing an effective fraud analysis and automatic decision support system for banking frauds. The scores calculated have a clear statistical meaning, aiding the analyst's activity. The goal is to support the analysis of (novel) frauds and anomalies by analyzing bank transfer logs. It provides the analysts with a ranked list of fraudulent transactions, along with the anomaly score of each user sorted in decreasing order. Top-ranked transactions have higher priority. Therefore, the focus is on collecting and correctly ranking evidence that support the analysis of fraudulent behavior, rather than just flagging transactions.

Figure below illustrates the general architecture of the system.

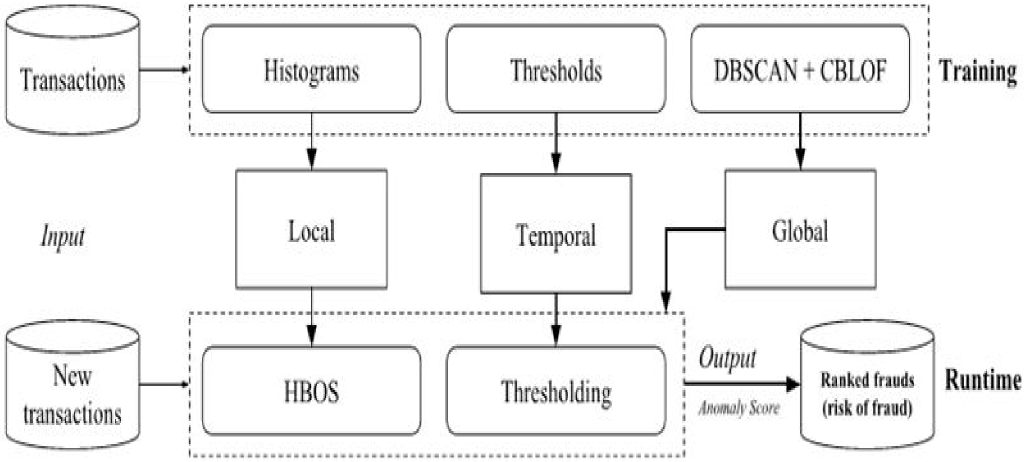


Fig. 1: General architecture of the system.

A. *Algorithmic Steps*

The algorithmic steps illustrating the overall execution process of the system are described below.

- Step 1: Initially, a series of n transactions is fed into the training phase as a trained dataset.
- Step 2: Process the transactions by determining different attributes of interest.
- Step 3: Split the amount of each transaction into k different ranges.
- Step 4: Count the number of transactions falling into each range.
- Step 5: Further, this is used to generate a user details file illustrating the account number from which the transaction is made, the total number of transactions done by each account holder, and the average amount of all the transactions made.
- Step 6: Form clusters of each user on the basis of its prior transactions.
- Step 7: It groups the users by considering the transactions made by each user based on the account number from which the transaction has taken place, the IP address of the account holder, the country from which the transaction is made, the account number to which the transaction is made and the country of the recipient's account holder.
- Step 8: Calculate the anomaly score for each user as well as the anomaly score for each of the transaction made by each user.
- Step 9: Sort the anomaly scores in decreasing order.
- Step 10: The anomaly score with the highest value is considered as being abnormal and should be suspected by the analyst.

B. *Dataset Description*

The Table 1 below provides the description of the list of the attributes for each type of transaction.

Table 1. List of attributes for each transaction.

Dataset Name	Attribute Name	Description
Bank_Transfers	Amount	Non-categorical
	Account_Number	Categorical
	CC_ASN	Categorical
	Account_Number_Recipient	Categorical
	Country_Recipient	Categorical
	IP_Address	Categorical
	Time_Stamp	Categorical

Table 1 illustrates the description of the attributes for each type of the transaction maintained in the trained dataset. The attributes include the following,

- Amount: the amount for each of the transaction.
- Account_Number: the account number of the user carrying out the transaction.
- CC_ASN: the country code i.e. the location of the user carrying out the transaction.
- Account_Number_Recipient: the account number of the recipient.
- Country_Recipient: the country i.e. the location of the recipient.
- IP_Address: the IP address of the machine through which the transaction has taken place.
- Time_Stamp: the time stamp duration of the transaction.

C. *Description*

This approach is split into two stages of development including the training phase and the runtime. During the training phase, it creates a profile for each user on the basis of its prior transactions. The training phase takes as input a series of transactions. It differentiates each user by using a local, global and temporal profile.

1) *Local profile:*

Local profiling illustrates foregoing user behaviour to measure the anomaly of each new transaction by using "a novel algorithm that uses the Histogram Based Outlier Score (HBOS)". Local profiling aims at generating histograms by considering the list of transactions performed by each user. It divides the amount for each transaction into separate ranges and provides a count of all the transactions falling into each range. This is used to generate a user details file illustrating the account number from which the transaction is made, the total number of transactions done by each account holder, and the average amount of all the transactions made. Local profiling thus highlights the individuals spending patterns by aggregating the transactions performed by each user.

2) *Global profile:*

The global profiling clusters users based on their transaction features by means of "an iterative version of Density-Based Spatial Clustering of Applications with Noise (DBSCAN)". For this, it uses "Cluster-Based Local Outlier Factor (CBLOF)". Global profiling aims at forming clusters for each user based on its prior transactions. It groups the users by considering the transactions made by each user based on the account number from which the transaction has taken place, the IP address of the account holder, the country from which the transaction is made, the account number to which the transaction is made and the country of the recipient's account holder.

3) *Temporal profile:*

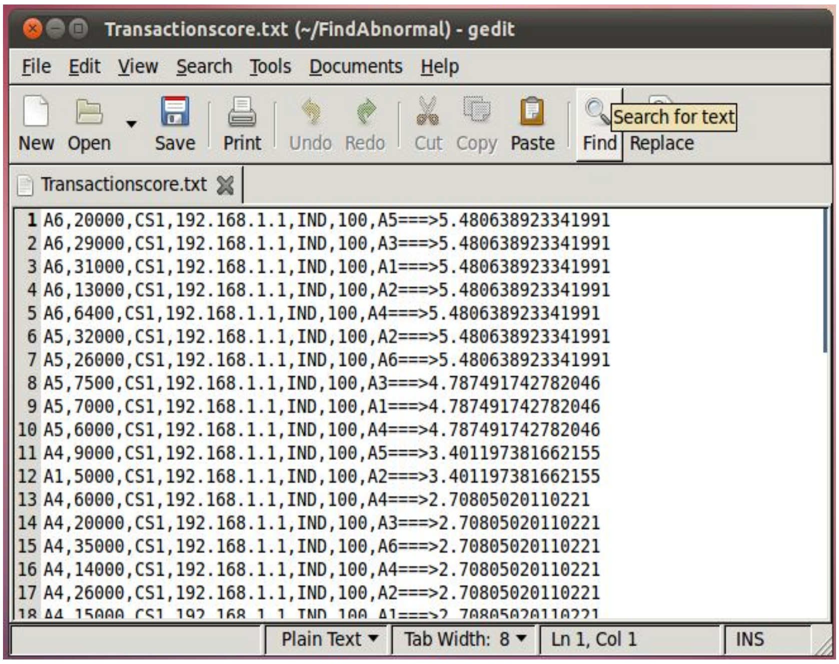
Temporal profiling is based on the prior transactions and it calculates the anomaly score at runtime by employing thresholds. According to the model built, each profile generates varied statistical features from the transaction attributes. Temporal profiling calculates the anomaly score for each user as well as the anomaly score for each of the transaction made by each user. It sorts the anomaly scores in decreasing order. And the anomaly score with the highest value is considered as being abnormal and must be suspected by the analyst.

At runtime, it sorts the unlooked transactions that differ from the learned profiles. In this approach, first each transaction's anomaly with respect to the user's profile history is measured. Then, it finds the global clusters of the user's with correlated spending patterns. It uses a temporal threshold system that quantifies the anomaly of the current spending pattern of each user with respect to his/her prior spending patterns. It aids in analyzing the frauds and anomalies by performing the analysis of bank transfer logs. This approach gives the analyst's a ranked series of abnormal transactions along with each user's anomaly score. The anomaly score measures the possibility of a transaction as a fraud with respect to the profiles learned. Accordingly, a general framework for semisupervised outlier detection is developed. It employs a mixture of distinct models to discover frauds of different types. In this approach, the major aim is gathering and correctly establishing information that helps to analyze the abnormal behavior.

V. RESULTS AND DISCUSSIONS

The goal is to measure the effectiveness of this system in correctly identifying the transactions that are fraudulent and are not seen before in its prior transactions. The trained dataset used consists of bank transfers, i.e. the money transfers that are carried out by an account belonging to a bank to any another account. The evaluation of this system is quite complex because, this system requires more complicated datasets that are usually very hard to obtain due to the privacy restrictions implied by the financial institutions. This work aims at developing an effective fraud analysis and automatic decision support system for banking frauds. The scores calculated have a clear statistical meaning, aiding the analyst's activity. The goal is to support the analysis of (novel) frauds and anomalies by analyzing bank transfer logs. It provides the analysts with a ranked list of fraudulent transactions, along with the anomaly score of each user sorted in decreasing order. Top-ranked transactions have higher priority. Therefore, the focus is on collecting and correctly ranking evidence that support the analysis of fraudulent behavior, rather than just flagging transactions.

Figure below illustrates the anomaly score for each type of transaction.



```
A6,20000,CS1,192.168.1.1,IND,100,A5===>5.480638923341991
A6,29000,CS1,192.168.1.1,IND,100,A3===>5.480638923341991
A6,31000,CS1,192.168.1.1,IND,100,A1===>5.480638923341991
A6,13000,CS1,192.168.1.1,IND,100,A2===>5.480638923341991
A6,6400,CS1,192.168.1.1,IND,100,A4===>5.480638923341991
A5,32000,CS1,192.168.1.1,IND,100,A2===>5.480638923341991
A5,26000,CS1,192.168.1.1,IND,100,A6===>5.480638923341991
A5,7500,CS1,192.168.1.1,IND,100,A3===>4.787491742782046
A5,7000,CS1,192.168.1.1,IND,100,A1===>4.787491742782046
A5,6000,CS1,192.168.1.1,IND,100,A4===>4.787491742782046
A4,9000,CS1,192.168.1.1,IND,100,A5===>3.401197381662155
A1,5000,CS1,192.168.1.1,IND,100,A2===>3.401197381662155
A4,6000,CS1,192.168.1.1,IND,100,A4===>2.70805020110221
A4,20000,CS1,192.168.1.1,IND,100,A3===>2.70805020110221
A4,35000,CS1,192.168.1.1,IND,100,A6===>2.70805020110221
A4,14000,CS1,192.168.1.1,IND,100,A4===>2.70805020110221
A4,26000,CS1,192.168.1.1,IND,100,A2===>2.70805020110221
A4,15000,CS1,192.168.1.1,IND,100,A1===>2.70805020110221
```

Fig. 2: Transaction score for each transaction of the user.

Fig. 2 shows the transaction score file generated on the basis of each transaction carried out by the user. It illustrates the account number through which the transaction has taken place, the amount of the transaction, the country code, the IP address of the machine, the time stamp, the recipient's account number and the anomaly score for generated for each of the transaction carried out by the user.

Most of the work that focuses on overcoming the limitations of this system requires more complicated datasets that are usually very hard to obtain due to the privacy restrictions implied by the financial institutions. Since the financial institutions are not ready to disclose their sensitive customer transaction data it is very difficult to work on the real world data. A major improvement of this system could be realized by providing support to analyze frauds and anomalies by analyzing transactions happening through prepaid cards and phone recharges. A temporary work is to provide provisions to examine the observations made by the analyst which requires detailed analysis on the detected anomalies.

VI. CONCLUSION

At present, building a well defined, manageable and well understood financial fraud monitoring system is the essential requirement of most of the financial institutions. Banking fraud analysis and decision support system is an effective semi-supervised approach to financial fraud detection and anomaly detection, using this decision support system is developed. Even with the typical privacy restrictions of the financial institutions it is feasible to achieve a decision support system that aids in supporting the analyst's to look over the possible reasons for the occurrence of fraud. Moreover, it helps the analyst with a reason for analyzing the outcomes making manual check much easier. Consequently, the target is on identifying the information correctly that aid in supporting the analysis of abnormal transactions.

REFERENCES

[1] Wee-Yong Lim, Amit Sachan, and Vrizlynn Thing, "Conditional weighted transaction aggregation for credit card fraud detection," G. Peterson and S. Shenoi (Eds.): Advances in Digital Forensics X, IFIP AICT 433, pp. 3–16, 2014, IFIP International Federation for Information Processing 2014.

[2] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston and N. M. Adams," Transaction aggregation as a strategy for credit card fraud detection," Springer Science+Business Media, LLC 2008.

[3] Mitali Bansal and Suman, "Credit card fraud detection using self organised map," International Journal of Information & Computation Technology, ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1343-1348.

[4] Dominik Olszewski, Janusz Kacprzyk, and Slawomir Zadrozny, "Employing self-organizing map for fraud detection," L. Rutkowski et al. (Eds.): ICAISC 2013, Part I, LNAI 7894, pp. 150–161, 2013, Springer-Verlag Berlin Heidelberg 2013.

[5] K. R. Seeja and Masoumeh Zareapoor, "FraudMiner: A novel credit card fraud detection model based on frequent itemset mining," Published 11 September 2014, The Scientific World Journal.

[6] John Akhilomen, "Data mining application for cyber credit-card fraud detection system," Proceedings of the World Congress on Engineering 2013 Vol III, WCE 2013, July 3 - 5, 2013, London, U.K.

[7] R. Roselin and C. Hanupriya, "Customer behaviour analysis for credit card proposers based on data mining techniques," International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 11 (November 2014).

[8] Evaristus Didik Matyatmadja and Mediana Aryuni, "Comparative study of data mining model for credit card application scoring in bank," Journal of Theoretical and Applied Information Technology, 20th January 2014. Vol. 59 No.2 ISSN: 1992-8645 E-ISSN: 1817-3195.

[9] Bilonikar Priya, Deokar Malvika, Puranik Shweta, Sonwane Nivedita and Prof.B.G.Dhake, "Survey on credit card fraud detection using hidden markov model," International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940 Vol. 3, Issue 5, May 2014.

[10] Ashphak P. Khan, Vinod S. Mahajan, Shehzad H. Shaikh and Akash B. Koli," Credit card fraud detection system through observation probability using hidden markov model," International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (7-16), Month: October-December 2013.

[11] Ms. Pratiksha L. Meshram and Prof. Tarun Yenganti," Credit and ATM card fraud prevention using multiple cryptographic algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013 ISSN: 2277 128X.

[12] Ms. Amruta D. Pawar, Prof. Prakash N. Kalavadekar and Ms. Swapnali N. Tambe, "A Survey on Outlier Detection Techniques for Credit Card Fraud Detection," IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VI (Mar-Apr. 2014).

[13] Michele Carminati, Roberto Caron, Federico Maggi, Ilenia Epifani and Stefano Zanero, "BankSealer: An online banking fraud analysis and decision support system," International Federation for Information Processing (IFIP), N. Cuppens-Boulahia et al. (Eds.): SEC 2014, IFIP AICT 428, pp. 380-394, 2014.