Outlier Detection
In Financial Transactions: A Review

Ayesha Azeema Maniyar and Padma Dandannavar

MTech Computer Engineering Student, Dept. of CSE, KLS Gogte Institute of Technology, Belagavi, Karnataka, India
Assistant Professor, Dept. of CSE, KLS Gogte Institute of Technology, Belagavi, Karnataka, India
Affiliated to Visveswaraya Technological University, Belagavi

Abstract- Outlier detection is considered as one of the most renowned methodologies that aid in establishing data objects that do not act in accordance with the overall conduct or the model of the data. Outlier detection is an essential point at issue that has been investigated within varied research disciplines and application domains. The key to outlier detection methods is observed in the fact that the outcomes can head towards the discovery of litigable (often critical) information. A general example for this can be fraud detection, where an outlier can witness, e.g., an unusual usage of a credit card that needs to be investigated. Thus, the disclosure of credit card fraud is obligatory. This paper addresses the general overview of outliers and subsequently it introduces the survey of the distinct techniques available for credit card fraud detection.

Keywords- Outlier, Outlier Detection, Fraud, Credit Card, Credit Card Fraud, Credit Card Fraud Detection.

I. INTRODUCTION

Data mining is the criterion towards interpreting huge amounts of data and viewing the appropriate information. Outlier detection is one among the data mining methodologies that aids in observing uncommon events, distinct objects and exceptions. These observations can inordinately disturb the outcomes of data analysis. In consequence with this regard it is excessively necessary to address this issue before inducing any data mining task. Outlier detection is sometimes mentioned as anomaly detection, novelty detection, noise detection, deviation detection or exception mining. Outlier detection is widespread and has gone into the perspective of a wide range of application domains. Outlier detection is applicative in an extensive listing of application disciplines enclosing the following [1],

- Fraud Detection: Outlier detection aims at detecting the unauthorized usage of a credit card or any fraudulent transaction for a credit card.
- Mobile Phone Fraud Detection: Monitors mobile phone activities to detect when an account appears to be misused.
- Insurance Claim Fraud Detection: Recognizes claims fraud, e.g. automobile insurance fraud.
- Intrusion detection: Outlier detection is applied to identify the break-ins that exist in a computer system.
- Insider Trading Detection: Detects frauds happening in stock markets where common people conceive heavy profits by disclosing the inside information.
- Medical and Public Health Outlier Detection: Finds out anomalous records of patients often occurring due to instrumentation or data recording errors.
- Industrial Damage Detection: Detects and prevents the normal wear and tear of the industrial units due to continuous usage from further escalation and damage.
- Image Processing: Detects transitions in an image over time and also helps to detect anomalous regions in an image.
- Outlier Detection in Text Data: Detects novel topics or events or news stories in a series of documents or news articles. Helps to rectify the variations in documents belonging to one category or topic.
- Sensor Networks: Identification of one or more faulty sensors.
- Other Domains: Outlier detection is also applicable in novelty detection in robot behavior, click through protection, detecting faults in web applications, detecting associations among criminal activities, detecting outliers in census data, speech recognition, traffic monitoring, detecting outliers in biological data.

Having aforesaid of the valuable insights of outlier detection, it is observed that outliers exist virtually in every real world dataset and the disclosure of outliers is elementary which aids in bettering the quality of the data and subsequently maintaining the aftereffect of data analysis.

II. ORGANIZATION OF THE PAPER

This paper presents a generic outline of outlier detection and consequently introduces the techniques available for credit card fraud detection. Section III presents the description of the terminologies correlated to outlier and credit card fraud detection. Section IV discusses about the related work carried all through. Section V looks at the addressed issues and presents a view of the strengths and limitations of the reviewed
approaches. Section VI closes out with the recommendations for future research.

III. BACKGROUND

A. Outlier:

Very often, we examine that there exists data objects that do not act in accordance with the overall conduct or the model of the data. Such alike data objects, which are diverging totally from or incomparable with the leftover set of data, are often designated as outliers. A general example for an outlier could be your credit card transactions. Wherein, the purchasing behavior of a credit card owner usually differs when the card is snatched. Outliers are often referred to as anomalies, novelties, noise, deviations, abnormalities, discordants and exceptions. Outliers are dissimilar when correlated to the noise data. Although these terms seem to look similar they are actually very distinct. In respect to this, noise is considered as any undesirable or unwanted signal or sometimes a part of a signal. Whereas, an outlier is a data point or value that is distinct from all or most of the data in the dataset.

Necessity for the isolation of outliers:

Recognition of potential outliers is crucial for the following reasons,

- Outliers are values that signify bad data. For example, the data may not be organized accurately or an experiment may have been run incorrectly. If it can be examined that the outlying point is veritably askew, then the outlying value should be eliminated or reformed (winsorized) if possible from the analysis.

- In few cases, it may be undesirable to examine if an outlying point is bad data. As such, detain the outlier and treat it like any other data point.

An example representing the outlying values:

Fig. 1 depicts the outliers in a one-dimensional data set. Fig. 2 illustrates the outliers plotted along a 2-dimensional dataset. With reference to Fig. 1, we observe that the data objects are plotted along a one-dimensional data set. Wherein, the data point at the right signifies an outlier that is considerably located at a distinct position from the rest of the data points.

In the next Fig. 2, we notice that the data objects are plotted along a 2-dimensional data set. Wherein, N1 and N2 are regions of normal behavior. And the point’s o1 and o2 that are seen to be consistently varying from the regions N1 and N2 are considered to be outliers. Whereas, the region O3 even though it consists of a few data points it is considered to be an outlier.

Reasons for the commencement of outliers:

Fig. 3 illustrates the major reasons for the commencement of outliers.
Outliers are said to be persuaded in the data for a collection of reasons. Of course the possibility is that the outliers induce errors [2]. There exist a few causes for the occurrence of an outlier including:

- **Measurement Error**: A measurement error is expected to take place due to the following inductions,
  - There may be a defect in the instrument used for recording data.
  - An explanation based on the misconception of a question asked or a poorly worded question.
  - Or an unclear answer misinterpreted by the interviewer.

- **Clerical Error**: An error that results when the data is translated or duplicated either manually or by a computer system and a fault in the translation takes place.

- **Sampling Frame Error**: One more kind of error is a sampling error: wherein a unit that actually does not exist in the target population is somehow included in the sample.

- **Change in the environment**: This includes variance such as a weather variation, or an unusual spending pattern among the consumers.

Accordingly, outliers are candidates for abnormal data that may consequently disturb the systems adversely such as by generating erroneous outcomes, misspecification of models, and partial estimation of parameters. For this reason, it is therefore necessary to determine the outlying values foregoing to modeling and analysis.

**B. Credit Card Fraud Detection:**

With the advent of credit cards and debit cards as widely accepted modes of payments, the occurrence of credit card frauds in e-commerce has become a primary issue for all the credit card issuer’s i.e. financial institutions such as banks and its card holders. Periodic usage of credit cards for procuring goods and services is usually accomplished through the use of either a physical card for offline transactions or a virtual card for online transactions. In a physical mode of payment, credit cards are instilled into a payment machine at a merchant shop for purchasing goods. The only means for a fraudster to gain access to a physical card is by stealing the physical card. Determining fraudulent transactions in this mode of payment is way out as the credit card is already stolen by the fraudster. The credit card holder exhibits a financial loss if he/she is unable to realize the loss of the credit card. In online payment mode, fraudsters make use of hardly any information involving card number, secure code, expiration date etc. With the attainment of this knowledge, fraudsters can easily obtain access to a card holder’s account and commit fraudulent transactions.

Accordingly, credit card fraud results into heavy losses to credit card companies as well as its consumers. With the popularity of credit card theft, it is necessary to implement well refined and strong fraud detection techniques so as to discover the implied differences between any fraudulent and legitimate transactions. In respect to this, the analysis and early detection of illegitimate transactions has become a widely researched area in various research disciplines, particularly in the case of e-commerce.

Credit card fraud detection techniques generally function at the account level and/or transaction level. Transaction-level fraud detection systems allocate each individual transaction based on certain characteristics such as the amount of transaction and the mode of payment. A transaction-level model is bounded as it does not take into consideration the previous transactions that could assist to identify fraudulent activities. Account-level fraud detection systems illustrate the normal behavior of consumers; a fraudulent activity is noticed when there is a strong deviation from normal behavior of the consumers. A general example is a huge online transaction from an account that was unexpected to happen. The account-level model considers the previous transactions of consumers, but it is restricted by the inapplicability of generating a global model covering all the consumers [3].

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.

IV. 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 trained 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 [3].

A. Conditional Weighted Transaction Aggregation

Wee-Young Lim et al. [3], 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. [4] 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. [4] 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 [5], 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. [6], 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 [7], 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 customer. A matching algorithm is also proposed to identify to which pattern (legal or fraud) the current transaction of a particular customer 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 customer and fraudulent behaviors. It periodically updates both the databases to reflect 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 [8], presents a data mining application that has been modeled as a subsystem which can be applicable to most of the financial institutions to detect credit card fraud. This application accepts input formatted on a particular pattern and matches 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 real time transactions 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.

E. Hidden Markov Model

Bilonikar Priya et al. [11], 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. [12], 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

R. Roselin and C. Hanupriya [9], 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 k-means gives an accuracy of 77%.

Evaristus Didik Madyatmadja and Mediana Aryuni [10], 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.

Ms. Pratiksha L. Meshram and Prof. Tarun Yenganti [13], 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. [14], 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. [15], have proposed a semi-supervised online 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 customer based on its prior transactions. The training phase takes as input a series of transactions. It differentiates each user by means of a local, global and 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 employs thresholds during runtime to calculate the anomaly score. According to the model built, each profile generates varied statistical features from the transaction attributes. During runtime, it sorts the unlooked transactions that differ from the learned profiles. In this approach, first the anomaly of each transaction with respect to the customer historical profile is measured. Then, it finds the global clusters of customers with correlated spending patterns. It uses a temporal threshold system that quantifies the anomaly of current spending pattern of each customer with respect to his/her prior spending behavior. It aids in the analysis of frauds and anomalies by analyzing bank transfer logs, prepaid cards and phone recharges. This approach provides the analysts with a ranked series of fraudulent transactions along with the anomaly score of each user. The anomaly score measures the statistical likelihood of a transaction being a fraud with respect to the learned profiles. Accordingly, a general framework for online semi-supervised outlier detection is developed. It employs a combination of different models to discover different types of frauds. In this approach, the focus is on collecting and correctly establishing information that support the analysis of fraudulent behavior, rather than just flagging transactions. 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.

V. OBSERVATIONS

This section introduces all the approaches that are applicable to credit card fraud detection that are reviewed in the foregoing work carried throughout. It provides a summary of all the varied techniques applied to credit card fraud detection along with their strengths and limitations.

Table I. A summary of the techniques applied to credit card fraud detection.

<table>
<thead>
<tr>
<th>Citations Used</th>
<th>Name of the Paper</th>
<th>Techniques Applied</th>
<th>Strengths</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>[3]</td>
<td>Conditional Weighted Transaction Aggregation for Credit Card Fraud Detection</td>
<td>Conditional weighted transaction aggregation</td>
<td>Provides an enhancement to the transaction aggregation method by applying aggregation strategy in a weighted manner. It involves the generation of weights for all the previous transactions in an aggregated period. It provides a major improvement to the existing transaction aggregation approach by considering all the preceding transactions. Thereby, resulting into an enhanced credit card fraud detection system.</td>
<td>Weights generated based on the continuous sequence of preceding transactions should be taken care of.</td>
</tr>
<tr>
<td>[4]</td>
<td>Transaction aggregation as a strategy for credit card fraud detection</td>
<td>Transaction aggregation</td>
<td>Implements a transaction aggregation strategy that aggregates transactions of the previous few days to boost fraud detection performance.</td>
<td>Manipulates the weight of a preceding transaction based on its distance from the current transaction. However, the major drawback is that it treats all the earlier transactions as equal, avoiding the continuous nature.</td>
</tr>
<tr>
<td></td>
<td>Title</td>
<td>Description</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Credit Card Fraud Detection Using Self Organised Map</td>
<td>Self Organized Maps (SOM) Normalization and clustering mechanisms of SOM</td>
<td>Aids in discovering hidden patterns from the transactions which cannot be identified using the various traditional approaches. Helps the financial institutions to handle frauds and also assists to abstain the occurrence of fraud as early as possible. Normalizing the values present in other fraud cases sometimes tend to be very ineffective.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Employing Self-Organizing Map for Fraud Detection</td>
<td>User accounts visualization and classification threshold-type detection based on (Self Organized Maps) SOM Grid and U-matrix</td>
<td>Enhances the original form of SOM which visualizes only the vectors. Assists in returning the continuous activities of each user. Does not perform the separation of fraudulent or non-fraudulent accounts which if included would offer much better fraud detection results.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining</td>
<td>Frequent Itemset Mining</td>
<td>Works independent of the attribute values and each attribute is given equal preference to identify the patterns. Assists in handling the class imbalance problem. Periodically updates the databases to reflect the behavioral changes that occur overtime. Does not perform well on larger transactional databases.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Data Mining Application for Cyber Credit-Card Fraud Detection System</td>
<td>Anomaly detection algorithm along with pattern recognition based on neural networks</td>
<td>Classifies a real-time transaction as being legitimate, suspicious and illegitimate transaction. Helps to discover fraud in real-time transactions and it does not introduces any flaws due to its trained classifier. IP address used to identify the location of the transactions being committed can be altered easily using varied proxy servers.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Customer Behaviour Analysis for Credit Card Proposers Based on Data Mining Techniques</td>
<td>Classification and clustering algorithms based on classification accuracy</td>
<td>Presents a comparative study between the various classification and clustering algorithms using classification accuracy for predicting the behavior of the consumers involved in the usage of a credit card. Assumes that most of the fraud is caused in the urban region. Restricted to the study of very few algorithms.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Comparative Study of Data Mining Model for Credit Card Application Scoring in Bank</td>
<td>Classification methods including Naive Bayes and ID3</td>
<td>Performs credit risk analysis using credit scoring to determine the eligibility of an applicant. Helps to improve the performance of credit scoring in banks. Important feature extraction turns out to be a difficult task.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Survey on Credit Card Fraud Detection Using Hidden Markov Model</td>
<td>Hidden Markov Model, RFID Device</td>
<td>Provides the users with a onetime password which enables the users to block the credit card as soon as the user realizes that the credit card has been stolen. Helps to recognize the genuine transactions. If the onetime password for a user is compromised, then there is no way to recover the user’s account.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Credit Card Fraud Detection System through Observation Probability Using Hidden Markov Model</td>
<td>Hidden Markov Model</td>
<td>Helps to identify the spending habits of all the customers. Comes out to be scalable for managing large volumes of data. Cannot be generalized to be well suited to the global fraud detection problem.</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>Title</td>
<td>Method/Algorithm</td>
<td>Benefits</td>
<td>Limitations</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[13]</td>
<td>Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithm</td>
<td>Cryptographic Algorithms: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES)</td>
<td>Helps to identify the original identity of a user. Provides multiple layers of security. Offers a fully secured file transfer process.</td>
<td>Completely relies on the user’s security pin number. If this is compromised, then the entire system works inappropriately.</td>
</tr>
<tr>
<td>[14]</td>
<td>A Survey on Outlier Detection Techniques for Credit Card Fraud Detection</td>
<td>Principal Component Analysis (PCA)</td>
<td>Helps to identify the only attributes of interest containing most of the major information. Aids in detecting frauds with less memory and computation requirements. Enables faster fraud detection.</td>
<td>Detects fraudulent transactions in a limited dataset.</td>
</tr>
<tr>
<td>[15]</td>
<td>BankSealer: An Online Banking Fraud Analysis and Decision Support System</td>
<td>Histogram Based Outlier Score (HBOS), Density-Based Spatial Clustering of Applications with Noise (DBSCAN), Cluster-Based Local Outlier Factor (CBLOF)</td>
<td>Helps to automatically detect fraudulent bank transfer transactions. It also considers debit card transactions and phone recharges. Allows to process new transactions in a faster way. Considers the user’s who perform very less number of transactions. Provides support to the analyst by aiding in his/her decision making activities.</td>
<td>Requires more complicated datasets that are usually very hard to obtain due to privacy restrictions implied by the financial institutions.</td>
</tr>
</tbody>
</table>
VI. CONCLUSION

At present, building a well defined, manageable and well understood credit card fraud monitoring system is the essential requirement of most of the financial institutions. In order to encounter credit card fraud majority of the credit card fraud detection systems have attracted a number of approaches, systems and models. This paper demonstrates the numerous techniques that are available to disclose credit card fraud. All of the approaches considered in this review adopt distinct techniques and possess its own strengths as well as limitations. Consequently, a survey of such kind facilitates to build a hybrid approach for the disclosure of credit card fraud.

REFERENCES


