Research & Reviews: Journal of Engineering and Technology

e-ISSN:2319-9873

A Survey on Application of Data Mining Techniques; It's Proficiency In Fraud Detection of Credit Card

Aliza Zafar* and Mehreen Sirshar

Department of Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan

Review Article

Received date: 21/11/2017

Accepted date: 08/01/2018

Published date: 30/01/2018

***For Correspondence**

Aliza Zafar, Department of Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan, Tel: +92 51 9292900.

E-mail: alizazafar95@gmail.com

Keywords: Mining techniques, Credit card, Hidden Markov model

ABSTRACT

Data mining techniques is widely used to detect frauds because these techniques are most effective. This paper present a comprehensive survey of various papers in which different data mining techniques are used to detect fraud. Based on defined criteria of evaluation, we have done analysis, compare techniques and evaluate each methodology on the basis of performance, efficiency and accuracy. The paper assesses strong and weak points of techniques and draws a conclusion at the end.

INTRODUCTION

Fraud can be defined as wrongful or criminal deception intended to result in financial or personal gain or to damage another individual without necessarily leading to direct legal consequences. There are two method to avoid frauds and losses, one is fraud prevention and other is fraud detection systems. Fraud prevention is the proactive mechanism which disables the occurrence of fraud. Fraud detection systems are used when the fraudsters surpass the fraud prevention systems and start a fraudulent transaction.

As the number of credit card user increases worldwide, the opportunities for attackers to steal credit card details, other information and subsequently, commit fraud are also increasing. If the credit cardholder does not realize the loss of card, it can lead to a substantial financial loss to the credit card company. Most of the time the cardholder does not aware that someone stoles his card information. The only way to detect this type of fraud is to analyze the patterns on every card and to point out any inconsistency w.r.t the usual pattern. Many techniques are used to detect credit card fraud like Decision Tree, Artificial Neural Network, Clustering, etc. This paper presents the survey of various papers on credit card fraud detection and evaluated on different parameters, the rest of papers as follow: Section II shows the existing implementation techniques in detail. In Section III, draws conclusion of the literature review. In Section IV, A comprehensive analysis of the techniques is presented.

CRIDIT CARD FRAUD DETECTION USING DATA MINING TECHNIQUES: A REVIEW

Increase in ecommerce application has resulted in the increase usage of credit card for online and also for offline payment. Credit card fraud can be defined as the illegal use of any system or, criminal activity through the use of physical card or card information without the knowledge of the cardholder. Most common techniques that are used for fraud detection are KNN, Outlier, Decision Tree, Artificial Neural Network, Clustering, Novel Method and Bayesian technique. This paper discussed summaries of other papers that are related to credit card fraud detection.

ANALYSIS ON CREDIT CARD FRAUD IDENTIFICATION TECHNIQUES BASED ON KNN AND OUTLIER DETECTION

This paper discussed that the Credit card fraud is growing along with the new development in technology. It can also be said that economics fraud extremely increases in the global communication improvement. The loss due to this fraudulent act is recorded every year and it is in billions of dollars. These frauds can be carry out very smartly that it can similar to genuine transections. An efficient method is needed to detect fraud that becomes the need for all banks in order to minimize the chaos and

bring order in place. Many techniques like classification, decision tree, machine learning sequence alignment, fuzzy logic etc. are used to for detecting credit card fraudulent transactions. Along with these techniques KNN and outlier are also used to optimize the best solution for the fraud detection problem. These techniques are proved to minimize the false alarm rates and increase the fraud detection rate. Both methods are used to in banks to detect and prevent the fraudulent transaction [1].

ADVERSARIAL LEARNING IN CREDIT CARD FRAUD DETECTION

This paper includes information about the fraudster motivation and knowledge base into an adaptive fraud detection system. In this paper adversarial learning method is used in order to model the best strategy, and also to classify the future fraudulent transactions. Use of GMM in determining a best strategy proved an effective way of finding optimal new transaction an adversary is likely to replicate. And use of SMOTE produce synthetic transactions of best strategy. These two contributions provided tools able to mimic an adversary's learning and giving the credit card company the ability to preemptively react to changing transaction strategies [2].

REAL-TIME CREDIT CARD FRAUD DETECTION USING STREAMING ANALYTICS

Increase in ecommerce application has resulted in the increase usage of credit card for online and also for offline payment. Credit card fraud is also growing with these ecommerce applications. Streaming analytical of data is a time based processing and it is used to enable near real time decision making by examining, comparing and analyzing the data even as it is streaming into application and database from myriad different sources. Streaming analytical technique is used to detect and prevent credit card fraud. Our technique is used to analyses the historical transaction data to model a system that can detect fraudulent pattern and then this model is used to analyze transaction in real time. Advantage of this technique is it can minimize the false alarm rate [3].

COMBINATION OF MULTIPLE DETECTORS FOR CREDIT CARD FRAUD DETECTION

This paper presents a signal processing technique for the credit card fraud detection. This technique establishes relationships between signal processing and pattern recognition issues around a detection problem with very low ratio between fraudulent and genuine transaction. Using fusion of scores, solution is proposed which are likely to ratio statistic. Classical detection problem analyzed by receiving operating characteristics curve is mapped to real world business requirements based on key performance indicators. Strong practical problem that combines surrogate and real data including comparison of proposed method with standard methods [4].

ONLINE CREDIT CARD FRAUD DETECTION: A HYBRID FRAMEWORK WITH BIG DATA TECHNOLOGIES

This paper proposed an online credit card fraud detection framework with big data technologies through which three major goals can achieve 1. Ability to combine multiple detection methods to improve accuracy 2. Ability to process large amount of data 3. And also ability to do the detection in real time. This paper proposed a workflow with new framework which consist of 4 layers a. distributed storage layer b. batch training layer c. key-value sharing layer d. and streaming detection layer. By using these four layers we able to support massive trading data storage, real time online fraud detection, quick model data sharing etc. This framework can also be used for other fraud detection like telecom fraud detection, internet advertising fraud detection and so on [5].

PREVENTION OF CREDIT CARD FRAUD DETECTION BASED ON HSVM

With growing technology of credit card in e-commerce credit card fraud also increases. Prevention from credit card fraud is better than detection. So the existing system prevented the credit card fraud by identifying fraud in the application of the credit card. This paper proposed a new algorithm along with existing algorithm due to the limitation of existing system. Limitations of existing system are: time constraint, scalability issues and extreme imbalanced class. These limitations are overcome by hybrid support vector machine (HSVM) along with communal and spike detection for credit card application fraud detection. HSVM is mostly used for pattern recognition and classification [6].

REAL-TIME FRAUD DETECTION IN THE BANKING SECTOR USING DATA MINING TECHNIQUES/ALGORITHM

Today's banking sector is very important almost every human has to deal with bank either physically or online. In this paper different types of fraud like insurance fraud, accounting fraud, credit card fraud etc. discuss. Detection of fraudulent activities is very important. In this paper fraudulent activities can be detected through different data mining techniques like Clustering, Artificial Neural Networking, association, forecasting, and classification to analyze the customer data in order to identify the patterns that can lead to frauds. Real time fraud detection saves the bank from huge loses and customers from financial loss as well [7].

CREDIT CARD FRAUD DETECTION AT MERCHANT SIDE USING NEURAL NETWORKS

With the increase of internet technology payment through credit card also increases. This evolution increase efficiency and

portability but this method of payment has some short comes. This make impossible for the merchant to verify whether the customers making purchase is the authentic cardholder or not. This makes it easy for a fraudulent transaction secretly. To detect fraudulent activity different techniques, patterns and algorithms are used. Many system are proposed but the system that present in this paper particularly focus on the merchant side of the industry that will beneficial to the merchant by reducing the merchant's losses [8].

AN EVALUATION OF COMPUTATIONAL INTELLIGENCE IN CREDIT CARD FRAUD DETECTION

This paper is proposed to detect credit card fraud; computational intelligence has been commonly used and plays a vital role. This paper analyzes and compares various techniques that have been commonly used to detect credit card fraud detection. It only focuses on the measure used to access the classification performance and rank of those techniques [9].

These techniques are apply on UCSD-FICO data mining contest 2009 dataset. From this experiment it analyze that fraud detection success rate is below 50% and the performance of tree classifier is better than other group of classifier. Overall success rate is taken to evaluate the performance of the classifier.

J.CREDIT CARD FRAUD DETECTION: A HYBRID APPROACH USING FUZZY CLUSTERING & AMP; NEURAL NETWORK

This paper proposed a novel based approach towards credit card fraud detection which is done in three phases. In first phase initial user authentication and verification of credit card is done. If the check is successfully cleared, then transection is passed to next phase. In second phase fuzzy clustering algorithm is applied where normal usage pattern of credit card user find based on their previous activities. According to the extent of deviation from normal pattern suspicious activity is calculated on this basis transaction is classified that it is guanine or fraud. If transaction is suspicious neural network based learning mechanism is applied whether it was actual fraud or an occasional deviation by a guanine user. By combining clustering with learning, detecting fraudulent activities and minimizing false alarms become more effective [10].

CLUSTER ANALYSIS AND ARTIFICIAL NEURAL NETWORKS: A CASE STUDY IN CREDIT CARD FRAUD DETECTION

In this paper a case study is presented that involve Multilayer Perceptron Artificial Neural Network and Cluster Analysis that applied to credit card fraud prevention. For qualitative data normalization cluster analysis was successfully used. A MLP trained using automatically normalized data presented promising results. Early results that obtained from cluster analysis and ANN on fraud detection has shown the neuronal inputs can be reducing by clustering attributes. Main objective of this paper is to present the early results obtained from ANN and cluster analysis [11].

CREDIT CARD FRAUD DETECTION AND CONCEPT-DRIFT ADAPTATION WITH DELAYED SUPERVISED INFORMATION

Fraud detection is particularly a challenging problem because of concept of drift and class unbalance. This paper describes an accurate fraud detection setting and also shows that investigator's responses and delayed labels handled distinctly. This paper proposed two fraud detection systems on the basis of an ensemble and sliding-window approach and this paper also shows that the winning strategy consists in training two separate classifiers and then aggregating the outcomes. A large dataset of real world transactions is used for experiments and results show that the alert precision, which is the primary concern of investigators, can be significantly improved by this approach [12].

CREDIT CARD FRAUD DETECTION: A CASE STUDY

This paper proposed a technique to detect credit card fraud. In this paper different technique like Genetic Algorithm, Behavior Based Technique and Hidden Markov Model is used to solve this problem. Main purpose of this paper was to detect least and accurate false fraud detection. Credit card fraud is against to security. These three techniques can be applied on each and every transaction. Hidden Markov Model maintaining log for previous transaction. Behavior Based method creates clusters or groups of data. Genetic Algorithm is used for calculating threshold value [13].

IMPLEMENTATION OF NOVEL APPROACH FOR CREDIT CARD FRAUD DETECTION

This paper present combination of techniques that were used to detect fraud. First one is shopping behavior based on which type of product that customer buys. Secondly spending behavior is detected which is based on the maximum amount spent. Third one is hidden Markov model in which users profiles are maintained and statistics of particular user and statistic of different fraud scenarios are clustered. Genetic algorithm also used for calculating threshold value. At the end average is taken by summing the results. Main purpose of this paper is to explore different views of the same problem and compare the efficiency and performance

of these three techniques [14].

A COMPARATIVE STUDY OF CHEBYSHEV FUNCTIONAL LINK ARTIFICIAL NEURAL NETWORK, MULTI-LAYER PERCEPTRON AND DECISION TREE FOR CREDIT CARD FRAUD DETECTION

Credit card fraud not only affecting common people but also making them lose huge amount of money. In this paper different data mining techniques like Decision Tree, Multi-Layer Perceptron, Chebyshev functional link artificial neural network (CFLANN) compare in terms of their classification accuracy and elapsed time for credit card fraud detection. Results show that in both the data set MLP outperformed CFLANN and Decision Tree in fraud detection. Though in credit card fraud prediction CFLANN performed better than MLP but in credit card fraud detection MLP has slightly an edge over CFLANN [15].

FRAUD DETECTION IN CREDIT CARD BY CLUSTERING APPROACH

Fraud is unauthorized activity taking place in automated payments systems but these are treated as illegal activities. Many techniques are used to detect fraud in credit card transaction. In this paper clustering technique is used. There are different methods of clustering like single link method, complete link method group average method etc. Data is generated randomly for credit card and K-means clustering is used for detecting the transaction whether it is fraud or genuine. Clusters are formed to detect fraud in credit card transaction which are low, high, risky and high risky. K-means algorithm is efficient for credit card fraud detection. To detect the fraud accurately and efficiently it is essential that real data should be available [16].

INVESTIGATION OF DATA MINING TECHNIQUES IN FRAUD DETECTION: CREDIT CARD

Now a day more secure data transfer takes place almost by means of internet but at the same time risk of transferring secure data also increases. Credit card fraud is one of the major issues. Due to increasing in volumes of data there is need to analyzed data using data mining techniques which are being used more and more. There are many papers that discuss the comparative study of five data mining techniques. This paper also analyzes the five most commonly used classification techniques in fraudulent detection. Still they suffer from uncertainty in real world dataset which is properly handled by these existing approaches. So more work is needed to overcome the problem of missing values, handling voluminous data precisely and also handling the incomplete dataset [17].

ANALYSIS ON CREDIT CARD FRAUD DETECTION TECHNIQUES: BASED ON CERTAIN DESIGN CRITERIA

Fraud in financial sector is increasing with the development of new technologies that will result in loss of billions of dollars worldwide each year. Fraud detection systems have become necessary for all credit card issuing banks to minimize their losses. Most commonly used techniques to detect fraud are Bayesian network, Decision tree, Rule-induction method, support vector machine, artificial neural network, KNN algorithm, Hidden markov model, Artificial immune system, fuzzy neural network, fuzzy Darwinian system and genetic algorithm. These all techniques can be used alone or meta-learning techniques to build classifiers. This paper presents a survey of nine different techniques that were used to detect credit card fraud and evaluates each methodology based on accuracy, speed and cost [18].

ANALYSIS ON CREDIT CARD FRAUD DETECTION METHODS

Fraudulent activities are scattered with genuine transactions and simple pattern matching techniques are not enough to detect those frauds precisely. Many different techniques are used to solve this problem like Artificial Intelligence, Genetic Algorithm, Fuzzy logic, Machine learning etc., a comprehension study on all these techniques will certainly lead to an efficient credit card fraud detection system. This paper presents a survey on different techniques that are used for detection mechanisms and evaluate each technique based on certain design criteria [19].

CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL

In this paper author model the sequence of operation in credit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, authors try to ensure that genuine transactions are not rejected. In this paper author present detailed experimental results to show the effectiveness of this approach and compare it with other techniques available in the literature [20].

IMPROVING A CREDIT CARD FRAUD DETECTION SYSTEM USING GENETIC ALGORITHM

In this paper author undertook the credit card fraud detection problem of a bank and tried to improve the performance of a

present solution. By doing this author did not take the typical objective of maximizing the number of correctly classified transactions but author defined a new objective function where the misclassification costs are variable and thus, correct classification of some transactions are more important than correctly classifying the others. For this author made an application of genetic algorithms which is a novel one in the related literature both in terms of the application domain and the cross-over operator used. The algorithm is applied to real life data where the savings obtained are almost three times the current practice. By using this algorithm performance of existing solution improved 200% [21].

NEURAL DATA MINING FOR CREDIT CARD FRAUD DETECTION

Most popular mode of payment is credit card but credit card frauds are becoming increasingly rampant in recent years. This paper model the sequence of operations in credit card transaction processing using confidence-based neural network. Receiver operating characteristic (ROC) analysis technology is also introduced in this paper to ensure the accuracy and effectiveness of fraud detection. Neural network technique is initially trained with synthetic data. If trained neural network model (NNM) is not accepted any credit card transaction with sufficiently low confidence, it is considered to be fraudulent. This paper shows how neural network algorithm, confidence value and ROC can be merged successfully to achieve credit card fraud detection [22].

CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL

By using credit card, risk of fraud transaction becomes increases. In existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done, so it is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the statistical tools for engineering and scientists to solve various problems. This paper shows that how credit card fraud can be detected by using hidden Markov model during transactions. HMM helps to obtain high fraud coverage combined with a low false alarm rate [23].

COMPARISON WITH PARAMETRIC OPTIMIZATION IN CREDIT CARD FRAUD DETECTION

In this paper five different classification method of data mining can be compare. For comparison parameters are adjusted for each method either through comprehensive search, or through genetic algorithm. These classifications can be compared in two training modes: a cost sensitive training mode where different costs for false positive and false negatives are considered in the training phase and the other is plain training mode. Cost sensitive training considerably improves the performance of all classification methods away from Naïve Bayes and independently of the training mode. Decision Tree and Artificial Immune System with optimize parameters are best methods in our experiments [24].

APPLICATION OF CLASSIFICATION MODELS ON CREDIT CARD FRAUD DETECTION

Credit card fraud activity has become increasingly widespread in recent few years. This study investigates the efficiency of applying classification methods to credit card fraud detection problems. Three different classification methods, i.e., decision tree, neural networks and logistic regression are tested for their applicability in fraud detections. This paper provides a useful framework to choose the best model to recognize the credit card fraud risk [25].

Table 1. Evaluation criteria for testing credit card detection using data mining techniques.

Parameters	Meaning	Possible values
Performance	Low utilization of resources, lower response time and mean time of Failure and recovery define the performance of the technique.	Yes, No
Correctness	Technique is working according to the specification.	Yes, No
Reliability	Technique is working or not till the time line is given.	Yes, No
Ease of use	Technique is easy to learn or use for the users.	Yes, No
Security	The proposed technique is able to detect and correct errors	Yes, No
Compatibility	Technique can combine with other techniques or not.	Yes, No t
Tool support	Tools are available for the proposed model.	Data Mining Techniques

Table 2. Analysis of parameters for testing credit card detection using data mining techniques.

Sr. No	Techniques	Performance	Correctness	Reliability	Security	Ease of Use	Compatibility	Tool support
1.	Malini N, et al. [1]	Yes	Yes	Yes	Yes	Yes	Yes	KNN and outlier detection
2.	Zeager MF, et al. [2]	No	No	Yes	Yes	Yes	Yes	Adversarial learning
3.	Rajeshwari U, et al. [3]	Yes	No	No	Yes	No	Yes	Streaming analytical
4.	Salazar A, et al. [4]	Yes	No	Yes	No	Yes	Yes	Signal processing
5.	Dai Y, et al. [5]	Yes	Yes	No	Yes	No	No	Hybrid Framework
6.	Mareeswari V, et al. [6]	No	No	No	Yes	No	No	HSVM
7.	John SN et al. [7]	Yes	Yes	Yes	Yes	Yes	Yes	Clustering, Artificial Neural Networking
8.	Srivastava A, et al. [8]	Yes	Yes	Yes	Yes	Yes	Yes	Neural Network
9.	Mahmud MS, et al. [9]	Yes	Yes	Yes	No	Yes	Yes	Decision Tree, Naïve Bayes, K-NN, SVM,NN
10.	Behera TK, et al. [10]	No	Yes	Yes	Yes	Yes	Yes	Fuzzy Clustering & amp; Neural Network
11.	Carneiro EM, et al. [11]	Yes	Yes	Yes	Yes	Yes	Yes	Cluster Analysis and Artificial Neural Networks
12.	Dal Pozzolo A, et al. [12]	Yes	No	Yes	Yes	No	No	Fuzzy Clustering & amp; Neural Network
13.	Agrawal A, et al. [13]	Yes	No	Yes	No	Yes	Yes	Genetic Algorithm, Behavior Based, HMM
14.	Kumar S, et al. [14]	Yes	Yes	No	Yes	No	No	Hidden Markov model, Genetic Algorithm
15.	Mishra MK, et al. [15]	No	Yes	No	Yes	No	Yes	Artificial Neural Network, Multi-layer Perceptron and Decision Tree
16.	Vaishali V et al. [16]	Yes	Yes	Yes	No	No	Yes	Clustering
17.	Gayathri R, et al. [17]	Yes	Yes	Yes	Yes	Yes	No	Decision Tree, Naïve Bayes, K-NN, SVM,NN
18.	Zareapoor M, et al. [18]	Yes	Yes	Yes	No	Yes	Yes	Rule-induction method,

ANALYSIS DESCRIPTION

Table 1 shows the evaluation criteria for credit card fraud detection using data mining techniques. **Table 2** shows the results of analysis of evaluation parameters defined in evaluation criteria. We have studied twenty five techniques and used seven parameters for their evaluation. Analysis of **Table 2** reveals the testing technique used in different research papers. It is seen that all the researchers have used different techniques in their research papers. Analysis shows that in only few techniques by Mareeswari V, et al. Performance is discussed but not good or effective in fraud detection. Performance is low utilization of resources and lower response time by the system. Some of techniques is not discussed this parameter. The techniques that discussed in this paper almost all like Malini N, et al. discussed correctness of their technique. Correctness defined as Technique is working according to the specification.

The technique that is trending among all researches is correctness and testability. All techniques that are used for fraud detection method are testable; the proposed technique is tested, and gave accurate result. All Techniques is working according to the specification.

Malini N, et al. used K-NN and Outlier detection techniques. K-NN method both legitimate and fraudulent examples are to be fed in order to train the data sets. This method can suit for detecting fraud with the limitation of memory. While Outlier detection mechanism use less memory and computation requirements. Outlier method work fast especially on online large datasets. These techniques optimize the best solution for fraud detection problem. By using these techniques false alarm rate become reduce and increased the fraud detection rate. By comparing these two techniques K-NN method is more accurate and efficient.

Zeager MF, et al. used adversarial learning approach. These authors first discussed the previous work done on this and then extend this framework to a practical and real world data set. GMM helped in finding the optimal new transaction an adversary is likely to replicate. Sridhar A, et al. also used SMOTE tool to provide synthetic transactions of this best strategies. Both GMM and SMOTE giving the credit card company the ability to preemptively react to the changing transaction strategies. These authors improved adversary learning by adding velocity variable in an effort to discover more revealing characteristics of the transactions.

Mareeswari V, et al. used Support Vector Machine method. This algorithm finds a special kind of linear model, maximum margin hyper plane and it classifies all training instances correctly by separating them into correct classes through a hyperplane. This technique has some limitation. Biggest limitation of SVM lies in the choice of the kernel and second is speed and size. John SN, et al. used clustering method to detect fraud.

Rajeshwari U, et al. used streaming analytical technique that is time based Processing data and it is used near real-time decision making by inspecting, relating and analyzing the data even as it is streaming into applications and database from myriad different sources. Rajeshwari U, et al. takes historical data to model a system that can detect fraudulent patterns. Streaming analytical model is used to analyze transaction in real-time. False alarm rate reduce through this technique by examining the relationship between the transaction that were actual fraud and those that were guessed as fraudulent. Model train according to the original card holder data and it is frequently updated by Salazar A, et al.

Used signal processing framework which also help to reduce the credit card fraudulent activities. Dai Y, et al. focus on online credit card fraud detection framework and achieve major goals, accuracy by combining the multiple detection models and apply model to analyze the large amount of data. Framework was implemented with latest Big Data technologies, which help to build a scalable, fault-tolerant and high performance system.

Mareeswari V, et al. used HSVM technique. There are some limitations in the existing system Scalability issues, extreme imbalanced class and time constraints. HSVM overcome these limitations with communal and spike detection. HSVM is the most used method for pattern recognition and classification. Agrawal A, et al. used hidden markov model in which users profiles are maintained and statistics of particular user and statistic of different fraud scenarios are clustered.

John SN, et al. used Clustering, Artificial Neural Networking, association, forecasting, and classification to analyze the customer data in order to identify the patterns that can lead to frauds. Agrawal A, et al. used Genetic Algorithm, Behavior Based Technique and Hidden Markov Model to solve the credit card fraud. These three techniques can be applied on each and every transaction. Hidden Markov Model maintain log for previous transactions. Behavior Based method creates clusters or groups of data. Genetic Algorithm is used for calculating threshold value. Gayathri R, et al. used five different techniques that were Neural Network, Decision Tree, Naïve Bayes, K-nn and Support Vector Machine. Each technique was applied on each transaction and after that compares their performance, accuracy and efficiency of these techniques. Zareapoor M, et al. used nine different techniques, Bayesian network, Decision tree, Rule-induction method, support vector machine, artificial neural network, KNN algorithm, Hidden markov model, Artificial immune system, fuzzy neural network, fuzzy Darwinian system and genetic algorithm which were used to overcome the fraudulent activities. Different techniques that were used to detect credit card fraud and evaluates each methodology based on accuracy, speed and cost.

Edwin R, et al. used Artificial Intelligence, Genetic A lgorithm, Fuzzy logic and Machine learning techniques. Each technique evaluate based on certain design criteria. Gadi MFA, et al. discussed five different classification methods of data mining and

compare in two training modes, a cost sensitive training mode where different costs for false positive and false negatives are considered in the training phase and the other is plain training mode. Cost sensitive training considerably improves the performance of all classification methods away from Naïve Bayes and independently of the training mode. Decision Tree and Artificial Immune System with optimize parameters are best methods in our experiments. Shen A, et al. three different classification methods, i.e., decision tree, neural networks and logistic regression are tested for their applicability in fraud detections. This paper provides a useful framework to choose the best model to recognize the credit card fraud risk.

John SN, et al. discussed the most common Neural Network technique to detect fraud. Neural network technique is totally based on the principle of human brain. But this technique has some limitation. This technique places a major role on network performance but, there is lack of method exists to determine the optimal topology for a given problem due to its high complexity of large networks.

Agrawal A, et al. all these techniques used genetic all techniques that discussed above give accurate result in algorithm to slove the credit card fraud detection problem, detecting fraud in all factors. All techniques are reliable and Mahmud MS, et al. work properly. These techniques can easily use for detecting and Dash R, et al. credit card fraud. Most of the paper discussed that data Zareapoor. Seeja S, et al. and its techniques help in considerable reduction and Shen A, et al. used Decision tree that is most common technique and easy to used. It most effective results. But decision tree also have some limitations that the decision contained in the decision tree are based on expectations, and these expectations lead to many errors in the decision tree.

Security factor is most important factor and only few techniques not follow this factor Salazar A, et al. somehow violate because for fraud detection credit card transaction data is used that is private. Security mean technique is able to detect and correct errors.

CONCLUSION

This paper present the comparative study related to different detection methods based on credit card (Decision Tree, Neural Network, Bayesian Network, genetic algorithm, support vector machine, k nearest neighbor and Artificial Immune System, Hidden Markov Model, fuzzy neural network, Novel approach, Artificial Neural Network, Genetic Algorithm, Clustering and fuzzy Darwinian system). The main objective of this paper is to discuss different detection techniques based on credit card by discussing the literature review of different papers. All the data mining techniques of credit card fraud detection discussed in this survey paper have its own weaknesses as well as strengths. Thus, this survey paper enables us to build a hybrid approach for developing some effective algorithms which can perform well for the classification problem with variable misclassification costs and with higher accuracy.

REFERENCES

1. Malini N, et al. Analysis on credit card fraud identification techniques based on KNN and outlier detection. IEEE International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). 2017;255-258.
2. Mary ZF, et al. Adversarial learning in credit card fraud detection. Systems and Information Engineering Design Symposium (SIEDS). 2017;112-116.
3. Rajeshwari U, et al. Real-time credit card fraud detection using Streaming Analytics. International Conference on Applied and Theoretical Computing and Communication Technology. 2016;439-444.
4. Addisson S, et al. Combination of multiple detectors for credit card fraud detection. IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). 2016;138-143.
5. You D, et al. Online credit card fraud detection: A hybrid framework with big data technologies. IEEE Trustcom/BigDataSE/ISPA. 2016;1644-1651.
6. Mareeswari V, et al. Prevention of credit card fraud detection based on HSVM. International Conference on Information Communication and Embedded Systems (ICICES). 2016; 1-4.
7. John SN, et al. Realtime fraud detection in the banking sector using data mining techniques/algorithm. International Conference on Computational Science and Computational Intelligence (CSCI). 2016;1186-1191.
8. Aman S, et al. Credit card fraud detection at merchant side using neural networks. International Conference on Computing for Sustainable Global Development (INDIACom). 2016;667-670.
9. Mahmud MS, et al. An evaluation of computational intelligence in credit card fraud detection. International Computer Science and Engineering Conference (ICSEC). 2016;1-6.
10. Tanmay BK, et al. Credit card fraud detection: A hybrid approach using fuzzy clustering & Neural Network. International Conference on Advances in Computing and Communication Engineering. 2015;494-499.
11. Emanuel CM, et al. Cluster analysis and artificial neural networks: A case study in credit card fraud detection. International

Conference on Information Technology - New Generations. 2015;122-126.

12. Andrea PD, et al. Credit card fraud detection and concept-drift adaptation with delayed supervised information. International Joint Conference on Neural Networks (IJCNN). 2015;1-8.
13. Ayushi A, et al. Credit card fraud detection: A case study. International Conference on Computing for Sustainable Global Development (INDIACom). 2015;5-7.
14. Ayushi A, et al. Implementation of novel approach for credit card fraud detection. International Conference on Computing for Sustainable Global Development (INDIACom). 2015;1-4.
15. Mukesh MK, et al. A comparative study of chebyshev functional link artificial neural network, multi-layer perceptron and decision tree for credit card fraud detection. International Conference on Information Technology. 2014;228-233.
16. Vaishali V. Fraud detection in credit card by clustering approach. International Journal of Computer Applications. 2014;98:29-32.
17. Gayathri R, et al. Investigation of data mining techniques in fraud detection: credit card. International Journal of Computer Applications. 2013;82:12-15.
18. Masoumeh Z, et al. Analysis on credit card fraud detection techniques: based on certain design criteria. International Journal of Computer Applications. 2012;52:35-42.
19. Edwin Raj SB, et al. Analysis on credit card fraud detection methods. International Conference on Computer, Communication and Electrical Technology (ICCCET). 2011;152-156.
20. Divya I, et al. Credit card fraud detection using Hidden Markov Model. World Congress on Information and Communication Technologies. 2011;1062-1066.
21. Özçelik MH, et al. Improving a credit card fraud detection system using genetic algorithm. International Conference on Networking and Information Technology. 2010;436-440.
22. Tao G, et al. Neural data mining for credit card fraud detection. International Conference on Machine Learning and Cybernetics. 2008;3630-3634.
23. Abhinav S, et al. Credit card fraud detection using Hidden Markov model. IEEE Transactions on Dependable and Secure Computing. 2008;5:37-48.
24. Gadi MFA, et al. Comparison with parametric optimization in credit card fraud detection. International Conference on Machine Learning and Applications. 2008;279-285.
25. Aihua S, et al. Application of classification models on credit card fraud detection. International Conference on Service Systems and Service Management. 2007;1-4.