Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 5, May 2019, pg.8 – 14

Analysis of Various Credit Card Fraud Detection Techniques

Geetika
Research Scholar, Punjabi University, Patiala, geetikapahuja1234@gmail.com

Dr. Gaurav Gupta
Assistant Professor, Punjabi University, Patiala, gaurav.shakti@gmail.com

ABSTRACT: Credit card frauds are on the rise and are getting smarter with the passage of time. Usually, the fraudulent transactions are conducted by stealing the credit card. When the loss of the card is not noticed by the cardholder, a huge loss can be faced by the credit card company. A very little amount of information is required by the attacker for conducting any fraudulent transaction in online transactions. For buying products and services online, the Internet or telephone devices are used. In some cases, the pattern in which transactions are done by the user is the only way through which it is possible to know that the card is stolen. A fraud detection method needs to be applied to reduce the rate of successful credit card frauds. This research work is based on the prediction of fraudulent credit card transactions. In this paper, various techniques for the credit card fraud detection are reviewed in terms of certain parameters.

Keywords: Credit card, machine learning, classification

I. INTRODUCTION

The prediction analysis is most useful type of data which is performed today. To perform the prediction analysis the patterns needs to generate from the dataset with the machine learning. The prediction analysis can be done by gathering historical information to generate future trends [1]. So, the knowledge of what has happened previously is used to provide the best valuation of what will happen in future with predictive analysis. The predication analysis models are designed according to application type. The model is trained using the sample data that includes known attributes. The new data can be analyzed and its behavior can be determined using this trained model. Credit card fraud detection is one of the applications of prediction analysis. In credit card fraud detection, the fraud transactions are predicted based on the historical information of credit card transactions [2].The credit cards are being used very commonly today for buying several goods and accessing various services in our daily lives. When the physical-card

based purchasing technique is applied, the card is given by the cardholder to the merchant so that a successful payment method can be performed. The fraudulent transactions are conducted by the attacker by stealing the credit card. When the loss of the card is not noticed by the cardholder, the huge loss can be faced by the credit card company. A very little amount of information is required by the attacker for conducting any fraudulent transaction in online transactions. For buying products and services online, the Internet or telephone devices are used. In some cases, the pattern in which transactions are done by the user is the only way through which it is possible to know that the card is stolen. A fraud detection method needs to be applied to reduce the rate of successful credit card frauds. The existing purchase data of the particular cardholder is the basis on which this fraud detection method is proposed. One of the biggest threats being faced by business organizations today is credit card fraud. The approaches that result in causing fraud need to be perceived initially so that they can be handled in an effective manner. For committing the fraud, a variety of methods are used by credit card fraudsters. When someone else's credit card is used for personal reasons and the owner of the card does not have any knowledge about it, the credit card fraud is outlined. The person who is conducting the fraud will never aim to contact the owner of the card or repay the losses to the actual user.

There are various issues and challenges being faced by fraud detection systems amongst which few are enlisted below [3]:

a. Defining the Type and Level of Fraud: It is very important to define the type and the level of fraud that has occurred in any transaction. However, a universal measurement approach through which all the frauds that exist today can be identified is impossible to be developed. Thus, the level of frauds is reported and then depending upon certain factors, that fraud is categorized into any of the subcategories that are predefined.

b. Fraud Departments Resides in Silos: Silos are the organizations which work individually and do not share any personal information with other groups.[4] It is impossible for a fraud detection approach to identify the fraudster that goes online, changes the account address of a genuine user and then requests for a new card for personal use, for such silo systems. It is possible for one team to just view the change is address and the other to view the transactions made from that card.

c. A requirement of Real-time Detection Techniques: The techniques available currently for detecting the frauds only work for cases where fraudulent transactions have occurred for more than one times. Also, the speed at which fraudster is moving is higher as compared to the fraud monitoring solution. Therefore, till the time that fraud is detected, the money of genuine user is already stolen. So, it is important to provide real-time detection [5] techniques for financial institutions for protecting their clients. The suspicious transaction patterns are to be monitored and recognized immediately by the tools such that actions can be made as soon as the fraudster makes any attempt. Thus, the losses can be prevented.

d. Fraud is measured a Reasonable Issue: The banks have considered fraud prevention techniques as their basic necessity since the numbers of frauds are growing with each day [6]. Therefore, a reasonable issue being faced today is the various potential gaps, which needs to be exposed and resolved.

e. Enhance Working Practices: The fraudsters are adapting new techniques too successfully launch frauds. The staff and systems can be much efficient so that it can quickly detect frauds in credit cards.

1.1 Types of Frauds

There are different kinds of frauds found in credit card transactions. Amongst them few are explained below [7]:

a. Application Fraud: When someone falsifies an application such that a credit card can be acquired, this kind of fraud occurs. There are three different ways in which the application fraud occurs:

- When the personal information of another person is obtained illicitly by an individual and the legitimate information is partly used for opening account on his or her name, the assumed identity fraud occurs.

- When false information related to the financial status is provided for attaining credit, the financial fraud occurs.

- When a card is stolen from the postal service before it is received at the actual destination, postal intercepts or Not-received items (NRIs) occurs. [8]

b. Lost/ Stolen Cards: The card is either lost or stolen from the actual account holder in order to perform certain criminal activities. A fraudster does not need to get involved in any kind of technology to conduct this kind of fraud. This kind of fraud was the first credit card fraud conducted ever.

c. Account Takeover: When the personal information of a valid customer is attained by a fraudster, this type of fraud occurs. Either the account number or card number of a legitimate account is taken by the fraudster to take control over it. Further, for mailing the contact information to new address, the fraudster masquerades the real cardholder by contacting the card issuer. A report of lost card and a request of replacement are demanded by the person who commits the fraud.

d. Fake and Counterfeit Cards: The highest threat within credit card frauds is related to the generation of counterfeit cards along with the stolen cards. For generating counterfeit cards, new and innovative ideas have been introduced by fraudsters over time.[9]

II. LITERATURE REVIEW

Kuldeep Randhawa et al. [10] proposed a technique using machine learning to detect credit card fraud detection. Initially, standard models were used after that hybrid models came into picture which made use of AdaBoost and majority voting methods. Publically available data set had been used to evaluate the model efficiency and another data set used from the financial institution and analyzed the fraud. Then the noise was added to the data sample through which the robustness of the algorithms could be measured. The experiments were conducted on the basis of the theoretical results which show that the majority of voting methods achieve good accuracy rates in order to detect the fraud in the credit cards. For further evaluation of the hybrid models noise of about 10% and 30% has been added to the sample data. Several voting methods have achieved a good score of 0.942 for 30% added noise. Thus, it was concluded that the voting method showed much stable performance in the presence of noise.

Abhimanyu Roy et al. [11] proposed deep learning topologies for the detection of fraud in online money transaction. This approach is derived from the artificial neural network with in-built time and memory components like long term short term memory and several other parameters. According to the efficiency of these components in fraud detection, almost 80 million online transactions through credit card have been pre-labeled as fraudulent and legal. They have used high performance distributed cloud computing environment. The study proposed by the researchers provides an effective guide to the sensitivity analysis of the proposed parameters as per the performance of the fraud detection. The researchers also proposed a framework for the parameter tuning of Deep Learning topologies for the detection of fraud. This enables the financial institution to decrease the losses by avoiding fraudulent activities.

Shiyang Xuan et al. [12] used two types of random forests which train the behavior features of normal and abnormal transactions. The researcher compares these two random forests which are differentiated on the basis of their classifiers, performance on the detection of credit card fraud. The data used is of an e-commerce company of China which is utilized to analyze the performance of these two types of random forests model. In this paper, the author has used B2C dataset for the identification and detection of fraud from the credit cards. Therefore, the researcher concluded from the result that the proposed random forests provide good results on small dataset but there are still some problems like imbalanced data which makes it less effective than any other dataset.

Zahra Kazemi et al. [13] proposed Deep autoencoder which is used to extract the best characteristics of the information from the credit card transaction. This will further add softmax software to resolve the class labels issues. An overcomplete autoencoder is used to map the data into a high dimensional space and a sparse model was used in a descriptive manner which provides benefits for the classification of a type of fraud. Deep learning is one of the most motivated and powerful techniques being employed for the detection of fraud in the credit card. These types of networks have a complex distribution of data which is very difficult to recognize. Deep autoencoder has been used in some stages to extract the best features of the data and for the classification purposes. Also, higher accuracy and low variance are achieved within these networks.

John O. Awoyemi et al. [14] proposed an investigation through which the performances of several algorithms were evaluated when they were applied on credit card fraud data that is highly skewed. The European cardholders' 284,807 transactions were used as a source to generate the dataset of credit card transactions. On the skewed data, a hybrid approach of under-sampling and oversampling is performed. On raw and preprocessed data, there are three different techniques applied in Python. Based on certain parameters like precision, sensitivity, accuracy, balanced classification rate and so on, the performances of these techniques are evaluated. It is seen through the achieved results that in comparison to naïve Bayes and logistic regression approaches, the performance of k-NN is better.

Sharmistha Dutta et al. [15] presented a study on the commonly found crime within the credit card applications. There are certain issues faced when the existing non-data mining approaches are applied to avoid identity theft. A novel data mining layer of defense is proposed for solving these issues. For detecting the frauds within various applications, two algorithms named Communal Detection and Spike Detection which generate novel layer. There is a large moving window, higher numbers of attributes and numbers of link types available which can be searched by CD and SD algorithms. Thus, results can be generated by the system by consuming a huge amount of time. Since the attackers do not get time to modify their behaviors with respect to the algorithms being deployed in real time, there is no true evaluation achieved even after a regular update of the algorithms. Therefore, it is not possible to properly demonstrate the concept of adaptability. These issues can be resolved by making certain enhancements in the proposed algorithm in future work.

Krishna Modi et al. [16] investigated several techniques that were used for detecting the fraudulent transactions and provided a comparative study amongst them. The fraudulent transactions can be detected by utilizing either one of these or integrating any of these methods. The model can possibly be trained in a more accurate manner by adding new features. Several data mining techniques are being used by bank and credit card companies for detecting fraud behaviors. The normal usage pattern of clients depending upon their past activities can be identified by applying any of these methods. Therefore, a comparative analysis is made here by studying different fraud detection techniques proposed over the years.

Table 1: Table of Comparison

Author	Year	Description	Outcome
Kuldeep Randhawa	2018	A technique using machine learning to detect credit card fraud detection. Initially, standard models were used after that hybrid models came into picture which made use of AdaBoost and majority voting methods. Publically available data set had been used to evaluate the model efficiency and another data set used from the financial institution and analyzed the fraud.	Several voting methods have achieved a good score of 0.942 for 30% added noise.
Abhimanyu Roy	2018	This approach is derived from the artificial neural network with in-built time and memory components like long term short term memory and several other parameters. According to the efficiency of these components in fraud detection, almost 80 million online transactions through credit card have been pre-labeled as fraudulent and legal.	The researchers also proposed a framework for the parameter tuning of Deep Learning topologies for the detection of fraud. This enables the financial institution to decrease the losses by avoiding fraudulent activities.
Shiyang Xuan	2018	The researcher compares these two random forests which are differentiated on the basis of their classifiers, performance on the detection of credit card fraud. The data used is of an e-commerce company of China which is utilized to analyze the performance of these two types of random forests model.	The researcher concluded from the result that the proposed random forests provide good results on small dataset but there are still some problems like imbalanced data which makes it less effective than any other dataset.
Zahra Kazemi	2017	Deep autoencoder which is used to extract the best characteristics of the information from the credit card transaction. This will further add softmax software to resolve the class labels issues. An overcomplete autoencoder is used to map the data into a high dimensional space and a sparse model was used in a descriptive manner which provides benefits for the classification of a type of fraud.	Deep autoencoder has been used in some stages to extract the best features of the data and for the classification purposes. Also, higher accuracy and low variance are achieved within these networks.

John O. Awoyemi	2017	The European cardholders' 284,807 transactions were used as a source to generate the dataset of credit card transactions. On the skewed data, a hybrid approach of under-sampling and oversampling is performed. On raw and preprocessed data, there are three different techniques applied in Python	It is seen through the achieved results that in comparison to naïve Bayes and logistic regression approaches, the performance of k-NN is better
Sharmistha Dutta	2017	There are certain issues faced when the existing non-data mining approaches are applied to avoid identity theft. A novel data mining layer of defense is proposed for solving these issues. For detecting the frauds within various applications, two algorithms named Communal Detection and Spike Detection which generate novel layer.	Therefore, it is not possible to properly demonstrate the concept of adaptability. These issues can be resolved by making certain enhancements in the proposed algorithm in future work.
Krishna Modi	2017	The fraudulent transactions can be detected by utilizing either one of these or integrating any of these methods. The model can possibly be trained in a more accurate manner by adding new features.	Therefore, a comparative analysis is made here by studying different fraud detection techniques proposed over the years.

Conclusion

The fraud transaction detection is the major issue of prediction due to frequent and large number of transactions. The fraud transaction prediction has the two phases which are feature extraction and classification. In the first phase, the feature extraction technique is applied and in the second phase classification is applied for the fraud transaction detection. In this paper, various techniques for the credit card fraud detection are reviewed in terms of certain parameters

References

[1] S.B.E. and Portia, A.A., Raj, "Analysis on credit card fraud detection methods," International Conference on Computer, Communication and Electrical Technology (ICCCET), pp. 152-156, 2015.

[2] Rajni, Bhupesh Gour, and Surendra Dubey Jain, "A hybrid approach for credit card fraud detection using rough set and decision tree technique," International Journal of Computer Applications, vol. 139, no. 10, pp. 1-6, 2016.

[3] Agrawal A.N Dermala N., "Credit card fraud detection using SVM and Reduction of false alarms," International Journal of Innovations in Engineering and Technology (IJIET), vol. 7, no. 2, pp. 176-182, 2016.

[4] Phua C., Lee V., Smith, Gayler K.R., "A comprehensive survey of data mining-based fraud detection research", arXiv preprint arXiv:1009.6119, 2010.

[5] Stojanovic A., Aouada D., Ottersten B Bahnsen A.C., "Cost-sensitive credit card fraud detection using Bayes minimum risk," in 12th International Conference on Machine Learning and Applications (ICMLA), pp. 333-338, 2013.

[6] Carneiro E.M., Dias L.A.V., Da Cunha A.M., Mialaret L.F.S., "Cluster analysis and artificial neural networks: A case study in credit card fraud detection", in 12th International Conference on Information Technology-New Generations, pp.122-126, 2015.

[7] S. Aghili and P. Zavarsky K. T. Hafiz, "The use of predictive analytics technology to detect credit card fraud in Canada," in 11th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, 2016.

[8] Bansal M Sonepat H.C.E., "Survey Paper on Credit Card Fraud Detection," International Journal of Advanced Research in Computer Engineering & Technology, vol. 3, no. 3, pp. 827-832, 2014.

[9] S., Tuyls, K., Vanschoenwinkel, B. and Manderick, "Credit card fraud detection using Bayesian and neural networks," in Proceedings of the 1st international naiso congress on neuro-fuzzy technologies, pp. 261-270, 2002.

[10] Kuldeep Randhawa, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim and Asoke K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," IEEE Access, vol. 6, pp. 14277-14284, 2018.

[11] A. Roy and J. Sun and R. Mahoney and L. Alonzi and S. Adams and P. Beling, "Deep learning detecting fraud in credit card transactions," in Systems and Information Engineering Design Symposium (SIEDS), pp. 129-134, 2018.

[12] Guanjun Liu, Zhenchuan Li, Lutao Zheng, Shuo Wang and Changjun Jiang Shiyang Xuan, "Random Forest for Credit Card Fraud Detection," in IEEE 15th International Conference On Networking, Sensing and Control (ICNSC), pp.1-6, 2018.

[13] Zarrabi, H. Kazemi, "Using deep networks for fraud detection in the credit card transaction," IEEE 4th International Conference In Knowledge-Based Engineering and Innovation (KBEI), pp. 0630-0633, 2017.

[14] John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadaren Awoyemi, "Credit card fraud detection using machine learning techniques: A comparative analysis."International Conference on Computing Networking and Informatics (ICCNI), pp. 1-9, 2017.

[15] S. Dutta, A. K. Gupta and N. Narayan, "Identity Crime Detection Using Data Mining, "3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, pp. 1-5, 2017.

[16] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions, "International Conference on Intelligent Computing and Control (I2C2), Coimbatore, pp. 1-5, 2017.

