Credit Card Fraud Detection System

Pavan Zadbuke[1] Prem Suryawanshi[2] Shruti Gaikwad[3] Shweta Gunnal[4] Mrs. Vrushali Kondhalkar[5]

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]JSCOE, Pune, India

Abstract— Credit card fraud is a highly problematic situation that has been plaguing banks and other credit institutions all across the globe. The criminals are being highly inventive in getting around the loopholes and the security protocols that have been designed by these institutions to prevent this kind of fraud. This has led to a lot of research being done on this topic which has been analyzed in depth in this survey article. The fraudulent transactions are highly difficult to detect due to the techniques used by the criminal that can effectively mark it as a legitimate transaction that goes unnoticed by the systems. To improve the effective detection of fraud on a credit card there is a need for an effective technique that utilizes machine learning approaches to improve the precision of the detection. For this purpose, an effective technique has been visualized through the implementation of the hidden Markov model and decision tree to achieve the fraud detection goals. This approach will be well defined in the future editions of this article.

Keywords: Hidden Markov Model, Decision Tree

I. INTRODUCTION

The significant improvements in the data analysis and machine learning approaches have been contributing towards an effective realization of processing and management of a large amount of data. Due to the significant increase in the number of users on the internet platform, there has been a considerable rise in the amount of data that is being generated every single day. These users have also been contributing significantly towards the development and the introduction of essential services that are realized through the internet platform. The services have been increasing significantly over the past few years which has led to the fact that almost everything can be achieved on or through the internet.

The various services offered on the internet platform have grown to accommodate social media websites E-Commerce and also banking facilities. These facilities allow for the effective creation of an online platform that can be utilized by the users for the purpose of improving ease of communication and performing other activities. A lot of these users effectively safeguarded against attacks and other intrusions through the use of robust security and authentication mechanisms.

Even though there has been the effective and useful implementation of these services on the internet platform there is always a security concern linked with it. The use of multiple securities and authentication services has been considered in the prevention of these crimes to a certain degree. But the various individuals with nefarious intentions still performed these activities through loopholes and other mechanisms. There has been a large infiltration and increase in the number of fraudulent transactions that are being committed on the online platform. These credit card transactions are being fraudulently made which can be highly problematic to the credit card holder as well as the financial institution providing the credit services.

The criminals have been effectively utilizing various techniques and bypassing the security protocols that are set by the financial institutions. These institutions try to safeguard against fraudulent practices as it could lead to a lot of losses for the investors as well as other customers of this financial institution. Banks and other credit services have been highly effective in achieving robust security protocols that can significantly reduce but cannot completely eliminate credit card fraud. This is due to the fact that the techniques being used by the criminals are highly complicated and complex which could lead to a lot of variables that need to be understood for the purpose of detection.

Therefore, there is a need for an effective technique for the purpose of detecting credit card fraud accurately by analyzing the different attributes and making a well-informed decision. For this purpose, a number of recent researchers on the paradigm of detecting credit card fraud have been effectively outlined in this survey article. These approaches have been instrumental in achieving our approach for this methodology effectively. The use of machine learning algorithms can provide a significant advantage as it can effectively analyze multiple attributes and provide probabilities for credit card fraud detection. This approach will be significantly elaborated in the upcoming research on this topic.

This literature survey paper dedicates section 2 for analysis of past work as a literature survey, and finally, section 3 concludes the paper with traces of future enhancement.

II. RELATED WORKS

1) I.Benchaji states in online sector credit fraud is the growing problems thus fraud can be to obtain the illegitimate funds from an account or to get good without paying money due to this user provider are facing various problems. [1] Developing Fraud Detection System (FDS) is used for the variance datasets which is challenging part in machine learning. According to similar attributes the data is clustered by using the k-means algorithm for split minority class. To handle the imbalanced data set the genetic algorithms is applied.
2) K.Hafiz elaborates the use of a PAT which includes cardholder's protection and also the credit card deception losses according to the Federally Regulated Financial Institutions (FRFI). Thus by having literature review PAT vendor came with solution which identified by the proposed paper. Thus the system detect and immediately recognize doubtful credit card transaction patterns. The PAT faces the issues such as false positive or false negative alerts created by the solution model.
3) S.Khatri presents credit card settlement is most commonly used in the recent years it also have their own

problems. The time taken by acceptance or rejection is done in very short period of time. Now days there has been electronic payment service such as credit and debit cards this is led to growth of the credit card frauds. [3] Thus to handle this problem some machine learning algorithms can be used such as Decision Tree, Logistic Regression, kNN and Naive Bayes. Decision Tree is known as preferred model so that the system can take the minimum time for the prediction.

4) F.Elhlouli explains credit card payments are increasing day by day due to increasing digitalization of the banking department billions of transactions are done every day in that lot of fraudulent is identified. [4]To bring the solution to this the author of the proposed paper came with solution by implementing two machine learning algorithm such as like Multilayer Perceptron (MLP) and Extreme Learning Machine (ELM). According to BBC statistics $21 billion Credit card cheat has cost worldwide.
5) Y.Lucas elaborates data mining techniques with the combination of machine learning to detect credit card frauds. There are several difficulties such as purchase evolve over time in credit card fraud detection.[5] The proposed paper comes with technique where the classifying the transactions is done every day and it is also compared with the other days. Thus this technique built distance matrix characterizing the difference between the two days.In paper the user is specified by his age, gender and bank and transaction by the amount, type of payment and by some secret features.
6) S. S. H Padmanabhuni describes the credit card double-dealing and credit card payment delay are growing every day and the account is ceased or it will go to default.[6] If any financial institution faces lot of default or ceased account institute have to face a huge loss. Many of the financial institutions forgot to track the customer payment bill due to wrong credentials so they don't pay the bill. Thus to classify this default account the proposed paper has implemented the machine learning algorithms for classification purpose it is examined by using machine learning and deep learning models.
7) K.Modi explains nowadays cashless transactions are becoming popular as there is increase cashless transaction such as mobile wallet, credit card transactions and online transactions other side there is also growth in fraudulent transactions. Fraudulent proceedings can be defined as to remove funds from the user's account using his confidential information without his or her permission. [7] In proposed paper the author use machine learning algorithm to predict

   Fraudulent transactions and comparison of these methods is done such hidden Markova model, artificial neural network and Convolutional neural network.
8) F.Ghobadi describes e-business is growing on larger scale in every country with this simultaneously fraud with associated with credit cards in banking transaction is also increasing. As there is increase in banking fraud lot of technique has been develop for financial cheat detection. In proposed paper the author uses Artificial Neural Networks (ANN) for credit fraud detection and for the prevention of credit fraud. [8] With ANN the author also implemented model known Cost Sensitive Neural Network (CSNN) for misuse detection approach. The proposed technique is compared with AFDM model for the better result
9) V.Jain narrates because of frauds occurring in the banking sector the credit card users and financial institution as to go under the huge losses. [9] Thus to detect the credit card frauds many researchers are working on it. The author of the proposed paper use a real set of data of more than one lakhs of credit and implement machine learning algorithms such as Decision tree, Random Forest and XGBOOST. XGBoost is an algorithm which contains one of the highest accuracy rates and decision tree contains the minimum accuracy rate. Thus paper comes to conclusion and results XGBOOST is better than the Decision Tree and Random Forest algorithms.
10) A.Thennakoon states in large quantities online transactions has been and credit card financial proceeding holds the huge transactions. [10] This fraud can be stopped by using only by the prevention and detection of the fraud. Thus the fraud detection method is newly imposed in the banking sector it may be expensive and high-risk thus to classify this issue Logistic Regression is used with this Gaussian Mixture Models is used for the occurrence of fraudulent transactions. The proposed paper overcomes problem such as filtering of large datasets, the formation of labeled and unlabeled data and the class imbalance.
11) A.Khine explains data is increasing exponentially from different sources and from the many applications. Thus to handle this huge data classification algorithms have been presented in this paper. The proposed paper implements Online Boosting (OLBoost) Approach to get the accurate prediction with less time complexity and memory complexity. [11] Two main analytical methods of data stream mining are classification and clustering. Decision tree learning method is the best data stream classification learning methods which fast. The system not only uses UCSD-FICO credit card dataset but also the dataset is downloaded from Kaggle website.
12) X..Yu presents the fraud detection system as the fraud is increasing day by day in the banking department due to various option of cashless transaction. In much different way the fraud is done. To build a fraud detection application the huge amount of data is collected from the bank sector by the researcher. [12] The fraud recognition system is developed by using the machine learning algorithms. The paper used the machine learning algorithm such as Naïve Bayes, logistic regression and support vector machine to develop fraud detection system. Thus by implementing neural network model it overtakes some traditional methods like SVM and logistic regression.

III. CONCLUSION AND FUTURE SCOPE

The methodology for the detection of fraudulent transactions on a credit card has been effectively surveyed in this survey article. Credit card fraud is highly problematic and a very costly affair as it can lead to large-scale losses to the financial

institution that is offering the credit. The criminals are highly intelligent and utilize their knowledge of the various security protocols laid in place to prevent such transactions to achieve fraud which is difficult to stop and perform its accurate detection. Therefore, for the purpose of effectively detecting the fraud being committed through credit cards precisely the implementation of machine learning approaches has been suggested through the effective review of the current literature on this topic. The approach implements a hidden Markov model and decision tree to realize the fraudulent transaction detection precisely. This technique will be further elaborated on in the upcoming editions of this research article.

REFERENCES

[1] I. Benchaji, S. Douzi and B. ElOuahidi, "Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Faud Detection," 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, 2018, pp. 1-5, doi: 10.1109/CSNET.2018.8602972.

[2] K. T. Hafiz, S. Aghili and P. Zavarsky, "The use of predictive analytics technology to detect credit card fraud in Canada," 2016 11th Iberian Conference on Information Systems and Technologies (CISTI), Las Palmas, 2016, pp. 1-6, doi: 10.1109/CISTI.2016.7521522.

[3] S. Khatri, A. Arora and A. P. Agrawal, "Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2020, pp. 680-683, doi: 10.1109/Confluence47617.2020.9057851.

[4] 4. F. Z. El hlouli, J. Riffi, M. A. Mahraz, A. El Yahyaouy and H. Tairi, "Credit Card Fraud Detection Based on Multilayer Perceptron and Extreme Learning Machine Architectures," 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 2020, pp. 1-5, doi: 10.1109/ISCV49265.2020.9204185.

[5] Y. Lucas et al., "Dataset Shift Quantification for Credit Card Fraud Detection," 2019 IEEE Second International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Sardinia, Italy, 2019, pp. 97-100, doi: 10.1109/AIKE.2019.00024.

[6] S. S. H. Padmanabhuni, A. S. Kandukuri, D. Prusti and S. K. Rath, "Detecting Default Payment Fraud in Credit Cards," 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT), Visakhapatnam, India, 2019, pp. 15-153, doi: 10.1109/ICISGT44072.2019.00018.

[7] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321781.

[8] F. Ghobadi and M. Rohani, "Cost sensitive modeling of credit card fraud using neural network strategy," 2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), Tehran, 2016, pp. 1-5, doi: 10.1109/ICSPIS.2016.7869880.

[9] V. Jain, M. Agrawal and A. Kumar, "Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2020, pp. 86-88, doi: 10.1109/ICRITO48877.2020.9197762.

[10] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga and N. Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 488-493, doi: 10.1109/CONFLUENCE.2019.8776942.

[11] A. A. Khine and H. W. Khin, "Credit Card Fraud Detection Using Online Boosting with Extremely Fast Decision Tree," 2020 IEEE Conference on Computer Applications(ICCA), Yangon, Myanmar, 2020, pp. 1-4, doi: 10.1109/ICCA49400.2020.9022843.

[12] X. Yu, X. Li, Y. Dong and R. Zheng, "A Deep Neural Network Algorithm for Detecting Credit Card Fraud," 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Fuzhou, China, 2020, pp. 181-183, doi: 10.1109/ICBAIE49996.2020.00045

