A Review on Credit Card Fraud Detection Techniques

Reethu Elza Joseph
PG Scholar, Department of CSE
Mangalam College of Engineering
Ettumanoor, Kottayam, India

Dr. L. C Manikandan
Professor, Department of CSE.
Mangalam College of Engineering
Ettumannoor, Kottayam, India

***Abstract*—Credit card fraudulent is presently the most frequently occurring problem in the present world. This is due to the increase in both online transactions and e-commerce platforms. Credit card fraud generally happens when the cardboard was stolen for any of the unauthorized purposes or maybe when the fraudster uses the master card information for his use. Currently, we are facing a lot of credit card problems. To detect the fraudulent activities the fraud detection system was introduced. This paper aims to focus mainly on machine learning and deep learning algorithms used for credit card fraud detection. In this review paper various techniques of Credit card fraud detection are reviewed.**

Keywords- Credit card fraud Detection, Fraud transaction, Machine Learning, e-commerce

I INTRODUCTION

Credit card plays a very important role in today's economic world. E-commerce and lots of other online sites have increased the web payment modes, increasing the danger for online frauds. Increase in frauds, researchers started using different machine learning methods to detect and analyse fraud rates in online transactions. With the emerging rise of technology today, the dependency on e-commerce and therefore the online payments has grown exponentially. There are two categories of credit card fraud: application fraud and behaviour fraud. Application fraud refers to fraudulent master card applications. Such fraud occurs when a fraudster initiates a new credit card process using false identity details and the issuer accepts the request. Behaviour fraud occurs after a master card is correctly issued and denotes master card transactions that involve fraudulent behaviour. Credit card fraud detection has been significant issue for master card users and financial organizations. Because detecting even a little number of fraudulent transactions would protect large amounts of cash .. The master card information is confidential, the bank and therefore the other financial enterprises doesn't want to disclose the knowledge about their customers. Risk management is critical for financial enterprises to survive in such competing industry. The provisional loss arises thanks to the "bad" accounts bank lends the cash to customers who eventually don't have capability to pay back. In the risk management, the probabilities of false negative (false "good" accounts) could still be high. However, by leveraging their performance like master card utilization, payment information, risks can further be managed to regulate provisional loss. In this paper, a focus on risk management as well as fraud detection is depicted. It shows an interest in classifying if a booked account as a "bad" account within 12 months since booked. Since an internal" account within 12 months since booked. Since an internal classification model is already available, , with a secondary interest to train a better classifier to outperform the benchmark model. Since there are few research initiatives that implements fraud detection. Concentration on how to optimize fraud detection techniques is brought to light. Machine Learning may be a natural outgrowth of the intersection of computing and Statistics. There are some tasks that humans perform effortlessly or with some efforts, but we Deep are unable to explain how we perform them.. Machine learning algorithms are helpful in bridging this gap of understanding.. Challenges involved in credit card fraud detection are Enormous Data is processed every day and the model build must be fast enough to respond to the scam in time, imbalanced Data, Data availability, Misclassified Data. The common drawbacks of these existing techniques are: (a) Different sets of features had an impact on the results. (b) SMOTE drawbacks is that under sampling may lose some potential information, and oversampling may lead the overfitting.(c)AdaBoost is mostly used classification whereas extra learning cost is a burden. In this paper, we attempt to collect andSome of the machine learning algorithms used for credit card fraud detection is SMOTE,AdaBoost and Majority Voting,Smote Technique and Whale Optimization Algorithm,variational automatic coding integrate various methods used in credit card fraud detection and analyse them from various aspects..The rest of study is organized as follows.section ii provides literature survey of different types of credit card fraud detection techniques and conclusion described in section 3.

II . LITERATURE SURVEY

In 2018, KULDEEP RANDHAWA , et al. proposes a. hybrid methods which uses AdaBoost and majority voting methods ,which are applied to standard models, for fraud credit detection .A publicly available credit card data set is used to evaluate the model efficiency. A real-world MasterCard data set from a financial organization is analyzed then . In addition, noise is added to the info samples to further assess the robustness of the algorithms. The experimental results positively indicate that

majority voting method achieves good accuracy rates in credit cards fraud detection. A number of ordinary models which include NB, SVM, and DL are utilized in the empirical evaluation. . A publicly available mastercard data set has been used for evaluation using individual (standard) models and hybrid models using AdaBoost and majority voting combination methods and therefore the accuracy rates are all above 99%. Hybrid methods which use AdaBoost and majority voting methods are applied.
choosed for performance evaluation. The majority voting method achieves good accuracy rates.
Easy to implement and AdaBoost improves individual results.Accuracy rates are still above 90% even with 30% noise in the data set. Data imbalance is observed In 2019, Sahayasakila.V, etal. proposes two main important algorithm techniques that are whale optimization algorithm(WOA) and Smote(synthetic minority oversampling technique). The Smote technique is employed to unravel Class imbalance problem. The Whale optimization algorithm comprises mainly of three operators which are used to stimulate the search for prey, encircling prey and bubble-net scratch around the behavior of humpback whales. It is also used to increase the efficiency of the credit card fraud detection system. The Smote technique is employed to unravel Class imbalance problem. Thus by using the SMOTE technique and Whale optimization algorithm master card fraud detection system solves the matter of knowledge imbalance, reliability, data optimization, and improvises the convergence speed.. The Kaggle datasets are trained by using the SMOTE technique. SMOTE technique is employed to unravel data imbalance problem. Smote Technique and whale optimization algorithm is used. Using the smote technique the data, which is nothing but the transactions are trained. The smote technique synthesizes all the fraud transactions from the original non-fraud transactions. The Smote technique is used to solve Class imbalance problem. Solves the problem of data imbalance, reliability, data optimization, and improvises the convergence speed.
Differentiate the fraud transactions from the original transactions done by the card holders SMOTE drawbacks is that under sampling may lose some potential information, and oversampling may lead the over fitting. Need good understanding of typical and abnormal behaviors for different type of fraud cases. SMOTE is not very practical for high dimensional data The WOA improvises the convergence speed and reliability. The whale optimization code gets the optimal weight of the transaction. Whale algorithm improves the efficiency of the system. The WOA formula optimizes the fraud transactions, detects the error and updates the weight. The architectural design of credit card fraud detection system involves two parts training the data and testing the data. The training part is split into two sub processes. The first process is that the card holders transaction amount is converted into observation symbols to calculate threshold from the sequence of amount. The second process is clustering. clustering groups the data into clusters. The experimental analysis of Credit card fraud detection system using whale optimization and SMOTE technique is observed to be much more efficient than BP neural networks. The problem of class imbalance is overcome using smote technique. Thus by using the simulation of the behaviour of the whales the convergence speed is improvised and the efficiency of the system is increased .The system differentiates all the fraud transactions from the authentic transactions. Thus this module is disdainful in solution accuracy.
In 2020, Altyeb Altaher Taha.et.al proposes an intelligent approach in credit card fraud detection using an optimized light gradient boosting machine (OLightGBM). A Bayesian-based hyper parameter optimization algorithm is intelligently integrated to tune the parameters of a light gradient boosting machine (LightGBM), intelligent approach for detecting fraud in credit card transactions using an optimized light gradient boosting machine (OLightGBM).This approach is based on the LightGBM algorithm, which can bundle unique features into a single bundle. LightGBMuses the gradient-based one side sampling (GOSS) method to preserve the accuracy of the information gain estimation. This approach obtained the highest Accuracy. Does not require prior information, the model is updated continuously by adding new mastercard transactions. To improve the performance, the paper does not contribute any methods The contribution for this intelligent approach for detecting fraud in credit card transactions using an optimized light gradient boosting machine in which a Bayesian-based hyperparameter optimization algorithm is utilized to optimize the parameters of the light gradient boosting machine. This method achieved the highest performance in terms of accuracy (98.40%), Area under receiver operating characterisic function (AUC) (92.88%), Precision (97.34%) and F1-score (56.95%),Here two different real-world data sets are considered . The first data set consists of 284,807 credit card transactions made by the credit card owners in September 2013 in Europe. The second data set is the UCSD-FICO and achieved an average accuracy of 0.98% for the two data sets, which is the ratio of correctly predicted credit card transactions to the total number of transactions. The results also highlight the importance and value of adopting an efficient parameter optimization strategy for enhancing the predictive performance In 2022, Ebenezer Esenogho, et.al proposes an efficient approach to detect mastercard fraud employing a neural network ensemble classifier and also a hybrid data resampling method. The ensemble classifier is obtained employing a long short term memory (LSTM) neural network because the base learner within the adaptive boosting (AdaBoost) technique. Meanwhile, the hybrid resampling is achieved using the synthetic minority oversampling technique and edited nearest neighbor (SMOTE-ENN) method. The mastercard fraud detection model employs the synthetic minority oversampling technique and edited nearest neighbor (SMOTE-ENN) method to get a balanced dataset. An efficient approach to detect mastercard fraud employing a neural network ensemble classifier and a hybrid data resampling method. This method is demonstrated using publicly available real-world mastercard transaction datasets. Long short term memory (LSTM) neural network because the base learner within the adaptive boosting.(SMOTE-ENN) method is employed . an efficient feature engineering method via resampling of the imbalanced

data using the SMOTE-ENN technique. This method is critical for 2 reasons: the LSTM may be a robust algorithm for modelling sequential data. Secondly, the AdaBoost technique builds strong classifiers that are less likely to overfit, with lesser false-positive prediction More resampling techniques and improved feature selection techniques for enhanced classification performance. The SMOTE-ENN may be a hybrid resampling technique that performs both oversampling and undersampling of the info . It uses SMOTE,oversample the minority class samples and ENN to get rid of overlapping instances and it obtains superior performance. The dataset contains transactions by mastercard performed within two days in September 2013 by European clients. LSTM ensemble with SMOTE-ENN data resampling achieved a sensitivity of 0.996, a specificity of 0.998, and an AUC of 0.990, which is superior to the opposite benchmark algorithms and state-of-the-art methods. LSTM obtains the simplest performance compared to the opposite classifiers. Therefore, combining the SMOTE-ENN data resampling technique and therefore the boosted LSTM classifier is an efficient method in detecting fraud transactions in credit card.

In 2020, Huang Tingfe, et.al proposes e an oversampling method supported variational automatic coding (VAE), combined with classic deep learning techniques, to unravel this problem. The VAE method is employed to get an outsized amount of diverse cases from minority groups in an imbalanced dataset, which are then wont to train the classification network .It is tested on open credit card fraud dataset, which contains transactions conducted by European cardholders over two days in September 2013. Experimental results show that the VAE method performs better than synthetic minority oversampling techniques and also traditional deep neural network methods. In addition, it outperforms recent oversampling methods supported generative adversarial network (GAN) models..An oversampling method based on variational automatic coding (VAE), combined with classic deep learning technique is proposed in this system. Deep learning method of variational encoding is used (VAE) to generate positive data. The contribution of this paper is the documentation and testing of a new supervised oversampling method, which is desirable when the application data is characterized by a significant imbalance in class sizes and can be effectively applied to imbalanced classification problems. This method cannot be applied to the unsupervised environment. This model is not inferior to the baseline model in terms of recall index performance To improve the effectiveness of classification results, a framework for detecting credit card fraud will usually try to eliminate the gap between the two categories of cases in the data set. The framework adopted in this paper is to inject positive data obtained by oversampling into the original training set to obtain a hybrid training set. The gap between the two types of samples in the mixed training set is reduced, and then the classifier is trained using the mixed training set. The performance of the VAE model in precision, F-measure, recall rate and accuracy rate are all suitable for fraud detection, But the recall rate of this model is not increased while increasing the precision and F-measure. Advantages and disadvantages of credit card fraud detection methods are shown in Table 1.

Table 1:Advantages and disadvantages of credit card detection methods

Method	Advantages	Disadvantages
AdaBoost and majority voting method	Achieve good accuracy rates in order to detect the fraud in the credit cards.	The precision value achieved is less as compared to other algorithms.
SMOTE technique and Whale optimization algorithm	WOA improvises the convergence speed and reliability. The problem of class imbalance is overcome	Need good understanding of typical and abnormal behaviors for different type of fraud cases. SMOTE is not very practical for high dimensional data.
OLightGBM	Obtains higher Accuracy	Performance is less
variational automatic coding (VAE)	Can be effectively applied to imbalanced classification problems.	Cannot be applied to the unsupervised environment
LSTM neural network	Less likely to overfit, with lesser false-positive prediction	May suffer from the problem of incomplete or noisy data
Bayesian Network	High processing and detection speed/high accuracy (0.9737)	Excessive training need/ expensive
Support Vector Machines (SVM)	SVMs can be robust, even when the training sample has some bias,	Poor in process largedataset/expensive/has low speed of detection/ medium accuracy/lack of transparency of results

III. CONCLUSION

Credit card frauds are increasing day by day no matter the varied techniques developed for its detection. Fraudsters are so expert that they generate new ways for committing fraudulent transactions every day which demands constant innovation for its detection techniques. The fraud transaction detection is that the major issue of prediction thanks to a frequent and enormous number of transactions. . Credit card fraud generally happens when the cardboard was stolen for any of the unauthorized purposes or maybe when the fraudster uses the mastercard information for his use. In the present world, we face tons of

mastercard problems. To detect the fraudulent activities the credit card fraud detection system was introduced.In this review paper various techniques of Credit card fraud detection are reviewed. The mastercard has become the foremost popular mode of payment for both online also as regular purchase, in cases of fraud related to it also are rising.

IV.REFERENCE

[1] Kuldeep Randhawa, Chu Kiong Loo, ManjeevanSeera, Chee Peng Lim and Asoke K. Nandi, "Credit card fraud detection using AdaBoost and majority voting", IEEE Access, Vol.6, pp. 14277-14284, 2018.
[2] KhyatiChaudhary, JyotiYadav, BhawnaMallick, "A Review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications Vol.45, No.1, 2012.
[3] Huang Tingfei, Cheng Guangquan, and Huang Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection", IEEE ACCESS, Vol.8, 2020.
[4] Ebenezer Esenogho , Bomoiye Domor Mienye ,Theo G. Swart, Kehinde Aruleba, and George Obaido, "A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection", IEEEAccess,volume 10,2022.
[5] 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.
[6] 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.
[7] Altyeb Altaher Taha and D.Sharaf Jameel Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine", IEEE Access, Vol.8, 25579 – 25587, 2020.
[8] 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
[9] Sahayasakila.V" Credit Card Fraud Detection System using Smote Technique and Whale Optimization Algorithm", IJEAT, ISSN: 2249-8958, Volume-8 Issue-5, June 2019

Dr.L.C.Manikandan is working as Professor at Mangalam College of Engineering, Kottayam, Kerala INDIA. He has received his Ph.D. and M.Tech. Degree in Computer and Information Technology from Manonmaniam Sundaranar University, M.Sc., and B.Sc. degree in Computer Science from Bharathidasan and Manonmaniam Sundaranar University. He carries out research in Digital Image Processing, Video Surveillance and Video coding.

Reethu Elza Joseph is pursuing M.Tech Degree in Computer science and Engineering from Mangalam College of Engineering,Ettumanoor,. Kottayam, Kerala.