International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 10 Issue 04 April 2023

Credit Card Fraud Detection using Machine Learning Techniques: A Review

Rizwana Parveen[1], Dr. Harsh Lohiya[2]
Ph.d. Research Scholar, Department of Computer Science and Engineering[1]
Assistant Professor, Department of Computer Science and Engineering[2]
Sri Satya Sai University of Technology & Medical Sciences, Sehore (M.P.)[1, 2]

Abstract: *In recent years, the use of credit cards around the world has grown enormously. On-line transaction and e-commerce growing day by day with using of internet. Thus, the numbers of fraud cases have also increased, resulting in losses of thousands of dollars and rupees and other currency in worldwide. Therefore, securing all transactions using a payment card has become one of their top priorities. Credit card fraud comes from obtaining a physical card, or from using information of a cardholder like his credit card number, card verification code (CVC) or the expiration date. In this paper we present the feed forward neural network classifier for the Credit card fraud detection and improved the accuracy rate over the previous approach. In this paper we review multiple classification and machine learning techniques for prevention of such types of fraud also compare different authors works basis of their techniques, performance parameters and publication details.*

Keywords: *Credit card, Fraud detection, Artificial intelligence, Machine learning, Accuracy*.

1. INTRODUCTION

Recent advancements in electronic commerce and communication systems have significantly increased the use of credit cards for both online and regular transactions. However, there has been a steady rise in fraudulent credit card transactions, costing financial companies huge losses every year. In recent years there has been an increase in financial fraud due to the growth of technologies and paradigms such as the e-commerce and the financial technology (FinTech) sectors [1]. The evolution of these technologies has sparked an increase in the number of credit card transactions. As a result, there has been a rapid spike in the number financial fraud cases that involved credit cards.

Credit card Fraud occurs when an unauthorized or undesirable use of a credit card is made by a criminal. This happens when the credit card authentication details are stolen using different types of fraudulent techniques such as intercepting an e-commerce transaction or cloning an existing card [1]. Moreover, the impact of credit card fraud affects institutions such as card issuers, merchants, and small businesses. In 2015, the global loss due to credit card fraud was estimated at $21.84 Billion. In 2019, credit card losses reached $28.65 Billion. This represents an increase of $6.81 Billion in 4 years. Therefore, it is crucial to implement credit card fraud detection systems that can guarantee the integrity and security of all systems that are involved in fulfilling credit card transactions.

Both businesses and customers are losing money due to financial fraud in credit card transactions. E-payment is made enjoyable, smooth, handy, easy, and simple to use, due to online purchases and payment services; yet, we must not overlook the capital losses that accompany e-commerce. It opens the door to a new sort of deception for crooks. Organizations and banks use effective security solutions to deal with these concerns, but fraudsters vary their subtle approaches over time. As a result, improving detection and preventive strategies is critical. We have credit card transactions physically and virtually. In physical transactions, cards play a significant role in the purpose of transactions; we used to swipe the card and make transactions. On the other hand, In virtual transactions like a CNP situation, we need some essential details like cardholder name, CVV number, passwords to swipe a card for net banking. While

dealing with fraud we use two methods: fraud detection and fraud prevention. Fraud prevention is primarily concerned with the prevention of fraud cases, although it also monitors transactions and prohibits legal activities. Whereas in fraud detection, The primary purpose is to discern between real and fake transactions. Using past data, the user's habits and behavior were examined and verified to determine if the transaction/payment was fraudulent or not. When a system fails to prevent fraudulent conduct, fraud detection becomes the responsibility of the individual.

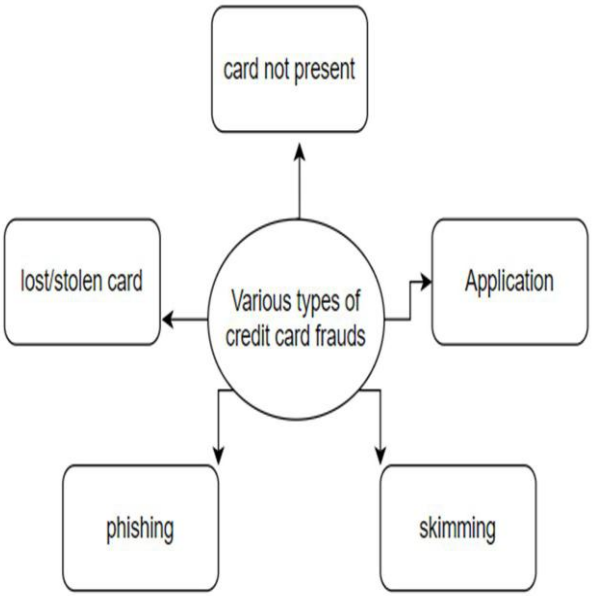

Figure 1: Different forms of credit card scams [4].

Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves [8].

The process of learning begins with observations or data, such as examples, direct experience, or instruction, in order to look for patterns in data and make better decisions in the future based on the examples that we provide. The primary aim is to allow the computers learn automatically without human intervention or assistance an adjust actions accordingly.

Deep learning is a subset of machine learning in artificial intelligence that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Deep learning is a technique used to generate face detection and recognize it for real or fake by using profile images and determine the differences between them.

Machine learning has revealed to be very rewarding at detecting and classification of fraud transactions. In another way, a great number of transaction reports may be used to train and validate fraud classifier. In spite of the fact that supervised learning has been tremendously successful in detecting fraudulent transactions, the progression of transactional fraud analysis technologies will never end. A Small enhancement in the classifier will save a company a noteworthy amount of money. The central objective of this study is to recognize the transactions in a dataset which contains fraud and non-fraudulent transactions by using Machine Learning algorithms such as Random Forest, Decision Tree, Logistic Regression, K-nearest neighbor, XgBoost algorithm. These algorithms are then evaluated to determine which performs best in identifying fraud transactions.

2. LITERATURE REVIEW

This section provides a literature review of previous researches that used ML techniques for credit card fraud detection.

[1] This framework was evaluated using the following ML methods: Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), Extreme Gradient Boosting (XGBoost), Decision Tree (DT), and Extra Tree (ET). These ML algorithms were coupled with the Adaptive Boosting (AdaBoost) technique to increase their quality of classification. The models were evaluated using the accuracy, the recall, the precision, the Matthews Correlation Coefficient (MCC), and the Area Under the Curve (AUC). Moreover, the proposed framework was implemented on a highly skewed synthetic credit card fraud dataset to further validate the results that were obtained in this research.

[2] This paper proposes an efficient approach to detect credit card fraud using a neural network ensemble classifier and a hybrid data re-sampling method. The ensemble classifier is obtained using a long short term memory (LSTM) neural network as the base learner in the adaptive boosting (AdaBoost) technique. Meanwhile, the hybrid re-sampling is achieved using the synthetic minority oversampling technique and edited nearest neighbor (SMOTE-ENN) method. The effectiveness of the proposed method is demonstrated using publicly available real-world credit card transaction datasets. The performance of the proposed approach is benchmarked against the following algorithms: support vector machine (SVM), multilayer perceptron (MLP), decision tree, traditional AdaBoost, and LSTM.

[3] This paper uses a self-paced ensemble neural network (SP-ENN) model to learn credit card fraud transactions by dividing the datasets with different hardness, then identifying these transactions by neural networks, and finally performing a comprehensive evaluation.

[4] This paper proposes a method, called autoencoder with probabilistic random forest (AE-PRF), for detecting credit card frauds. The proposed AE-PRF method first utilizes the autoencoder to extract features of low-dimensionality from credit card transaction data features of high-dimensionality. It then relies on the random forest, an ensemble learning mechanism using the bootstrap aggregating (bagging) concept, with probabilistic classification to classify data as fraudulent or normal. The credit card fraud detection (CCFD) dataset is applied to AE-PRF for performance evaluation and comparison. Experimental results show that the performance of AE-PRF does not vary much whether re-sampling schemes are applied to the dataset or not.

[5] Machine learning has opened up new tools for financial fraud detection. Using a sample of annotated transactions, a machine learning classification algorithm learns to detect frauds. With growing credit card transaction volumes and rising fraud percentages there is growing interest in finding appropriate machine learning classifiers for detection. However, fraud data sets are diverse and exhibit inconsistent characteristics. In this work, we evaluate sampling methods as a viable pre-processing mechanism to handle imbalance and propose a data-driven classifier selection strategy for characteristic highly imbalanced fraud detection data sets.

[6] In this paper, we explore different sampling techniques such as under-sampling, Synthetic Minority Oversampling Technique (SMOTE) and SMOTE-Tomek, to work on the unbalanced data. Classification models, such as k-Nearest Neighbour (KNN), logistic regression, random forest and Support Vector Machine (SVM), are trained on the sampled data to detect fraudulent credit card transactions. The performance of the various machine learning approaches are evaluated for its precision, recall and F1-score. The classification results obtained is promising and can be used for credit card fraud detection.

[7] In the manuscript an attempt has been made for finding the frauds in the credit card business by using the algorithms which adopted machine learning techniques. In this regard, two algorithms are used viz Fraud Detection in credit card using Decision Tree and Fraud Detection using Random Forest. The efficiency of the model can be decided by using some public data as sample. Then, an actual world credit card facts group from a financial institution is examined. Along with this, some clatter is supplemented to the data samples to auxiliary check the sturdiness of the systems. The significance of the methods used in the paper is the first method constructs a tree against the activities performed by the user and using this tree scams will be suspected. In the second method a user activity based forest will have constructed and using this forest an attempt will be made in identifying the suspect.

[8] In this study, we compare different machine learning algorithms to effectively and efficiently predict the legitimacy of financial transactions. The algorithms used in this study were: MLP Repressor, Random Forest Classifier, Complement NB, MLP Classifier, Gaussian NB, Bernoulli NB, LGBM Classifier, Ada Boost Classifier, K Neighbors Classifier, Logistic Regression, Bagging Classifier, Decision Tree Classifier and Deep Learning. The dataset was collected from Kaggle depository.

Table 1: The above table represents the comparative study for credit/debit card fraud detection.

Ref.	Classification techniques/ Machine learning/ Deep learning	Performance Parameter	Performance parameter Result Value	Publication year
[1]	Adaboost	Accuracy	98 %	2021
[3]	Ensemble neural Network	F1-Score	78 %	2022
[4]	Random Forest	Accuracy	98 %	2021
[5]	K-nearest Neighbor	F1-Score	78 %	2022
[6]	Random Forest	Accuracy	97 %	2022
[8]	Logistic Regression	Accuracy	96 %	2022
[9]	Genetic algorithm with ML	Accuracy	99 %	2022
[12]	Support Vector Machine	Accuracy	97 %	2022

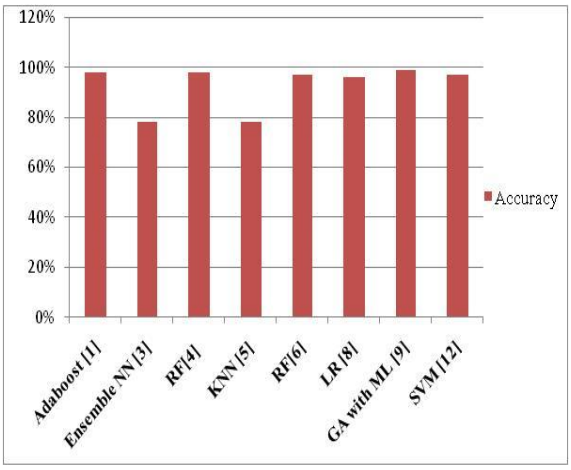

Figure 2: The above figure represents the comparative study for credit/debit card fraud detection with accuracy parameter.

3. PROPOSED MODEL

Artificial intelligence is an emerging technologies for now days applicable to various filed, health care is one of them, good health is primary requirement for nay human, in our country as we know that we are the second largest population in the world, to provide good health care infrastructure is very challenging task for them. Here the propose techniques is based on the machine learning which is subset of artificial intelligence techniques. The proposed work used the convolution neural network model for the prediction of diseases and improves the ratio of predicted performance evaluation value and overall health care system.

Credit card scam finding is while a trade receipts steps to preclude whipped cash, merchandises, or amenities attained via an illegal credit card business. Credit card scam can occur together by the customer or by somebody else. To avoid happening such frauds, there are many techniques invented. If such frauds happen, then how to track the misused transactions are also improvised. Among the many methods, machine learning algorithms make accurate predictions by extracting some underlying information features based on large data samples of different dimensions. To reduce the bias caused by unbalanced data and improve the accuracy of credit card detection, scholars have mainly focused on studied in several aspects, such as data re-sampling, cost-sensitive learning, unbalanced regression, ensemble learning algorithms, and deep learning algorithms. Machine learning techniques available for fraud detection can be separated as supervised, semi-supervised and unsupervised [5]. Supervised learning uses labeled fraud and normal transactions to learn a model that is able to identify frauds in new transactions (in case of classification) or provide a risk rating (in case of regression) so that investigators can prioritize on a subset of highly probable frauds. Unsupervised learning attempts to cluster transactions into fraud and normal based on similarities in features and does not require labeled data. Semi-supervised techniques use partly labeled data. Many machine learning techniques such as NN can be used in all modes, though supervised algorithms and models are most common.

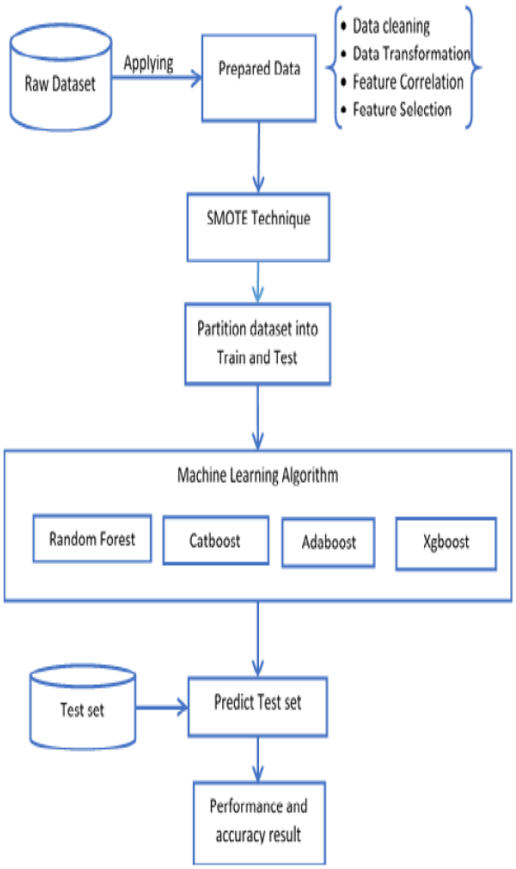

Figure 3: proposed system model to predict credit/debit card fraud detection using machine learning techniques.

4. CONCLUSION

Artificial intelligence is an emerging technologies for now days applicable to various filed, machine learning and deep learning is a subset of an artificial intelligence techniques, credit/debit card fraud detection of one of them, use of internet is increasing day by day and online or e-

commerce transactions are very use in now a days. In this work we review various machine learning technique applied for credit/debit card fraud detection and compare their performance parameter based result evaluation, in future work we implement a efficient model based on the machine learning techniques and improve the performance of existing system.

REFERENCES

[1] Emmanuel Ileberi, Yanxia Sun, Zenghui Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost", IEEE Access, 2021, pp. 165286-165295.

[2] Ebenezer Esenogho, Ibomoiye Domor Mienye, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection", IEEE Access, 2022, pp. 16400-16408.

[3] Wei Zhou, Xiaorui Xue, "Credit card fraud detection based on self-paced ensemble neural Network", ITCC 2022, pp. 92-99.

[4] Tzu-Hsuan Lin, Jehn-Ruey Jiang, "Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest", Mathematics 2021, pp. 1-16.

[5] Gayan K. Kulatilleke, "Credit Card Fraud Detection Classifier selection Strategy", 2022, pp. 1-17.

[6] Konduri Praveen Mahesh, Shaik Ashar Afrouz, "Detection of fraudulent credit card transactions: A comparative analysis of data sampling and classification techniques", Journal of Physics: Conference Series, 2021, pp. 1-9.

[7] Dileep M R, Navaneeth A V, "A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms", IEEE, 2021, pp. 1025-1028.

[8] Mosa M. M. Megdad, Bassem S. Abu-Nasser, " Fraudulent Financial Transactions Detection Using Machine Learning", International Journal of Academic Information Systems Research, 2022, pp. 30-39.

[9] Shubham Shah, Dhairya Shah, "Credit Card Fraud Detection System using Machine Learning", International Journal of Research in Engineering and Science, 2022, pp. 9-14.

[10] Appala Srinuvasu Muttipati, Sangeeta Viswanadham, "Recognizing Credit Card Fraud Using Machine Learning Methods", Turkish Journal of Computer and Mathematics Education, 2021, pp. 3271-3278.

[11] Akhil Songa, Sri Teja Kumar Reddy Tetali, Naga Sai Tanmai Raavi, "Credit Card Fraud Detection using Various Machine Learning Algorithms", International Journal for Research in Applied Science & Engineering Technology, 2022, pp. 1174-1185.

[12] G. Sudha Sadasivam, Mutyala Subrahmanyam and Dasaraju Himachalam, Bhanu Prasad Pinnamaneni, "Corporate governance fraud detection from annual reports using big data analytics", Int. J. Big Data Intelligence, Vol. 3, No. 1, 2016

[13] Ophir Gottlieb, Curt Salisbury, Howard Shek, Vishal Vaidyanathan, "Detecting Corporate Fraud: An Application of Machine Learning", December 15, 2006

[14] Renjith, S. Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. International Journal of Engineering Trends and Technology (2018).

[15] Roy, Abhimanyu, et al. "Deep learning detecting fraud in credit card transactions." 2018 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2018.

[16] Pumsirirat, Apapan, and Liu Yan. "Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine." International Journal of advanced computer science and applications 9.1 (2018): 18-25.