IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, March 2024

Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms

Miss. Shraddha S. Dhatrak[1], Miss. Janvi S. Patil[2], Miss. Riddhi B. Bodke[3],
Miss. Sadiya A. Pathan[4], Prof. M. P. Bhandakkar[5]
Department of Information Technology
Matoshri Aasarabai Polytechnic, Eklahare, Nashik, India

Abstract*: People can use credit cards for online transactions as it provides an efficient and easy-to-use facility. With the increase in usage of credit cards, the capacity of credit card misuse has also enhanced. Credit card frauds cause significant financial losses for both credit card holders and financial companies. In this research study, the main aim is to detect such frauds, including the accessibility of public data, high-class imbalance data, the changes in fraud nature, and high rates of false alarm. The relevant literature presents many machines learning based approaches for credit card detection, such as Extreme Learning Method, Decision Tree, Random Forest, Support Vector Machine, Logistic Regression and XG Boost. However, due to low accuracy, there is still a need to apply state of the art deep learning algorithms to reduce fraud losses. The main focus has been to apply the recent development of deep learning algorithms for this purpose. Comparative analysis of both machine learning and deep learning algorithms was performed to find efficient outcomes. The detailed empirical analysis is carried out using the European card benchmark dataset for fraud detection. A machine learning algorithm was first applied to the dataset, which improved the accuracy of detection of the frauds to some extent. Later, three architectures based on a convolutional neural network are applied to improve fraud detection performance. Further addition of layers further increased the accuracy of detection. A comprehensive empirical analysis has been carried out by applying variations in the number of hidden layers, epochs and applying the latest models. The evaluation of research work shows the improved results achieved, such as accuracy, f1-score, precision and AUC Curves having optimized values of 99.9%,85.71%,93%, and 98%, respectively. The proposed model outperforms the state-of-the-art machine learning and deep learning algorithms for credit card detection problems. In addition, we have performed experiments by balancing the data and applying deep learning algorithms to minimize the false negative rate. The proposed approaches can be implemented effectively for the real-world detection of credit card fraud.*

Keywords: Fraud detection, deep learning, machine learning, online fraud, credit card frauds, transaction data analysis

I. INTRODUCTION

Credit card fraud (CCF) is a type of identity theft in which someone other than the owner makes an unlawful transaction using a credit card or account details. A credit card that has been stolen, lost, or counterfeited might result in fraud. Card-not-present fraud, or the use of your credit card number in e-commerce transactions has also become increasingly common as a result of the increase in online shopping. Increased fraud, such as CCF, has resulted from the expansion of e-banking and several online payment environments, resulting in annual losses of billions of dollars. In this era of digital payments, CCF detection has become one of the most important goals. As a business owner, it cannot be disputed that the future is heading towards a cashless culture. As a result, typical payment methods will no longer be used in the future, and therefore they will not be helpful for expanding a business. Customers will not always visit the business with cash in their pockets. They are now placing a premium on debit and credit card payments. As a result,

DOI: 10.48175/IJARSCT-15741

companies will need to update their environment to ensure that they can take all types of payments. In the next years, this situation is expected to become much more severe.

In 2020, there were 393,207 cases of CCF out of approximately 1.4 million total reports of identity theft . CCF is now the second most prevalent sort of identity theft recorded as of this year, only following government documents and benefits fraud. In 2020, there were 365,597 incidences of fraud perpetrated using new credit card accounts. The number of identity theft complaints has climbed by 113% from 2019 to 2020, with credit card identity theft reports increasing by 44.6%. Payment card theft cost the global economy $ 24.26 billion last year. With 38.6% of reported card fraud losses in 2018, the United States is the most vulnerable country to credit theft.

As a result, financial institutions should prioritize equipping themselves with an automated fraud detection system. The goal of supervised CCF detection is to create a machine learning (ML) model based on existing transactional credit card payment data. The model should distinguish between fraudulent and nonfraudulent transactions, and use this information to decide whether an incoming transaction is fraudulent or not. The issue involves a variety of fundamental problems, including the system’s quick reaction time, cost sensitivity, and feature pre-processing. ML is a field of artificial intelligence that uses a computer to make predictions based on prior data trends.

ML models have been used in many studies to solve numerous challenges. Deep learning (DL) algorithms applied applications in computer network, intrusion detection, banking, insurance, mobile cellular networks, health care fraud detection, medical and malware detection, detection for video surveillance, location tracking, Android malware detection, home automation, and heart disease prediction. We explore the practical application of ML, particularly DL algorithms, to identify credit card thefts in the banking industry in this paper. For data categorisation challenges, the support vector machine (SVM) is a supervised ML technique. It is employed in a variety of domains, including image recognition , credit rating, and public safety. SVM can tackle linear and nonlinear binary classification problems, and it finds a hyperplane that separates the input data in the support vector, which is superior to other classifiers. Neural networks were the first method used to identify credit card theft in the pas. As a result, (DL), a branch of ML, is currently focused on DL approaches.

In recent years, deep learning approaches have received significant attention due to substantial and promising outcomes in various applications, such as computer vision, natural language processing, and voice. However, only a few studies have examined the application of deep neural networks in identifying CCF. . It uses a number of deep learning algorithms for detecting CCF. However, in this study, we choose the CNN model and its layers to determine if the original fraud is the normal transaction of qualified datasets. Some transactions are common in datasets that have been labelled fraudulent and demonstrate questionable transaction behaviour. As a result, we focus on supervised and unsupervised learning in this research paper.

The class imbalance is the problem in ML where the total number of a class of data (positive) is far less than the total number of another class of data (negative). The classification challenge of the unbalanced dataset has been the subject of several studies. An extensive collection of studies can provide several answers. Therefore, to the best of our knowledge, the problem of class imbalance has not yet been solved. We propose to alter the DL algorithm of the CNN model by adding the additional layers for features extraction and the classification of credit card transactions as fraudulent or otherwise. The top attributes from the prepared dataset are ranked. using feature selection techniques. After that, CCF is classified using several supervised machine-driven and deep learning models. this study, the main aim is to detect fraudulent transactions using credit cards with the help of ML algorithms and deep learning algorithms. This study makes the following contributions: Feature selection algorithms are used to rank the top features from the CCF transaction dataset, which help in class label predictions. The deep learning model is proposed by adding a number of additional layers that are then used to extract the features and classification from the credit card farad detection dataset.

II. LITERATURE REVIEW

Electronic commerce, also known as e-commerce, is the electronic purchasing and selling of goods and services through online platforms. Retail shops, internet banking, hotel reservations, money transfers, virtual goods, and so on are all activities that can be done through e-commerce. Each of these examples falls under one of the main three types of e-commerce: business to customer, customer to customer, and business to business

DOI: 10.48175/IJARSCT-15741

The dependency on e-commerce is continually increasing, as many classical businesses have begun to widen their targeted client base by going online. Over the years, from the most technological, such as security , databases and software-related concerns , to the least technological, such as marketing , company growth, and customer-related concerns .

The development of electronic commerce may be attributed to a combination of technological advancements and government regulatory quality improvements. The Internet has been critical to the growth of e-commerce platforms. It was brought to the globe in the 1960s, sparking a revolutionary change in this regime .[1]

In the 1990s, the development of the World Wide Web and web browsers was the next major stimulus to the e-commerce situation. Significant advancements in the field of e-commerce occurred in the 1970s, which greatly affected the industry and facilitated its expansion. The establishment of Amazon in 1994, an online store formerly used for book sales, was one of the fundamental events that were a result of technological innovation. Growing up, Jeff Bezos turned the service into one of the leading online selling platforms that shaped today's e-commerce. In 2020, Amazon's earnings are soaring by 200 percent .[2]

III. PURPOSE

Credit card fraud (CCF) is a type of identity theft in which someone other than the owner makes an unlawful transaction using a credit card or account details. A credit card that has been stolen, lost, or counterfeited might result in fraud. Card-not-present fraud, or the use of your credit card number in e-commerce transactions has also become increasingly common as a result of the increase in online shopping. Increased fraud, such as CCF, has resulted from the expansion of e-banking and several online payment environments, resulting in annual losses of billions of dollars.

IV. OBJECTIVE OF SYSTEM

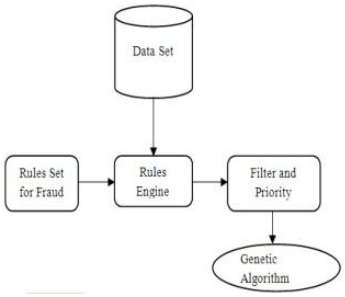
The specific objective of this project is to:

1. Develop a fraud detection system that can accurately identify and classify fraudulent and credit card transactions that are not fraudulent using machine learning techniques.
2. Implement a reliable authentication system that uses various authentication methods, such as face recognition authentication and one-time passwords verify the legitimacy of the credit card user.
3. Train the system on a dataset of past fraudulent activities to identify patterns and recognize similar fraudulent transactions, thereby increasing the accuracy of the fraud detection algorithm.
4. Increase the security of credit card transactions by detecting and preventing fraudulent activities before they occur, leading to significant savings for consumers and financial institutions.

V. PROPOSED SYSTEM

Credit card fraud (CCF) is a type of identity theft in which someone other than the owner makes an unlawful transaction using a credit card or account details. A credit card that has been stolen, lost, or counterfeited might result in fraud. Card-not-present fraud, or the use of your credit card number in e-commerce transactions has also become increasingly common as a result of the increase in online shopping. Increased fraud, such as CCF, has resulted from the expansion of e-banking and several online payment environments, resulting in annual losses of billions of dollars.

SYSTEM ARCHITECTURE



DOI: 10.48175/IJARSCT-15741

Advantages:

- Detection of anomalies faster.
- Better Predictions.
- Saves Time and Money

Disadvantages:

- Inacurate Prediction.
- Difficult to Interprit.
- Expensive

VI. CONCLUSION

CCF is an increasing threat to financial institutions. Fraudsters tend to constantly come up with new fraud methods. A robust classifier can handle the changing nature of fraud. Accurately predicting fraud cases and reducing false-positive cases is the foremost priority of a fraud detection system. The performance of ML methods varies for each individual business case. The type of input data is a dominant factor that drives different ML methods. For detecting CCF, the number of features, number of transactions, and correlation between the features are essential factors in determining the model's performance. DL methods, such as CNNs and their layers, are associated with the processing of text and the baseline model. Using these methods for the detection of credit cards yields better performance than traditional algorithms. Comparing all the algorithm performances side to side, the CNN with 20 layers and the baseline model is the top method with an accuracy of 99.72%. Numerous sampling techniques are used to increase the performance of existing examples, but they significantly decrease on the unseen data. The performance on unseen data increased as the class imbalance increased. Future work associated may explore the use of more state of art deep learning methods to improve the performance of the model proposed in this study.

VII. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the Computer Department and its staff for their continuous support. Our sincere thanks go to Principal of Matoshri Aasarabai Polytechnic, Eklahare, Nashik for his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported us throughout this project.

REFERENCES

[1] S. S. Lad, I. and A. C. Adamuthe, "Malware classification with improved convolutional neural network model", *Int. J. Comput.Netw. Inf. Secur.*, vol. 12, no. 6, pp. 30-43, Dec. 2021.

[2] J. Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szelński and R. Słowiński, "Auto loan fraud detection using dominance-based rough set approach versus machine learning methods", *Expert Syst. Appl.*, vol. 163, Jan. 2021.

[3] B. Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão and P. Bizarro, "Interleaved sequence RNNs for fraud detection", *Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp. 3101-3109, 2020.

[4] F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T. Akishita and O. Elshocht, "Adversarial attacks for tabular data: Application to fraud detection and imbalanced data", *arXiv:2101.08030*, 2021.

[5] H. Abdi and L. J. Williams, "Principal component analysis", *Wiley Interdiscipl. Rev. Comput. Statist.*, vol. 2, no. 4, pp. 433-459, Jul. 2010.

[6] V. Arora, R. S. Leekha, K. Lee and A. Kataria, "Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence", *Mobile Inf. Syst.*, vol. 2020, pp. 1-13, Oct. 2020.

[7] A. O. Balogun, S. Basri, S. J. Abdulkadir and A. S. Hashim, "Performance analysis of feature selection methods in software defect prediction: A search method approach", *Appl. Sci.*, vol. 9, no. 13, pp. 2764, Jul. 2019.

[8] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms", *Proc. Comput. Sci.*, vol. 165, pp. 631-641, Jan. 2019.

DOI: 10.48175/IJARSCT-15741

[9] Y. Abakarim, M. Lahby and A. Attioui, "An efficient real time model for credit card fraud detection based on deep learning", *Proc. 12th Int. Conf. Intell. Systems: Theories Appl.*, pp. 1-7, Oct. 2018.

[10] B. Bandaranayake, "Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia", *J. Cases Educ. Leadership*, vol. 17, no. 4, pp. 34-53, Dec. 2014.

DOI: 10.48175/IJARSCT-15741