International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Credit Card Fraud Detection using Deep Learning Techniques

R. Shailaj
2111CS020502
School of Engineering
MallaReddy University

P. Soumya
2111CS020533
School of Engineering
MallaReddy University

B. Soumya
2111CS020534
School of Engineering
MallaReddy University

Y. Sravya Reddy
2111CS020537
School of Engineering
MallaReddy University

P. Sravya Reddy
2111CS020538
School of Engineering
MallaReddy University

Dr P Anjaiah Professor,
Department of AIML
School of Engineering
MallaReddy University

1. ABSTRACT

People can use credit cards for online transactions as it provides an efficient and easy-to-usefacility.With the increase in usage of credit cards, the capacity of credit card misuse has also enhanced. Creditcard 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, dueto low accuracy, there is still a need to apply state of the art deep learning algorithms to reduce fraudlosses. 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.. 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.

2. 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.. 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

.

3. LITERATURE REVIEW

In the last decades Machine Learning achieved notable results in various areas of data processing and classification, which made the creation of real-time interactive and intelligent systems possible. The accuracy and precision of those systems depends not only on the correctness of the data, logically and chronologically, but also on the time the feed-backs are produced. This paper focuses on one of these systems which is a fraud detection system. In order to have a more accurate and precise fraud detection system, banks and financial institutions are investing more and more today in perfecting the algorithms and data analysis technologies used to identify and combat fraud. Therefore, many solutions and algorithms using machine learning have been proposed in literature to deal with this issue. However, comparison studies exploring Deep learning paradigms are scarce, and to our knowledge, the proposed works don't consider the importance of a Real-time approach for this type of problems. Thus, to cope with this problem we propose a live credit card fraud detection system based on a deep neural network technology. Our proposed model is based on an auto-encoder and permits to classify, in real-time, credit card transactions as legitimate or fraudulent. To test the effectiveness of our model, four different binary classification models are used as a comparison. The Benchmark shows promising results for our proposed model than existing solutions in terms of accuracy, recall and precision. Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence.

4. PROBLEM STATEMENT

The aim of this project is to develop a deep learning- based system for detecting credit card fraud accurately an efficien-tly. The system will analyze transaction data in real-time an flag potentially fraudulent activities for further investigation by financial institutions.The key objectives are Develop a Deep learning model capable of analyzing large volume transaction data to identify patterns indicative fraudul ent activity and Train the model using comprehensive dataset containing both legitimate and fraudulent transactions to ensure robus- tness and accuracy.

5. METHODOLOGY

Data Collection:Gather a comprehensive dataset of credit card transactions, including both legitimate and fraudulent examples. Ensure the dataset is diverse, representative, and contains sufficient instances of fraudulent activity. Include features such as transaction amount, timestamp , merchant category code (MCC), geographic location, etc., to capture relevant information for analysis.

Data Preprocessing: is critical step in building any machine learning model,especially for tasks like credit card fraud det ection where the data might be imbalanced and noisy.Here's a general outline of steps you might take for preproccesing data.Duplicates should be removed to avoid skewing the model.OuTliers may need special treatment depending on their impact on the model features often have different scales,which can impact the performance of certain machine learning algorithms. Scaling features to a similar range (eg;using techniques like Min-Max scaling or Standardization) can help algorithms coverage faster and perform better

6. EXPERIMENTAL RESULTS

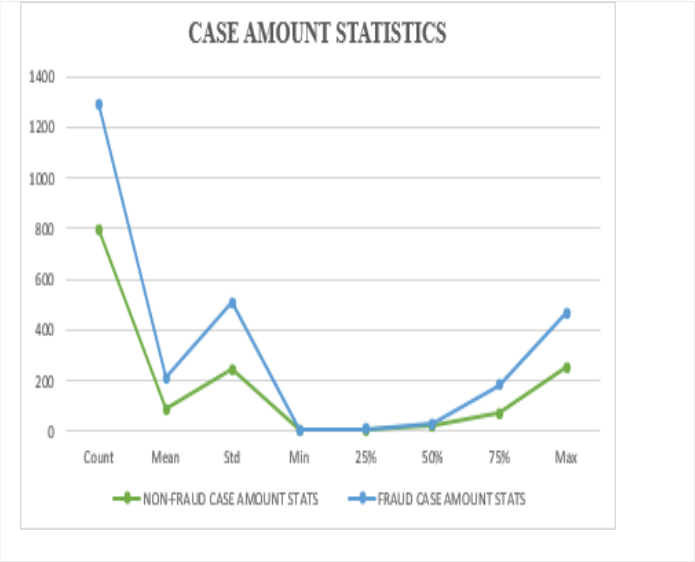

Fig 6.1 The case count statistics for fraud and non-fraud transactions

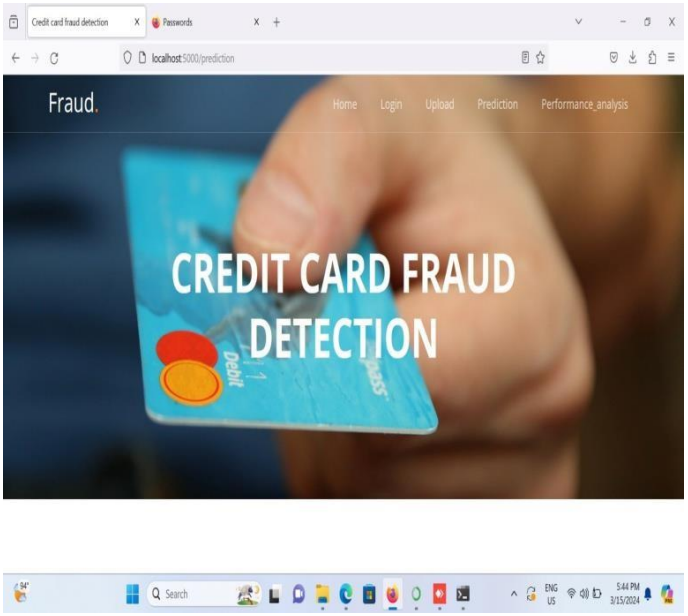

Fig 6.2 Output Screen

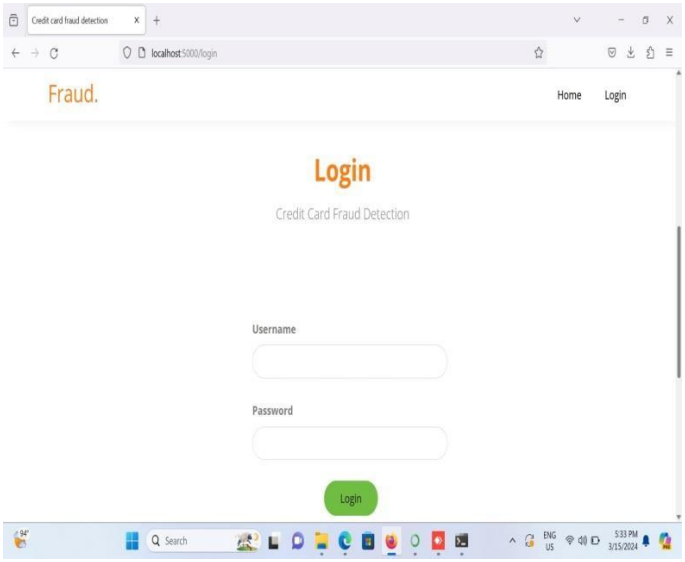

Fig 6.3 Output Screen

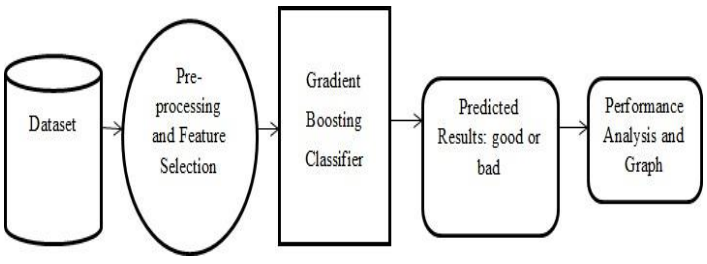

Fig 6.4 Architecture of Credit Card Fraud Detection

7. CONCLUSION

The prevention of credit card fraud is essential for increased credit card use. The financial losses suffered by financial institutions are significant and ongoing, and the detection of credit card fraud is becoming more challenging, thus it is crucial to create more efficient methods for doing so. Gradient Boosting Classifier Is used in this paper to suggest an intelligent method for Identifying fraud in credit card transactions. We performed a number of experiments utilising actual data.Performance analysis metrics were used to assess the performance of the suggested approach. According to the experimental findings, the suggested method out performed other machine learning algorithms and attained the maximum accuracy performance. The outcomes demonstrate that the suggested method outperforms alternative classifiers. The outcomes further emphasise the significance and benefit of implementing an effective parameter optimization strategy for boosting the suggested approach's predictive capabilities

8. FUTURE ENHANCEMENT

CCF is an increasing threat to financial institutions. Fraud-sters 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

9. REFERENCES

[1] Pantelimon, F.-V., Georgescu, T. M., & Posedaru, B.-S. (2020). The impact of mobile e-commerce on GDP: A comparative analysis between Romania and Germany and how covid-19 influences the e-

[2] Kaushik, D., Gupta, A., & Gupta, S. (2020). E-commerce security challenges: A Review. SSRN ElectronicJournal. https://doi.org/10.2139/ssrn.3595304.

[3] Khan, S. W. (2019). Cyber security issues and challenges in e-commerce. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3323741 .

[4] Kaabi, S., & Jallouli, R. (2019). Overview of E-commerce technologies, data analysis capabilities and marketing knowledge. Lecture Notes in BusinessInformation Processing, 183–193.https://doi.org/10.1007/978-3-030-30874-2_14.

[5] Katsikeas, C., Leonidou, L., & Zeriti, A. (2019). Revisiting international marketing strategy in a digital era. International Marketing Review, 37(3), 405–424. https://doi.org/10.1108/imr02-2019-0080.

[6] Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szelg, , and R. Słowiński, ‘‘Auto loan fraud detection using dominance-based rough set approach versus machine learning methods,’’ Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 1137

[7] Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão, and P. Bizarro, ‘‘Interleaved sequence RNNs for fraud detection,’’ in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2020, pp. 3101–3109, doi: 10.1145/3394486.3403361.

[8] S. S. Lad, I. Dept. of CSERajarambapu Institute of TechnologyRajaramnagarSangliMaharashtra, 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, doi: 10.5815/ijcnis.2020.06.03.

[9] V. N. Dornadula and S. Geetha, ‘‘Credit card fraud detection using machinelearning algorithms,’’ Proc. Comput. Sci., vol. 165, pp. 631–641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.