10.48047/jocaaa.2024.32.01.36

Blockchain fraud transaction for Fraud Detection in Banking Data

Dr.V. Anantha Krishna[1], Dodda Praneetha[2], A.Srinija[3], Yaragani Sri Harsha[4]

[1]Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

Email: Krishnaananthav@gmail.com

[2,3,4,]B.Tech Student, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India

ABSTRACT:

Credit cards rose to prominence as a payment mechanism as e-commerce services proliferated and technology developed, leading to a rise in the amount of banking transactions. High financial transaction costs are also necessary due to the notable rise in fraud. Consequently, identifying fraudulent activity has grown to be an interesting subject. In this paper, we examine how to regulate the relative weights of fraudulent and genuine transactions using class weight-tuning hyperparameters. Specifically, to optimise the hyperparameters while addressing real-world problems like imbalanced data, we use Bayesian optimisation. In order to enhance the performance associated with the Light GBM approach by taking into consideration the voting mechanism, we suggest using XG Boost and Cat Boost in addition to weight-tuning as an additional pre-process for imbalanced data. Finally, to further enhance performance, we fine-tune the hyperparameters (especially our suggested weight-tuning one) using deep learning. To verify the suggested approaches, we do a few tests using actual data. Recall-precision measures are used alongside to the conventional ROC-AUC to better cover imbalanced datasets. A 5-fold cross-validation technique is used to assess Cat Boost, Light GBM, or XG Boost independently. Moreover, the integrated algorithms' performance is evaluated using the majority vote ensemble learning approach. As per the findings, Light GBM and XG Boost meet the optimal level requirements of ROC-AUC = 0.95, accuracy 0.79, remember 0.80, F1 rating 0.79, and MCC 0.79. Through the use of deep neural networks and the Bayesian optimisation technique, we are also able to get the following results: ROC-AUC = 0.94,

10.48047/jocaaa.2024.32.01.36

accuracy = 0.80, recall = 0.82, which is F1 rating = 0.81, and MCC = 0.81. When compared to the state-of-the-art techniques, this is a major advance.

INTRODUCTION

The growth of financial institutions plus the growing popularity overall web-based e-commerce have resulted in a notable rise in the number of financial transactions in recent years. Fraud detection has never been difficult, and fraudulent transactions are becoming an increasingly common issue in online banking. The pattern of card fraud has constantly evolved along with the evolution of credit cards. Fraud with credit cards has always been updated, and scammers do their hardest to make it seem genuine. Con artists do their hardest to make it seem It was genuine that Zhan Bu, the assistant editor, oversaw the manuscript's examination and gave the go-ahead for publishing. They keep stimulating these systems and attempt to understand how systems for detecting fraud operate, which makes fraud detection more difficult. That's why scientists are always looking for new approaches or ways to make the current ones work better. Fraudsters often use flaws in commercial applications' safety, control, and monitoring systems to forward their agendas. Nonetheless, technology may be used as a weapon to stop fraud. It's critical to identify fraud as soon as it occurs in order to stop any more fraud from happening. Fraud is defined as dishonest or illegal deceit used to bring about monetary or private benefit. Card fraud is associated with the unauthorised use of information from credit cards. Volume 11, 3034, 2023 For purchases made either digitally or physically, refer to IEEE Transactions on Machine Learning and Applications, Volume 11, Issue Date January 20, 2023. Fraud may occur with digital transactions since cardholders often submit the card number, expiry date, or card verification number over the phone or online. To minimise losses caused by fraud, two strategies fraud detection and prevention can be used. The proactive strategy of fraud prevention prevents fraud from occurring in the initial place. On the other side, when a fraudster tries to complete a fraudulent transaction, fraud detection is required. Data is categorised as either legal or fraudulent in order to aid in the identification of fraud in the financial industry. It is either difficult or very time-consuming to manually evaluate and identify patterns of fraudulent transactions due to the volume of financial data and the datasets that include a lot of

10.48047/jocaaa.2024.32.01.36

transaction data. For this reason, algorithms based on machine learning are essential to the identification and forecasting of fraud. Massive data sets with fraud detection can be handled more effectively thanks to machine learning techniques and powerful processing capabilities. Real-time issues may also be quickly and effectively solved with the use of deep learning and machine learning techniques. In this article, we propose an effective method to identify credit card fraud, which has been tested on publicly accessible datasets and makes use of deep learning, hyperparameter settings, majority voting paired methods, optimised computations Light GBM, which the XG Boost the Cat Boost, or logistic regression separately. More suspicious transactions should be detected by a perfect fraud detection system, and the precision of such cases should be high, meaning that all results ought to be correctly detected, thereby fostering customer trust in the bank and preventing losses through incorrect detection.

RELATED WORK

Global versus local outliers in a multifaceted strategy to bitcoins fraud detection

In the world of Bitcoin, interpreting aberrant financial conduct might get obscured due to a lack of class markers. A complex method is suggested to comprehend fraud in the most recent financial sector growth. This study describes Bitcoin fraud using reduced k-means and kid-trees utilising global and local viewpoints. Random forests, maximum likelihood-based, and boosted binary regression models are used to further explore the two spheres. The global outlier perspective performs better than the local viewpoint, despite both viewpoints demonstrating strong performance, with the exception of random forest, which displays almost flawless outcomes from both dimensions.

Fraud detection and risk assessment in an automated insurance system using a safe AI-driven architecture

One of the businesses that is expanding the quickest is the private insurance industry. The last ten years have seen amazing changes driven by this quick expansion. The majority of high-value assets, including cars, jewels, health and life insurance, and residences, are covered by insurance

10.48047/jocaaa.2024.32.01.36

products these days. In order to maximise profit while managing their clients' claims, insurance firms are at the forefront of using cutting-edge operations, procedures, and mathematical models. Time-consuming and imprecise are the hallmarks of traditional approaches that only rely on human-in-the-loop models. In this work, we create an automated and secure insurance system architecture that decreases human involvement, safeguards insurance operations, warns and educates about high-risk clients, identifies fraudulent claims, and lessens financial loss for the insurance industry. We propose to use the extreme gradient boost (XG Boost) artificial intelligence algorithm for the previously mentioned insurance products to contrast its performances to those of other modern algorithms following presenting the a blockchain-based framework that allows secure data and transaction sharing among various interacting agents inside the insurance network. Based on an automobile insurance dataset, the acquired findings show that the XG boost outperforms other current learning algorithms in terms of performance. For example, it achieves 7% more accuracy in identifying fraudulent claims than decision tree models. Based on an automobile insurance dataset, the acquired findings show that the XG boost outperforms other current learning algorithms in terms of performance. For example, it achieves 7% more accuracy in identifying fraudulent claims than decision tree models. We also demonstrate how our online learning solution beats another current state-of-the-art algorithm in handling real-time changes of the insurance network. In order to build and simulate the blockchain-based artificial intelligence framework, we finally link the created machine learning modules to the Hyperledger fabric composer.

A blockchain-based structure for insurance procedures

In order to facilitate the execution of transactions in insurance procedures, we create a distributed platform that uses bitcoin as a system service. The insurance business primarily relies on several procedures between parties involved in transactions to initiate, manage, and close a wide range of policies. Timeliness in processing transactions, settling payments, and safeguarding process execution security are crucial considerations. Blockchain technology is being used more and more in

10.48047/jocaaa.2024.32.01.36

various FinTech systems to meet efficiency and security needs. Originally, it was intended to serve as an irreversible distributed record for identifying cryptocurrency double spending. Understanding the fundamental company procedures in great detail is necessary for applying blockchain to FinTech processing. Smart contracts are used to enable automatic interactions among the blockchain and current transaction systems. The primary objective of this article is to provide a blockchain-enabled platform that facilitates the efficient processing of insurance-related transactions. Using Hyperledger Fabric, an open-source permissioned blockchain design framework, an experimental prototype is created. We describe key design criteria and accompanying design proposals, and we use smart contracts to encode different insurance procedures. Numerous tests were carried out to evaluate the security and functionality of our framework.

A fraud detection platform built on the blockchain.

The phrases "corruption" and "fraud" are now often used in relation to international government agencies. If it is not addressed, it often results in a number of social and economic issues. Any nation's progress is negatively impacted by a rise in its level of corruption. Officers who are avaricious pocket the public monies or funds designated for the wellbeing of the people. With blockchain technology, this study project seeks to lessen fraud and corruption. We worked on a typical scenario to develop our framework, where a government runs a number of programmes for the benefit of the general public, and the money are distributed via an intricate structure of government that passes through a number of entities. Corruption in numerous systems at different levels may be caused by a lack of openness, improper administration of government documents, and delays in the verification process. Blockchain is a more powerful technology that may aid in combating corruption within an experimental generic situation since it is a transparent, immutable, and decentralised approach.

METHODOLOGY

To implement this paper author has used dataset which contains user and transaction details and then we extracted all transaction details and then process dataset to normalize

10.48047/jocaaa.2024.32.01.36

value and then replace missing values with 0 and then remove all non-numeric data.

1.upload & preprocess dataset: By using this module used to upload and read dataset and then remove missing values

2.generate Train& test model: By using this module we can generate Train and test the model.

3.run logistic algorithm: By using this module we can run logistic algorithm

4.run MLP algorithm: By using this module we can run MLP algorithm

5.run naive bayes algorithm: By using this module we can run naïve bayes algorithm

6.run ad boost algorithm: By using this module we can run ad boost algorithm

7.run decision tree algorithm: By using this module we can run decision tree algorithm

8.run sum algorithm: By using this module we can run SVM algorithm

9.run random forest algorithm: By using this module we can run random forest algorithm

10.run deep Network algorithm: By using this module we can run deep network algorithm

11.comparision graph: By using this module we can plot comparison graph.

RESULT AND DISCUSSION

In above screen click on 'Upload & Preprocess Dataset' button to upload and read dataset and then remove missing values

In above screen we can see all data converted to numeric format and we can see total records found in dataset with total columns and then split dataset into train and test and now train and test data is ready and

10.48047/jocaaa.2024.32.01.36

now click on each button to run all algorithms and get below output

In above screen we can see the accuracy, precision, recall and FSCORE of each algorithm in graph and tabular format and in all algorithms Random Forest giving better result

CONCLUSION

Every paper listed above has provided an overview of the technology of blockchain and its distinguishing features. Moreover, they examine cutting-edge methods for identifying online fraud as well as intrusions, point out specific fraudulent and malicious acts that blockchain systems can successfully stop, and offer suggestions for tactically fending off a range of attacks that blockchain technology may be susceptible to. It may be possible to detect fraud and breaches in blockchain-based transactions using already-existing machines learning and data-mining technologies. Through behavioural trend detection, transaction history tracking, and profile creation, guided machine learning techniques like as support vector machines, deep learning neural networks, or Bayesian believe networks may be able to identify unusual activity. The issue of video fraud persists despite technological advancements, and there is now no tangible remedy for it. Further study is necessary to advance technology and associated defence strategies.

REFERENCES

[1] Joshi, P., Kumar, S., Kumar, D., & Singh, A. K. (2019, September). A blockchain based framework for fraud detection. In 2019 Conference on Next Generation Computing Applications (Next Comp) (pp. 1-5). IEEE.

[2] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1), 1-10.

[3] Dhiran, A., Kumar, D., & Arora, A. (2020, July). Video Fraud Detection using Blockchain. In 2020 Second International

10.48047/jocaaa.2024.32.01.36

Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 102-107). IEEE.

[4] Nerurkar P, Bharu S, Patel D, Ludi nard R, Bushel Y, Kumari S. Supervised learning model for identifying illegal activities in Bitcoin. Appl Intel. 2020;209(1):1- 20.

[5] Ostapowicz, M., & Żbikowski, K. (2020, January). Detecting fraudulent accounts on blockchain: a supervised approach. In International Conference on Web Information Systems Engineering (pp. 18-31). Springer, Cham.

[6] Rekwar, M., Mazumdar, S., Raj, S., Gupta, S. S., Chattopadhyay, A., & Lam, K. Y. (2018, February). A blockchain framework for insurance processes. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-4). IEEE.

[7] Dheeb, N., Ghazali, H., Besbes, H., & Massoud, Y. (2020). A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement. IEEE Access, 8, 58546-58558.

[8] Shanmuga Priya P and Swetha N, "Online Certificate Validation using Blockchain", Special Issue Published in Int. Jnl. Of Advanced Networking and Applications (IJANA).

[9] Monam, P. M., Marinate, V., & Twala, B. (2016, December). A multifaceted approach to bitcoin fraud detection: Global and local outliers. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 188-194). IEEE.

[10] Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 1-9. [11] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[12] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[13] K. Elissa, "Title of paper if known," unpublished.