ISSN: 2249-7196
IJMRR/Sep. 2024/ Volume 14/Issue 7/148-155
Dr.K.Smitha / International Journal of Management Research & Review

BLOCKCHAIN FRAUD TRANSACTION FOR FRAUD DETECTION IN BANKING DATA

Dr.K.Smitha [1], Chenna Sathvika [2], Adlapur Supriya [3], Bashetti Divya [4]

[1] Associate Professor, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad

[2], [3], [4] Student, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad

ABSTRACT: *The use of credit cards for purchases and other financial activities grew in tandem with the proliferation of e-commerce services and other technological advancements. High bank transaction fees are necessary due to the evident rise in fraud. Therefore, identifying fraudulent activity has become an intriguing subject. To regulate the relative weights of fake and legitimate transactions, this study investigates how category weight-tuning hyperparameters might be used. In order to solve real-world problems like imbalanced data and optimize the hyper parameter values, we use Bayesian optimization. If we want to make the Light GBM method work better by taking the voting mechanism into consideration, we need pre-process imbalanced data using X G Boost and Cat Booster on top of weight-tuning. They use deep learning to refine the hyperparameters, namely the one we suggest—weight-tuning—to further optimize performance. To ensure the suggested approaches work, we conduct several trials using actual data. In addition to the classic ROC-AUC, recall-precision measurements are used to better cover imbalanced datasets. Different versions of XG Boost, Light GBM, and Cat Boost are tested independently via a 5-fold cross-validation procedure. Using an overwhelming ballot ensemble learning approach, we may evaluate the coupled algorithms' performance even further. Light GBM & XG Boost meet the optimal level requirements with ROC-AUC = 0.95, preciseness 0.79, recall 0.80, F1 rated 0.79, and MCC 0.79– according to the findings. Employing deep neural networks in conjunction with the Bayesian optimization method also yields the following results: With an F1 rating of 0.81, an MCC of 0.81, an accuracy of 0.80, and a recall of 0.82, the ROC-AUC is 0.94. Compare this to the status quo, and you'll see a huge improvement.*

INTRODUCTION

The growth of banking institutions and the widespread adoption of online shopping have both contributed to a dramatic uptick in the number of monetary transactions in recent years. Identity theft is becoming more of an issue in online banking, and it's simpler than ever to spot fraudulent activities. There is a strong correlation between the pattern of card fraud and the growth of credit cards. The methods used to commit credit card fraud are constantly developing, and con artists will stop at nothing to make their schemes seem legitimate. Con artists will stop at nothing to make things seem as The work was reviewed and accepted for publication by Zhan Bu, the interim editor. Their persistent efforts to understand these systems' inner workings and stimulate them further make fraud detection more difficult. As a result, researchers are continually on the lookout for fresh concepts or ways to enhance current ones. Criminals often take advantage of loopholes in commercial programs' security, control, and tracking systems to accomplish their goals. On the other hand, technology may be used to fight fraud. To stop more fraud from happening, it is necessary to identify it quickly as it does. Fraud is defined as the use of dishonest or illegal means to get financial or personal benefit. The unauthorized use of data from credit cards is associated with credit card fraud. Pages 3034–2023, volume 11. Volume 11, Issue Date 2023, published in IEEE Transactions on Machine Learning (for both online and offline purchasing), is the place to look. Because cardholder often provide their full card details (number, expiry date, and verification code) over the phone or online, digital transactions pose a risk of fraud. Losses caused by fraud may be mitigated via the deployment of two strategies: fraud detection and prevention. The proactive method of preventing fraud is to stop it before it starts. On the other side, when con artists try to complete a fraudulent transaction, fraud detection becomes critical. The banking industry uses data classifications such as "fraudulent" or "legitimate" to aid in the detection of fraud. Examining datasets that include massive volumes of transaction data and financial information by hand to find trends in fraudulent transactions is either extremely difficult or takes an inordinate amount of time. Because of this, algorithms that rely on machine learning are essential for spotting and predicting instances of fraud. Machine learning techniques and powerful processing capacities allow for more effective management of

large data sets associated with fraud detection. Rapid and effective resolution of real-time issues is also possible with the application of deep learning and machine learning techniques. We provide a method for detecting credit card fraud that relies only on logistic regression, paired majority voting procedures, and optimized mathematical operations in this paper. Hyperparameters, deep learning, and light GBM are all part of the XG Boost, which is also known as Cat Boost. The method has been tested using datasets that are accessible to the public. If it were perfect, a fraud detection system would have a far higher rate of success in spotting questionable transactions. Customers will have more faith in the banking institution and less losses will occur from false positives if all outcomes are correctly recognized.

RELATED WORK

Outliers on a global vs. a local scale in a multi-factor model for detecting bitcoin fraud

Problems with evaluating suspicious financial activity may arise in the Bitcoin ecosystem due to the lack of class indications. A more nuanced strategy is suggested for comprehending fraud in the financial industry's recent growth. This study employs kid-trees and reduced k-Means to characterize Bitcoin fraud from both a global and local standpoint. Additional research into the two areas is conducted via the use of random forests, maximum likelihood-based, and boosted binary regression models. The random forest view demonstrates almost flawless outcomes from both dimensions, yet even with that, the global anomalous viewpoint performs better than the local one.

Evaluation of potential dangers and identification of fraudulent activity in an AI-powered, fully automated insurance system

One area that is expanding at a rapid pace is the private insurance market. We have seen tremendous change in the last decade as a result of this quick progress. Nowadays, insurance protects the majority of high-value assets, including houses, cars, jewelry, health, life, and other policies. When it comes to managing claims for consumers and maximising profits, insurance

firms were early adopters of cutting-edge operations, procedures, and mathematical models. Traditional approaches that rely only on human-in-the-loop models are known for their inaccuracy and tediousness. The goal of our work is to develop a safe and secure industrial system architecture that can run on the cloud. This system will safeguard insurance operations, identify high-risk consumers, prevent fraudulent claims, and minimize financial losses. We suggest using the robust severe a slope encourage (XG Boost) manufactured brain method for the previously mentioned insurance products after introducing a blockchain-based framework that enables safe particular data and transaction sharing among numerous interconnected agents inside the insurance network. This will allow us to contrast its abilities to those of other modern algorithms. According on the findings obtained using an automobile insurance dataset, the XG boost outperforms other current neural networks. For example, it achieves a 7% higher rate of success than decision tree models in identifying false claims. Based on an auto insurance dataset, the findings show the XG boost outperforms other current machine learning methods. For example, it achieves a 7% higher rate of success than decision tree models in identifying false claims. We also demonstrate that our online learning method beats another state-of-the-art algorithm while handling instantaneous changes to the insurance network. Finally, to build and simulate the AI system based on blockchain technology, we implement the Hyperledger Textiles Composer to link the created neural network modules.

An insurance framework powered by blockchain technology

To facilitate the execution of insurance-related transactions, we build a decentralized platform that employs bitcoin as a system service. The insurance sector relies on many procedures comprising entities engaged in transactions to originate, manage, and finish a wide range of policies. Important considerations include ensuring secure process execution, completing transactions quickly, and making payments on time. Bitcoin software is being integrated into an increasing variety of FinTech systems to meet efficiency and security needs. Its original intent was to prevent cryptocurrency double spending by serving as a decentralized, irreversible record of all transactions. To use blockchain technology to financial technology processing, one must have an in-depth familiarity with the fundamental operations of the company. Smart contracts provide for the possibility of automated communication between the blockchain and preexisting

transaction systems. The primary objective of this article is to provide a blockchain-enabled system that facilitates efficient processing of underlying transactions pertaining to insurance. Hyperledger Fabric, a permissioned blockchain architectural framework that is publicly accessible, is used to construct the test version. We use smart contracts to encode many insurance processes and lay out critical design criteria and associated design ideas. We put our framework through its paces in order to ensure its functionality and security.

A technique for detecting fraud that is built on the blockchain.

Words like "fraud" and "corruption" are tossed about quite a bit these days when discussing foreign countries. When not addressed, it may cause a cascade of problems in both society and the economy. Any nation's progress is stunted when corruption levels rise. Officers with plenty of personal wealth steal from the public coffers. Using blockchain technology, this study hopes to lessen instances of fraud and corruption. The typical scenario whereby a government oversees several public programs and disperses monies via a network of interdependent government entities was the primary inspiration for our design. Corruption at different levels may result from inadequate administration of official paperwork, a lack of openness, and bottlenecks in document verification. In an experimental broad scenario, blockchain technology may aid the battle against corruption because to its decentralised, transparent, and immutable nature.

METHODOLOGY

The author used a data set that included information on users and their transactions to carry out this job. We cleaned up the dataset by removing non-numerical information and replacing missing values with zeroes once we had all of the deal details.

1. Read and upload datasets: Prior to removing missing values, this module is used to read and upload datasets.
2. Build a test and train model: This module allows us to build, train, and evaluate a framework.
3. run the logistic regression This module allows us to run the logistic algorithm.
4. we can use this module to perform the MLP algorithm.

5. This module enables us to run the naïve bayes algorithm, which is Execute the App Boost Program

6. With this module, we can run the AdBoost algorithm.

7. we may use this module to perform the decision tree algorithm.

8. Apply the sum algorithm: This module allows us to run the support vector machine method.

9. You may apply the method known as random forest with this module, which brings us

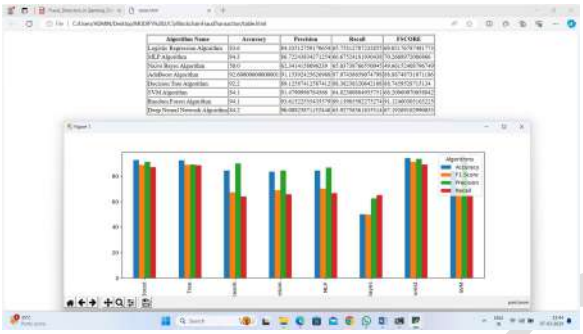
10. In this module, we may execute the deep network algorithm, which brings us

11. Graph of comparisons: We can make a chart of comparisons using this module.

RESULT AND DISCUSSION

To upload, read, and then delete missing values from the dataset, click the "Upload & Preprocess Dataset" button on the above page.

The result above displays all of the data in numeric format, along with the total number of records and total number of columns in the dataset. The dataset was then divided into train and test, and both the test and training data are now available. Click on every option to execute each method and get the results shown below.



The aforementioned panel displays each algorithm's accuracy, precision, recall, and FSCORE in a graph and tabular manner. Random Forest produces superior results across all methods.

CONCLUSION

In each of those articles, you can get a summary of blockchain technology along with some of its peculiarities. Furthermore, they examine cutting-edge methods for detecting cyber intrusions and fraud, point out specific types of fraud and malicious activity that systems powered by blockchain can successfully prevent, and offer guidance on ways to strategically defend against a range of threats that blockchain technology could face. Machine learning and data mining tools that are now available may help find instances of fraud or security breaches in blockchain-based transactions. Through the use of behavioural trend detection, transaction history tracking, and profile development, guided machine learning methods like assistance vector algorithms, deep retraining neural network systems, or Bayes belief systems may be able to identify anomalous activity. There is currently no workable answer to the issue of video fraud, despite technological advancements. To advance technology and associated defense methods, further study is needed.

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 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.