iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59690

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

A Token-based Approach to Detect Fraud in Ethereum Transactions

Praniket Walavalkar[1], Ansh Dasrapuria[2], Meghna Sarda[3], Lynette D'mello[4]
[1, 2, 3, 4]*Department of Computer Engineering, University of Mumbai*

Abstract: ***As a consequence of mass unemployment being the byproduct of COVID-19, people around the world discovered investment in cryptocurrency as a means to tackle their declining financial condition. Subsequently, the prominence of Ethereum as a platform for crypto transactions also gave rise to fraudulent transactions. The need to detect these frauds exists even today. This study proposes a token-based approach to detect fraud in Ethereum transactions incorporating the ERC20 standard, by employing machine learning techniques. After cleaning and preprocessing of the dataset, the transaction data was fed to Random Forest (RF), AdaBoost, Extra Trees (ET), Gradient Boosting (GB) and Extreme Gradient Boosting (XGB) classifiers in search of the most suitable model for fraud detection. Meticulous evaluation revealed that RF, ET and XGB classifiers yielded the highest accuracy of 95%. The proposed token-based approach hence presents a novel and efficient solution for fraud detection, with room for improvement and scalability.***
Keywords: Ethereum, Fraud Detection, Machine Learning, Token-Based, Transactions, ERC20

I. INTRODUCTION

Ethereum is an open-source, decentralized blockchain platform that enables the development of decentralized apps and the execution of smart contracts. Nevertheless, because of its transparency and anonymity, it is susceptible to fraud and illicit activities. Machine learning finds a major application in the field of fraud detection. Machine learning models may learn from patterns in regular behavior. They can swiftly adapt to deviations in regular activity and discover patterns of fraudulent transactions. Using cutting-edge technologies like machine learning, this project seeks to proactively identify fraudulent activity on the Ethereum network.

The use of smart contracts has been more widespread in recent times due to their ability to automate certain processes, do away with the need for middlemen, and guarantee the reliable execution of agreements. As with any new technology, smart contracts have led to the emergence of a new kind of fraud called smart contract scams. One such type of smart contract scams is token sales scams that aims to deceive investors into transferring cryptocurrency to the scammers' wallets by giving them the chance to buy a new token that is predicted to appreciate in value over time. Investors lose all their money in this kind of fraud, where the token is often useless.

By using token-related data based on the ERC-20 standard for smart contracts, this research proposes implementing a distinctive approach for detecting fraud during transactions. The primary objective is to detect fraud even in relatively secure Ethereum transactions that take place using smart contracts and the ERC20 standard. The novel yet efficient approach suggested in this study offers an adequate solution to the growing loopholes in generic fraud detection mechanisms. The reliability of the ERC20 standard can be optimized by means of this approach to make transactions safer for all users.

The structure of this paper is as follows:

Section 1 introduces the general idea and purpose behind this study, followed by the thorough review of existing research in Section 2. A comprehensive explanation and walkthrough of the entire methodology is provided in Section 3 whereas the results of the implemented techniques have been evaluated and explained in Section 4 of the paper. Section 5 summarizes the entire study in a concise manner and suggests possible improvements and applications in the future.

II. LITERATURE SURVEY

Elmougy, Y., & Manzi, O. [1] concentrate on detecting fraudulent accounts and transactions by locating abnormalities in the Ethereum and Bitcoin transaction networks. Meta data for a large number of accounts is derived by utilising GPU-accelerated machine learning models. Models trained on the Bitcoin dataset reach 96.9% accuracy and 0.987 recall while on the other hand, they achieved an accuracy of 80.2% and 0.835 recall on the Ethereum dataset.

©IJRASET: All Rights are Reserved

Apart from the known smart contracts based on Ponzi Scheme, Jung, E., et al. [2] created a dataset of perhaps benign Ethereum smart contracts and developed features using the transactions and generated code. J48, Random Forest, and Stochastic Gradient Boosting are three machine learning models that are assessed using metrics including F1 score, recall, and accuracy. Using the previously described models, a behaviour-based model, a full-feature model, and a 0-day model for early detection are built. The entire feature model yielded the best results, with 0.97 f1 score, 0.97 recall, and 0.99 accuracy.

Hou, W., et al. [3] propose the use of Graph Convolutional Network (GCN) with Conditional Random Field (CRF) as an efficient phishing scams detection method. In order to create transaction graphs, accounts are first processed alongside their neighbors for transaction records. Since portrait information is lacking, DeepWalk is employed to supply each node with its initial features.

Huang, B., et al. [4] focus on a method named HTSGCN for Ethereum account phishing fraud detection. The technique fully utilizes the type and direction information present in transactions since it is based on heterogeneous transaction subnets. According to experimental results, HTSGCN is more effective than earlier research based on homogenous networks at identifying phishing accounts. The HTSGCN method produced optimal outcomes, with a f1 score of 0.85, recall of 0.84, and precision of 0.86.

Roy, K. S., et al. [5] provide a deep learning based fraud detection model for the Ethereum blockchain transaction data. To categorize the fraudulent behaviors occurring within the system, a deep learning-based detection model is constructed in conjunction with a trustworthy dataset in this domain. A dense unit and a Long Short-Term Memory (LSTM) unit make up the suggested classification model, which is used to identify fraudulent transactions. Based on the experimental data, it is seen that the suggested model outperforms existing state-of-the-art methods with a detection accuracy of 99.59%.

Tan, R., et al. [6] suggest mining Ethereum-based transaction records as a means of identifying Ethereum scams. Labeled fraudulent addresses are obtained via web crawlers, and a suggested amount-based network embedding approach extracts node attributes for fraudulent transaction identification. The classification of addresses into legitimate and fraudulent ones is done using a graph convolutional network model. At 95% accuracy, the system performs well.

Ibrahim, R. F., et al. [7] used three distinct machine learning algorithms—decision tree (j48), Random Forest, and K-nearest neighbors (KNN)—to develop a Fraud detection model after looking into illicit accounts on the Ethereum blockchain. The most useful features are determined by the correlation coefficient, and just six features are employed to create a new data set. KNN had the most accuracy, coming in at 98.77%.

A neural-network based method for Ethereum fraud detection is presented by Dahiya, M., et al. [8]. This suggested model has been evaluated with its peers to verify the impact of the performance. The neural network performs the best compared to the other models, including K-nearest neighbor, SVM, Gaussian Naive Bayes, and Logistic Regression. Its accuracy of approximately 97.09% is higher than the other models'. The ability of neural networks to identify intricate patterns in the dataset and categorize subsequent transactions as authentic or fraudulent is then demonstrated.

A community discovery-based approach for anomaly identification has been proposed by Li, M., et al. [9]. First, a transaction network is constructed using the transaction data from the Ethereum public chain, and communities are then separated inside the transaction network using the Louvain method. Second, the community is categorized using the LightGBM method. Lastly, the HBOS, LOF, K-Means, KNN, and iForest algorithms are constructed as benchmark algorithms for anomaly identification based on the classification findings. The results of anomaly detection using the original transaction network are compared with the experimental results of the suggested approaches. The findings demonstrate that the community detection-based approach may successfully raise the AUC value of fraudulent account detection while reducing the amount of data by 35.53%.

Hu, J., et al. [10] present and suggest a heterogeneous multi-digraph embedding technique to enhance the efficacy of Ethereum phishing fraud detection. The technique fully captures the temporal linkages of transaction records and enriches node representations by aggregating the properties of interactions between various entities. Specifically, the suggested methodology surpasses the baseline techniques with a recall and precision of 0.76 and 0.76, respectively.

The work done by Haojie Sun, et al.[11] addresses phishing detection. The research introduces an attention-based graphical learning representation approach (ABGRL) which uses many channels to extract distinct feature information and then merges the different feature information using adaptive attention convolution. In addition, they used a self-supervised regression model to enhance the feature information of the tail node. In the final phase, a number of thorough investigations were carried out to confirm the effectiveness of the proposed paradigm.

The research carried out by M. Mazhar Rathore, et al.[12] exploited the decision-tree based machine learning model using a boosting approach, particularly XGBoost, to identify the fraudulent addresses in the Ethereum crypto-currency.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Initially, four highly performed decision tree learning approaches including CART, random forest, LGBM, XGBoost, were applied and a cross validation mechanism was used to select the top one based on accuracy. Amongst them, the XGBoost model was selected as the final model. Finally, the model, built on 80% of the training data, produced an accuracy of more than 96% on test data.

The study by Yousef K., et al.[13] presents a novel approach which efficiently detects abnormal attacks within the Ethereum network, named as ATD-SGAN. For this, a semi-supervised generative adversarial network was employed. The findings show that ATD-SGAN considerably improved the performance of cutting-edge IDSs. The false alarm rate decreased from 42.29% to 0.15%, and the detection accuracy increased from 3.78% to 11.05%. Moreover, ATD-SGAN greatly improves the F1-measure, which varies from 10.39% to 3.79%, in comparison to the current IDSs.

A novel framework called the multi-triplet augmented heterogeneous graph neural network (MAHGNN) was developed by Chengxiang Jin, et al.[14] for the detection of Ponzi schemes. In order to facilitate the definition of account features, the Conditional Variational AutoEncoder (CVAE) was developed to capture the semantic information of various triplet interaction patterns. Numerous tests revealed that MAHGNN is capable of identifying Ponzi schemes at the highest level and managing multi-edge interactions in heterogeneous Ethereum interaction graphs.

A federated learning-based anomaly detection system was developed and trained in the work of R Saravanan et al.[15] using aggregate data obtained from watching blockchain activity on the end device itself. Trials carried out on the whole history logs of the Ethereum Classic network demonstrated that the model is capable of automatically signing digital transactions to add further security and accurately identifying assaults that have been made public. Many categorization techniques and machine learning algorithms were looked at in order to categorize the accurate model.

The paper written by Baran et al.[16] proposes a system to identify the blacklisted addresses in the Ethereum blockchain. The process is initiated by collecting data based on Ethereum blockchain transactions and blacklisted addresses. Further, features of addresses are extracted once the transaction graph of Ethereum is constructed. Lastly, standard machine learning models are trained and class of addresses are predicted. The results obtained show that the blacklisted addresses can be predicted with an accuracy of more than 97%.

M.Vamsi Krishna, et.al[17] developed a comparative study with the focus to identify financial frauds. Supervised machine learning models such as Random forest and Logistic regression were employed and their performance was analyzed. The results obtained highlighted that Random forest's precision, 76.29%, was higher than that of Logistic Regression. Hence, it was concluded that Random forest could detect frauds at a significantly better efficiency as compared to Logistic regression.

In addition to attempting to reduce false positives, the primary goal of the article by Palarapu Saket et al.[18] was to compare several fraud detection techniques. The authors used a variety of assessment measures and eventually proposed which model is most appropriate for the purpose of fraud detection in Ethereum transactions.

III. METHODOLOGY

This research proposes a four-step sequential process that initiates with gathering and visualizing the data. The next step is to clean and preprocess the raw dataset, extracting only the relevant token-based attributes and resolving the imbalance in the data. The refined dataset is then fed to five machine learning classifiers that have been employed using the scikit learn module and their performances are compared and analyzed. The overall flow of the methodology is illustrated in Fig. 1.

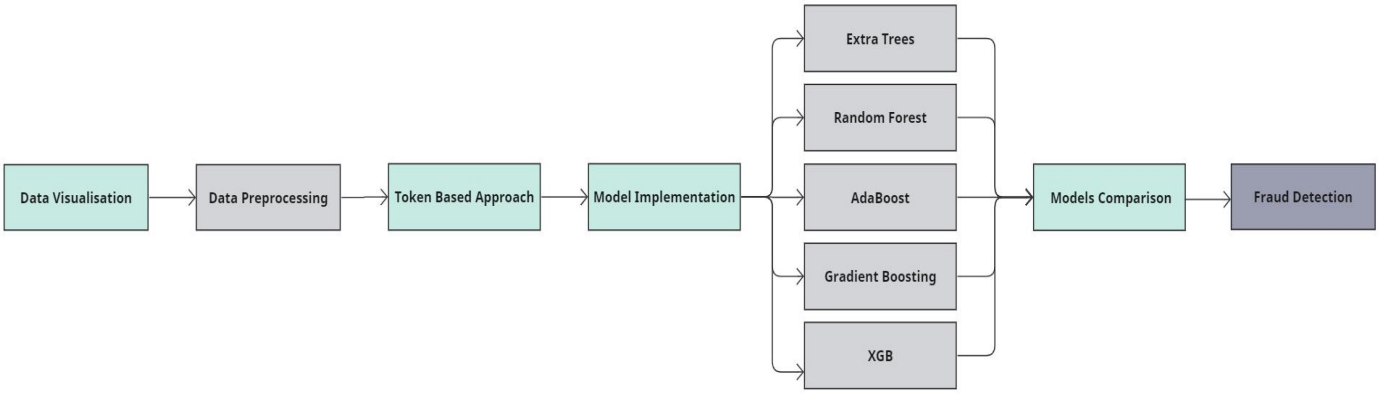


Fig. 1 Flow of the methodology

A. Dataset Description

The dataset incorporated in this study is a set of records of crypto accounts and their transactions carried out on the Ethereum platform. All in all, the dataset comprises 50 attributes divided into two sets: generic attributes and token-based attributes. The generic attributes majorly include:

Address of the Ethereum account, a binary flag value specifying if the transaction is fraudulent or not, time difference between the transactions, total number of transactions sent and received by an account, minimum, maximum, and average value of ether sent and received, transactions made via contracts, etc.

The token-based attributes are the above-mentioned generic attributes when the transactions are carried out using the ERC20 token standard. The Ethereum blockchain standard known as Ethereum Request for Comment 20 (ERC20) stipulates that when a smart contract creates a transferable token, it must employ two events and nine scripting functions. ERC20 can be best understood as a collection of guidelines that an Ethereum smart contract has to follow.

The dataset used in this research however, was initially imbalanced containing a total of 9841 transaction records out of which 7662 were normal and 2179 were fraudulent, as portrayed in the pie chart in Fig. 2.



Fig. 2 Imbalance of the dataset

B. Data Preprocessing

In this study, exploratory data analysis was carried out as an initial step to fully comprehend the data prior to preparing the data for classification. Next, a variety of cleaning and data preprocessing steps were employed to polish the raw dataset before feeding it to the classifier.

Initially, null values in the dataset were identified. This step was followed by converting the variable attributes into categorical attributes for better computational efficiency. Now, the next step is to replace missing values of numerical attributes. This is usually done by replacing the missing values with either the mean or the median value of that attribute. In this study, replacement by median method has been implemented.

Subsequently, the need to filter features with 0 variance was observed. Since they have the same value across all samples of the dataset, these features have no discriminative power, no impact on prediction and no computational efficiency. Hence, the features with 0 variance were dropped. One of the highly correlated features as well as features containing mostly zeroes were also dropped to optimize the data even further.

C. Token-based approach

As mentioned earlier in this paper, this study focuses on a novel approach to detect fraud in Ethereum transactions using token-related data. In order to prepare the data accordingly, all generic attributes were dropped, leaving only the ERC20 token-based features to be used for training. Being a standard for smart contract tokens, the values of these features evidently differed from those of the generic attributes.A correlation matrix was generated to gain inferences on the degree of correlation amongst these features as shown in Fig. 3.

The data was now ready to be prepared for the task of classification. To solve the problem of imbalance in the dataset, the SMOTE oversampling method was employed. SMOTE is a technique used to up-sample the minority cases, in this case fraudulent transactions, while ensuring there is no overfitting.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Before employing SMOTE, the count of non-fraud and fraud transactions was 6115 and 1757 respectively. Whereas after using SMOTE, the new count of non-fraud and fraud cases was 6115 and 6116 respectively, hence balancing the dataset. The balanced dataset is then split into training data (80%) and testing data (20%).

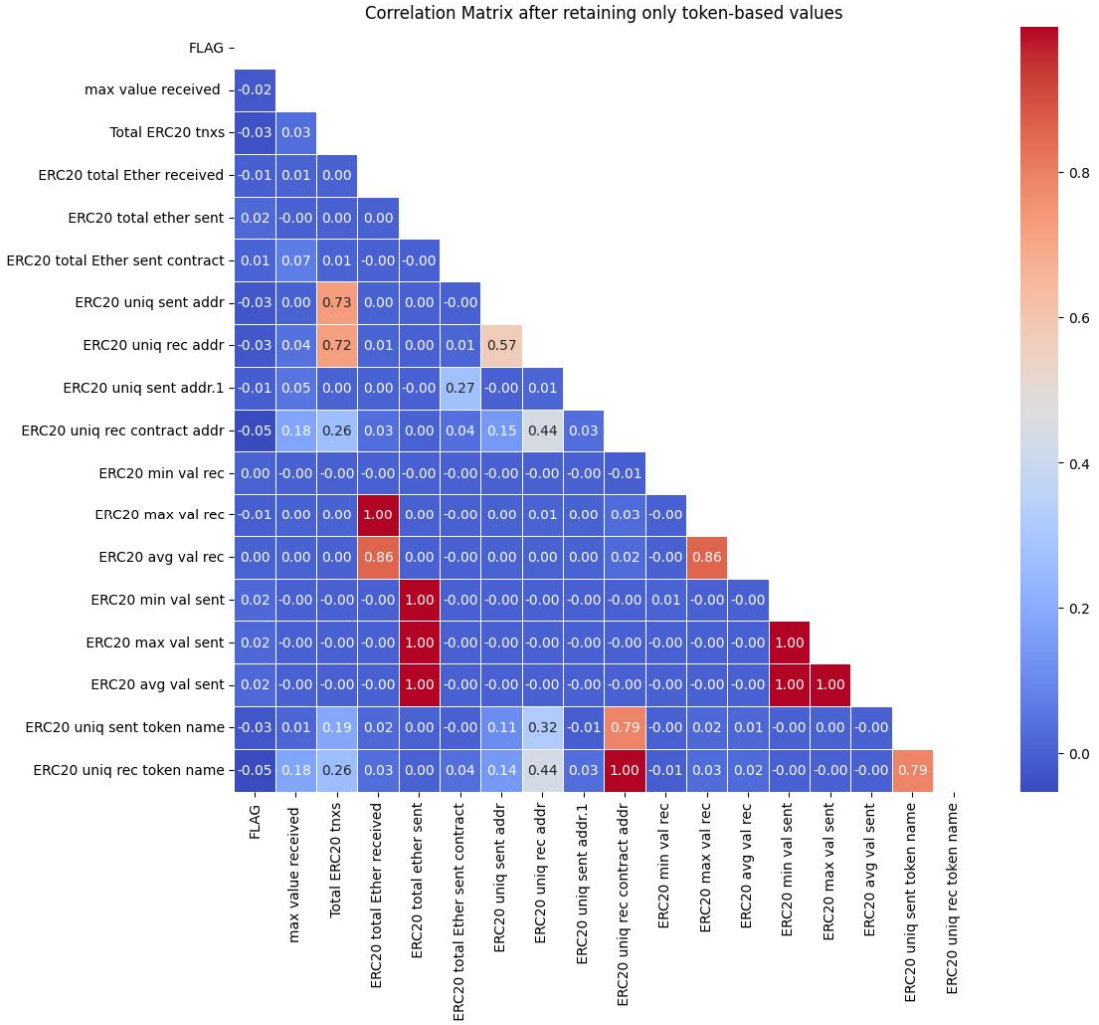


Fig. 3 Correlation matrix of ERC20 token-based features

D. Model Implementation

Finally, once the training data is preprocessed and adequately prepared, it is fed to five machine learning models namely, RF classifier, AdaBoost classifier, ET classifier, GB classifier and XGB classifier to determine the most suitable one. Standard Scalar normalization technique was used to enhance computational efficiency of all classifiers.

RF classifier was implemented to capitalize on its ability to handle nonlinearity in data and its robustness to overfitting. Adaboost classifier was used because of its versatility and the ability to automatically select adequate features for classification. ET classifier was used to maximize parallelization and enhance insensitivity to noise and outliers. The GB classifier was employed to utilize its flexibility, robustness and its ability to handle complex relationships between data. Lastly, XGB classifier was implemented to incorporate in-built regularization techniques to avoid overfitting.

Once all the models had been trained, they were tested and their yields were compared on the basis of the fundamental performance metrics namely, accuracy, precision, and recall. The results have been illustrated and discussed in the following section.

IV. RESULTS AND DISCUSSION

Following the successful implementation of the five machine learning models namely, RF classifier, AdaBoost classifier, ET classifier, GB classifier and XGB classifier, the evaluation metrics upon which the models were evaluated, were then analyzed.

Confusion matrices were plotted for all the classifiers in order to have a better understanding about how well the algorithms were able to detect false positives and false negatives.

RF classifier yielded an accuracy of 95% along with a precision of 91% and a recall of 94%. The confusion matrix for the same has been illustrated in Fig. 4.

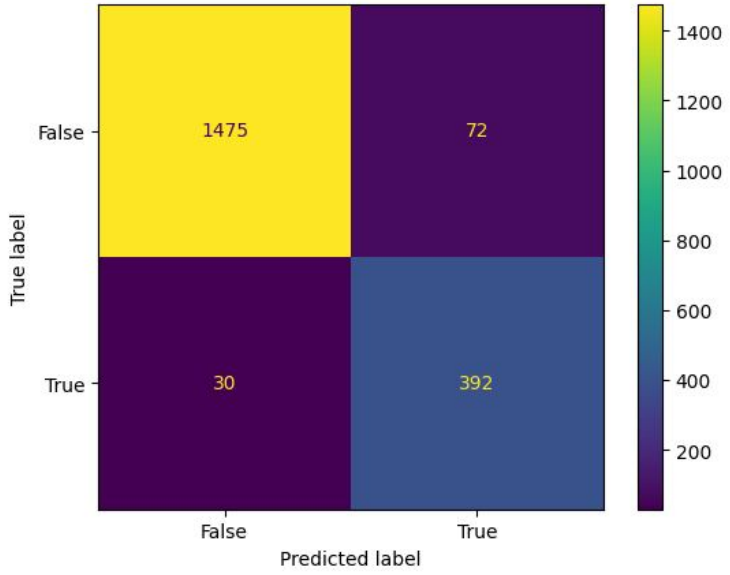


Fig. 4 Confusion matrix for RF classifier

As shown in the confusion matrix in Fig. 5, the AdaBoost classifier produced a slightly lower metric score with accuracy, precision, and recall of 90%, 84%, and 92%, respectively.

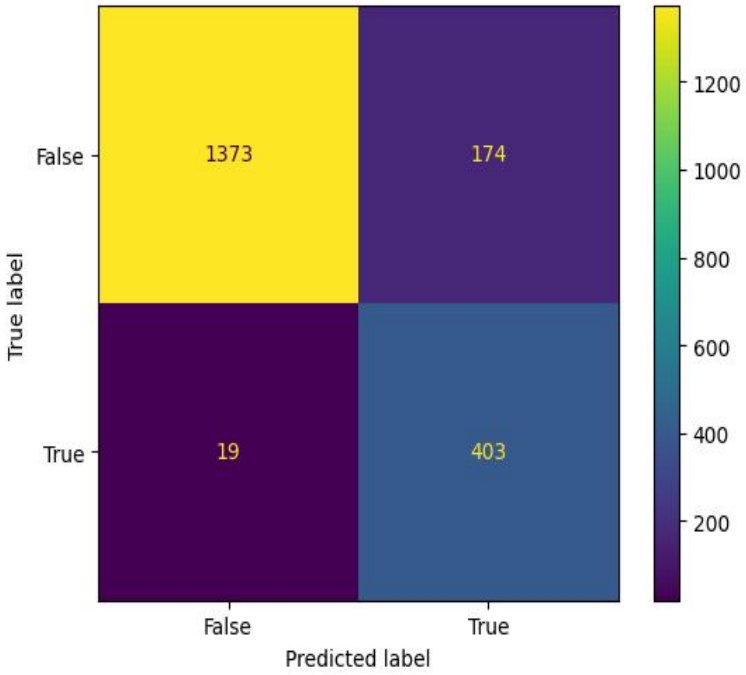


Fig. 5 Confusion matrix for AdaBoost classifier

In addition, the ET classifier produced precision and recall of 91% and 93%, respectively, with the same 95% accuracy as the RF classifier. Fig. 6 illustrates the confusion matrix for the ET classifier.

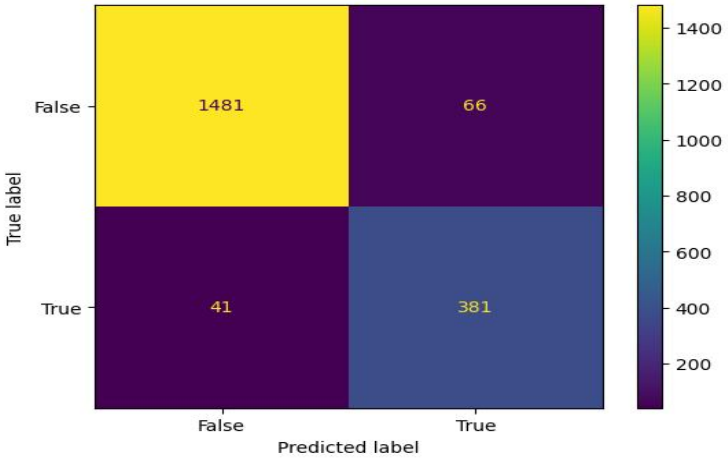


Fig. 6 Confusion matrix for ET classifier

Furthermore, the GB classifier distinguished between safe and fraudulent transactions with 94%, 89%, and 95% accuracy, precision, and recall, respectively. As shown in Fig. 7, the confusion matrix for the GB classifier is displayed.

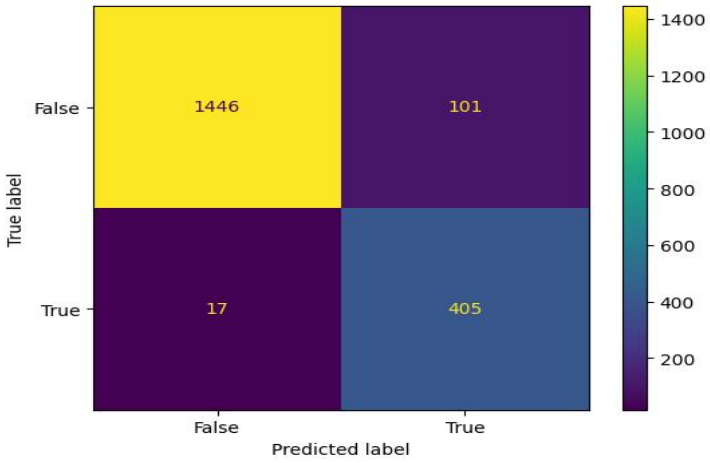


Fig. 7 Confusion matrix for GB classifier

Finally, the XGB classifier had a 95% accuracy rate, equivalent to both RF and ET classifiers. The XGB classifier has a 92% accuracy and a 95% recall rate. The confusion matrix for the XGB classifier is shown in Fig. 8.



Fig. 8 Confusion matrix for XGB classifier

For a better and simpler comparative analysis of the results of the employed models, a bar graph was plotted as depicted in Fig. 9. to provide a visual representation of the comparison. The same comparison is also numerically represented in Table 1.

TABLE I
PERFORMANCE COMPARISON OF IMPLEMENTED MODELS

Classifiers	Accuracy	Precision	Recall
Random Forest	95%	91%	94%
AdaBoost	90%	84%	92%
Extra trees	95%	91%	93%
Gradient Boosting	94%	89%	95%
XGB	95%	92%	95%

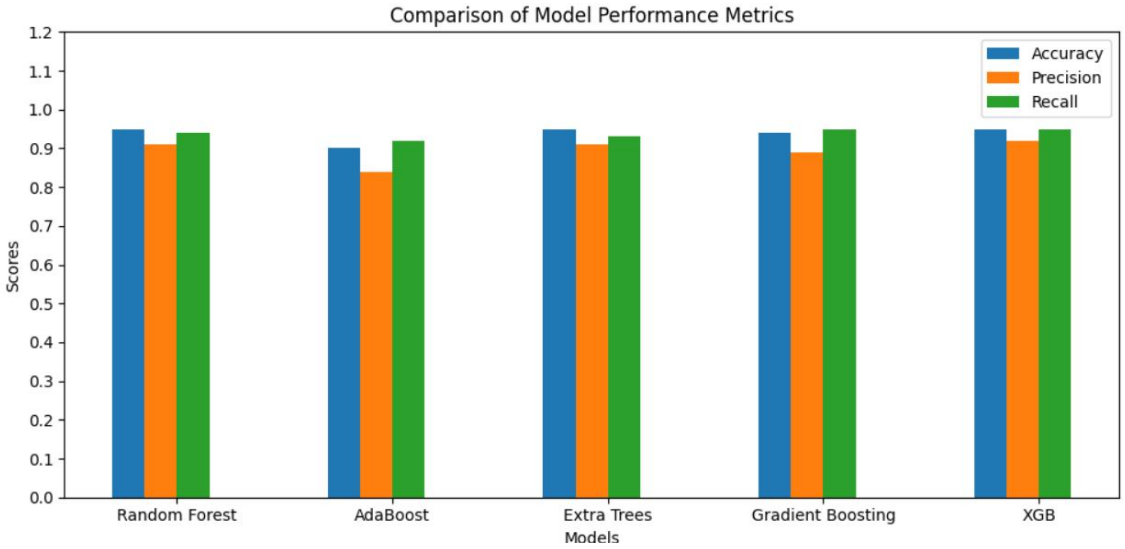


Fig. 9 Bar plot for comparison of model performance

After thorough analysis of the performance of the classifiers, it was observed that RF, ET and XGB classifiers yielded the highest accuracy of 95%, suggesting that they are the most suitable for detection of fraud in Ethereum transactions.
Furthermore, the token-based method proposed and implemented in this study surpassed the proficiency of the conventional methods used in existing research [1,5,6,8,10,11,15].

V. CONCLUSION

Despite the increased reliability and security of the Ethereum platform, attackers have managed to find loopholes in the comparatively safer ERC20 standard as well. These fraudulent smart contract transactions impede safe exchange of cryptocurrency on the platform. The need for adequate detection of these frauds was the primary reason for this study. This research presents a novel and efficient method for detecting fraudulent transactions on Ethereum by employing machine learning methods. Primarily preparing the dataset to focus only on the ERC20 token-based attributes was the pivotal step that induced novelty in the approach. Optimistic outcomes were obtained after using several supervised machine learning models—RF, AdaBoost, ET, GB, and XGB—on the refined dataset. Following a comprehensive evaluation of the classifiers' performance, it was found that the RF, ET, and XGB classifiers produced the best results, with an accuracy rate of 95%, indicating that they are the most appropriate for identifying fraud in smart contract Ethereum transactions. Being a newly implemented approach, there is plenty of room for improvement and optimization.

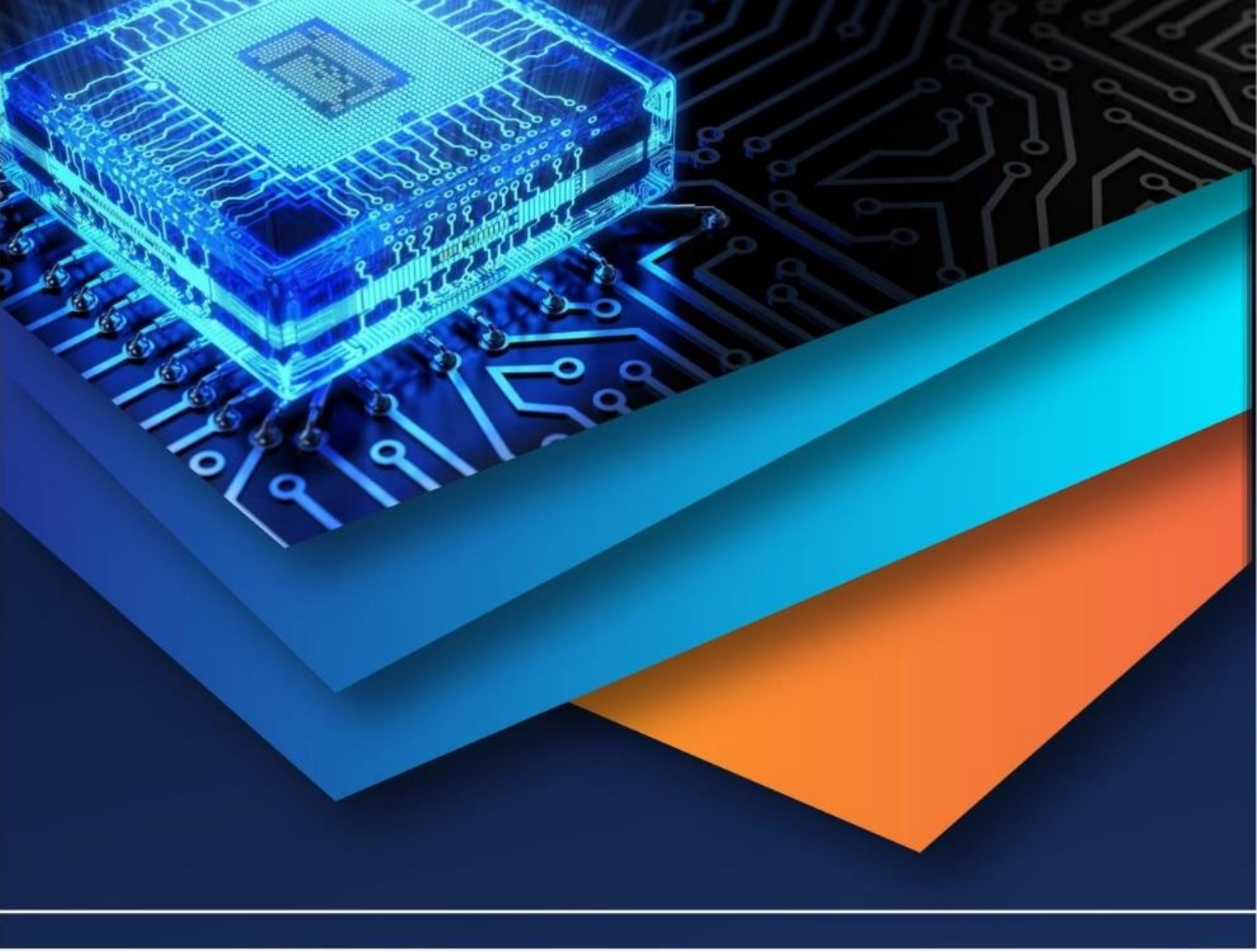
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

One such improvisation technique would be the use of neural networks, Graph Neural Networks in particular, to efficiently incorporate a larger number of attributes and multiple combinations of these attributes to yield better results. Token-based approaches such as the one proposed in this study can also find other applications in authentication of healthcare records, enhancing security and integrity of online voting systems, and securing real estate transactions as well.

REFERENCES

[1] Elmougy, Y., & Manzi, O. (2021, December). Anomaly Detection on Bitcoin, Ethereum Networks Using GPU-accelerated Machine Learning Methods. In 2021 31st International Conference on Computer Theory and Applications (ICCTA) (pp. 166-171). IEEE.
[2] Jung, E., Le Tilly, M., Gehani, A., & Ge, Y. (2019, July). Data mining-based ethereum fraud detection. In 2019 IEEE international conference on blockchain (Blockchain) (pp. 266-273). IEEE.
[3] Hou, W., Cui, B., & Li, R. (2022, December). Detecting Phishing Scams on Ethereum Using Graph Convolutional Networks with Conditional Random Field. In 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys) (pp. 1495-1500). IEEE.
[4] Huang, B., Liu, J., Wu, J., Li, Q., & Lin, D. (2023, May). Ethereum Phishing Fraud Detection Based on Heterogeneous Transaction Subnets. In 2023 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1-5). IEEE.
[5] Roy, K. S., Karim, M. E., & Udas, P. B. (2022, December). Exploiting Deep Learning Based Classification Model for Detecting Fraudulent Schemes over Ethereum Blockchain. In 2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-6). IEEE.
[6] Tan, R., Tan, Q., Zhang, P., & Li, Z. (2021, December). Graph neural network for ethereum fraud detection. In 2021 IEEE international conference on big knowledge (ICBK) (pp. 78-85). IEEE.
[7] Ibrahim, R. F., Elian, A. M., & Ababneh, M. (2021, July). Illicit account detection in the ethereum blockchain using machine learning. In 2021 international conference on information technology (ICIT) (pp. 488-493). IEEE.
[8] Dahiya, M., Mishra, N., & Singh, R. (2023, May). Neural network based approach for Ethereum fraud detection. In 2023 4th International Conference on Intelligent Engineering and Management (ICIEM) (pp. 1-4). IEEE.
[9] Li, M., Cui, B., Hou, W., & Li, R. (2023, June). Research on Malicious Account Detection Mechanism of Ethereum Based on Community Discovery. In 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 705-710). IEEE.
[10] Hu, J., Cao, M., Zhang, X., Zhang, X., & Zhu, Y. (2023, May). Temporal Weighted Heterogeneous Multigraph Embedding for Ethereum Phishing Scams Detection. In 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 1208-1213). IEEE.
[11] Sun, H., Liu, Z., Wang, S., & Wang, H. (2024). Adaptive Attention-Based Graph Representation Learning to Detect Phishing Accounts on the Ethereum Blockchain. IEEE Transactions on Network Science and Engineering.
[12] Rathore, M. M., Chaurasia, S., Shukla, D., & Anand, P. (2023, December). Detection of Fraudulent Entities in Ethereum Cryptocurrency: A Boosting-based Machine Learning Approach. In GLOBECOM 2023-2023 IEEE Global Communications Conference (pp. 6444-6449). IEEE.
[13] Sanjalawe, Y. K., & Al-E'mari, S. R. (2023). Abnormal Transactions Detection in the Ethereum Network Using Semi-Supervised Generative Adversarial Networks. IEEE Access.
[14] Jin, C., Zhou, J., Gong, S., Xie, C., & Xuan, Q. (2023, December). Multi-triplet Feature Augmentation for Ponzi Scheme Detection in Ethereum. In 2023 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 649-655). IEEE.
[15] Saravanan, R., Santhiya, S., Shalini, K., & Sreeparvathy, V. S. (2023, April). Comparative Study Analysis of MachineLearning Algorithms for Anomaly Detection in Blockchain. In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-6). IEEE.
[16] Kılıc, B., Sen, A., & Özturan, C. (2022, September). Fraud detection in blockchains using machine learning. In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA) (pp. 214-218). IEEE.
[17] Krishna, M. V., & Praveenchandar, J. (2022, October). Comparative analysis of credit card fraud detection using logistic regression with random forest towards an increase in accuracy of prediction. In 2022 International Conference on Edge Computing and Applications (ICECAA) (pp. 1097-1101). IEEE.
[18] Saket, P., Jyothi, P., Patnaik, A. B. V. A., Reddy, N. C. V., & Suresh, S. (2024, January). Cost Sensitive Approach to Ethereum Transactions Fraud Detection using Machine Learning. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-8). IEEE.
[19] Hu, H., Bai, Q., & Xu, Y. (2022, May). Scsguard: Deep scam detection for ethereum smart contracts. In IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.
[20] Zkik, K., Sebbar, A., Fadi, O., Mustapha, O., & Belhadi, A. (2023, July). A Graph Neural Network Approach for Detecting Smart Contract Anomalies in Collaborative Economy Platforms Based on Blockchain Technology. In 2023 9th International Conference on Control, Decision and Information Technologies (CoDIT) (pp. 1285-1290). IEEE.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)