

Original Article

Security Enhancement for Cryptocurrency Transactions Using Machine Learning

Polasani Sai Adithya¹, Syed Sameer¹, Rohith Juluri¹, Kasi Bandla^{1*}

**Department of Electronics and Computer Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India.*

**Corresponding Author : kasi.b@sreenidhi.edu.in*

Received: 22 April 2024

Revised: 27 May 2024

Accepted: 10 June 2024

Published: 29 June 2024

Abstract - This paper introduces an architecture for enhancing the security of cryptocurrency transactions through machine learning techniques. The process begins with importing blockchain data and conducting exploratory data analysis (EDA) to address missing values and visualize data distributions. It also involves feature selection and managing data imbalance with the Synthetic Minority Over-Sampling Technique (SMOTE). To evaluate anomaly detection, three machine learning algorithms—Linear Regression, Naive Bayes, and XGBoost—are compared for their performance. Among them, XGBoost outperforms Linear Regression and Naive Bayes, which are often preferred in other domains. In detecting typical versus anomalous transactions, XGBoost delivers superior results. This study contributes to building robust security systems that protect Bitcoin transactions from fraudulent activities, thereby increasing trust and reliability in the cryptocurrency ecosystem. The proposed architecture integrates machine learning methods with blockchain data to bolster the robustness of Bitcoin transactions, reinforcing the integrity of the cryptocurrency market.

Keywords - Cryptocurrency, Machine Learning, Enhanced security, XGBoost, EDA, SMOTE.

1. Introduction

The rapid growth of cryptocurrencies in recent years has gone hand in hand with a surge in security risks. As digital currencies like Bitcoin gain broader adoption, they attract both legitimate users and malicious actors seeking to exploit vulnerabilities for financial gain. Traditionally, security in the Bitcoin ecosystem has relied on cryptographic methods, but the relentless evolution of cyber threats calls for more sophisticated defenses. To address this critical need, incorporating machine learning (ML) into Bitcoin security systems is emerging as a compelling solution.

ML algorithms have already shown remarkable success in fields such as image recognition and natural language processing, and their application in cybersecurity is gaining momentum. By harnessing the flexibility and adaptability of machine learning, Bitcoin's security systems can evolve dynamically to respond to new threats in real-time.

It is now challenging to distinguish between fraudulent transactions and those that are safe on the Bitcoin blockchain due to the vast volume of transactions that occur there every day. While previous machine learning algorithms can detect fraudulent transactions, the accuracy and effectiveness of the current approaches remain a significant issue that this work aims to address.

This article seeks to investigate the convergence between Bitcoin transactions and machine learning, offering light on the potential benefits and drawbacks of this combination. To accomplish this goal, we perform a thorough study of the existing literature and look at pertinent case studies that show the effectiveness of ML-driven approaches in improving Bitcoin transaction security. The use of machine learning techniques has various benefits in terms of improving the security of Bitcoin transactions. One of the primary advantages is the capacity to detect irregularities in transaction patterns, which may indicate fraudulent behavior. ML algorithms excel at detecting deviations from typical behavior, allowing for early detection and prevention of fraudulent transactions [1].

Furthermore, machine learning can help security systems discover complex patterns of fraudulent conduct that traditional rule-based detection methods may miss [2]. Furthermore, predictive modelling techniques can use previous data to identify potential security breaches, allowing for proactive risk mitigation steps before they occur [3]. However, integrating machine learning into Bitcoin security systems raises some obstacles. One key worry is the possibility of adversarial assaults, in which hostile actors try to manipulate ML systems by providing them with manipulated input data to avoid detection methods [4].



Furthermore, maintaining the robustness and dependability of ML models in the face of dynamic and developing threats necessitates continuous monitoring and adaptation [5]. Furthermore, privacy concerns may arise as a result of the large amounts of sensitive transaction data involved, needing careful evaluation of data handling and protection procedures[6].

This work explores the effective use of Machine Learning(ML) to bolster the security of Bitcoin transactions. By examining the benefits and challenges of merging ML with cryptocurrency security, we aim to guide the creation of robust security frameworks for the evolving world of cryptocurrencies. Strengthening trust and reducing risks can lead to more secure transactions and sustainable growth in the Bitcoin ecosystem. Section 2 of this paper discusses the background, while Section 3 presents the methodology with a design approach. Experimental results are shown in Section 4 along with comparisons with other candidate designs for benchmarking. The paper is concluded in Section 5.

2. Background

A wide range of methodologies and approaches are covered in the vast and varied literature on Bitcoin price prediction and forecasting techniques. We examine recent studies and research articles that explore the intersection of blockchain technology, machine learning, and cryptocurrency price prediction in this overview of the literature.

A method for calculating the global computational capacity of blockchain networks based on cryptocurrency prices was proposed by [7]. Through an analysis of the correlation between cryptocurrency values and processing power, the authors developed a model that forecasts the processing power of blockchain networks in the future. However, because cryptocurrency values are so erratic, this method has a big disadvantage. This problem was resolved by [8] carrying out an empirical investigation on the modeling of Bitcoin price prediction using Bayesian neural networks based on blockchain data. Their findings highlight the necessity of using blockchain information to improve the accuracy of Bitcoin price predictions. However, this approach has limitations because Bitcoin values are influenced by a variety of external factors. Combining machine learning and blockchain technologies appears to be a viable method for predicting the value of cryptocurrencies. A hybrid methodology has the potential to increase price projection accuracy by fusing machine learning algorithms such as support vector regression and long short-term memory networks with the transparency and security of blockchain data. This method [9] offers a fresh take on Bitcoin forecasting by addressing some of the limitations seen in conventional Bayesian neural network Models. The authors developed decision trees and regression models for predicting

price changes using historical Bitcoin market data [10]. Their research advances our knowledge of traditional machine learning techniques as they relate to predicting bitcoin prices. Due to the overfitting and under-fitting of the decision tree and regression models, researchers looked at the cryptocurrency Bitcoin and its potential. Later, the researchers gained insight into the fundamental mechanics that drive cryptocurrency price fluctuations by looking into several factors influencing Bitcoin's price volatility and market dynamics [11]. Their efforts improve our knowledge of the processes affecting the Bitcoin ecosystem. However, compared to other approaches, this one is more complex and needs a lot of data training. To address this complexity and shorten training time, the next researchers undertook a thorough investigation of the cryptocurrency sector, including its evolution, market trends, and prospects. Focusing on how fresh cryptocurrency creation, legal developments, and technology advancements affect the direction of the sector [12]. This report clarifies the workings of the cryptocurrency market as well as the implications for stakeholders and investors. The body of research on predicting the price of Bitcoin indicates that there is growing interest in accurately estimating price patterns through the use of machine learning techniques and blockchain technology. To increase the precision and dependability of bitcoin price forecasts, researchers are experimenting with a range of instruments and methodologies, from empirical studies to theoretical analysis. As the cryptocurrency space develops, further study is required to comprehend market dynamics.

3. Methodology

3.1. Proposed System

The proposed system enhances cryptocurrency transaction security by utilizing machine learning algorithms such as XGBoost, Naive Bayes, and Linear Regression. Extensive testing has shown that XGBoost is more effective than Linear Regression and Naive Bayes in identifying fraudulent activity. By utilizing the capabilities of multiple weak learners, its ensemble learning technique enhances projected performance and robustness against anomalies. Because it is straightforward and effective, Naive Bayes is used to estimate probabilities, while Linear Regression reveals the linear relationships between transaction characteristics and possible fraudulent activity. The system aims to enhance security measures by accurately identifying and addressing fraudulent transactions in real-time through the combination of various algorithms. Better accuracy and dependability are made possible by ongoing observation and adaptation, giving customers the confidence to safeguard their Bitcoin investments.

3.2. System Architecture

A multi-stage, structured pipeline is part of the system architecture for integrating machine learning into the security of Bitcoin transactions. The two primary datasets used by the

system’s Machine Learning module are Training Data and Testing Data. In the beginning, the Training Data are preprocessed using Exploratory DataAnalysis (EDA), which handles missing values and shows distributions of the data. Following the processing of the Training Data, a Learning

Model is trained using methods such as XGBoost, Naive Bayes, and Linear Regression. The trained model’s ability to identify fraudulent activity in Bitcoin transactions is then assessed by comparing it to the Testing Data.

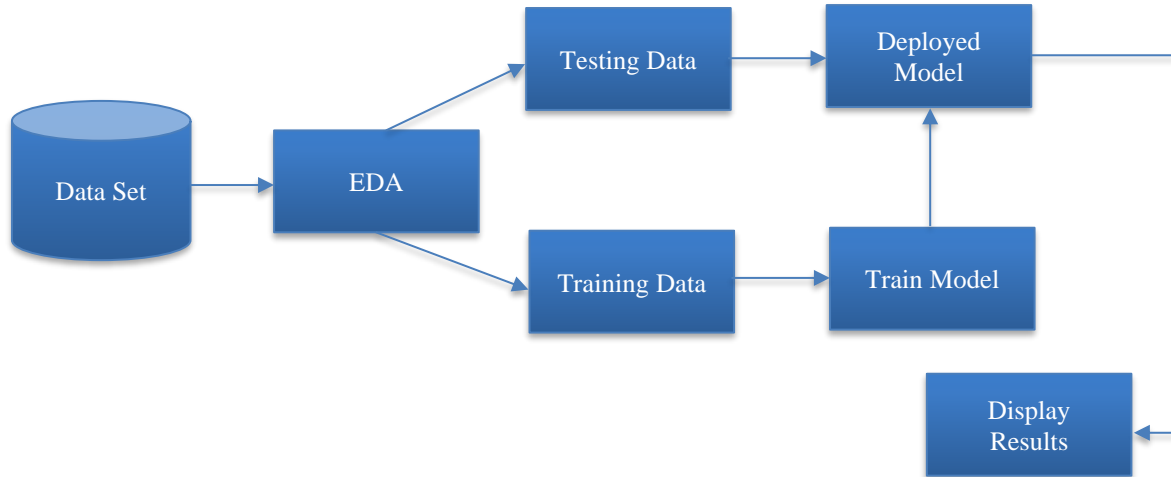


Fig.1 Proposed architecture

The model is incorporated into the system after proving to be accurate enough. By analyzing real-time transaction data, the Deployed Model makes predictions by applying previously discovered patterns and features. Because this prediction method operates in real-time, fraudulent transactions can be quickly identified and mitigated. The model’s long-term performance is ensured by constant observation and modification, which improves its accuracy and dependability in protecting cryptocurrency assets. All things considered, our rigorous approach effectively integrates machine learning into the security of Bitcoin transactions, offering robust defense against new threats.

3.3. Data Collection

The “Cryptocurrencies” dataset is an extensive collection of data regarding different cryptocurrencies that are available for purchase. The name, ticker symbol, market capitalization, trading volume, price history, circulating supply, and historical performance metrics of the cryptocurrency are usually included in this dataset. Additionally, it might include information about blockchain, such as mining difficulty, network activity, and transaction volumes. A wide variety of cryptocurrencies, including less well-known altcoins and well-known ones like Bitcoin, Ethereum, Ripple, and Litecoin, may be included in the dataset, which spans several time periods. This information is used by analysts, investors, and researchers for a range of purposes, including academic research, trend forecasting, market analysis, and investment decision-making. Keeping this dataset updated and maintained is essential, given the rapid growth and change of the cryptocurrency market, in order to remain current with the latest developments.

3.4. Data Processing

In the data processing stage, we modify and get the data ready for additional analysis and modeling using both the Pandas and Keras data frames. The first step is importing the data into a panda data frame, a powerful Python tool for handling structured data. The data frame’s superfluous columns are eliminated to streamline the dataset and get rid of information that is redundant or unnecessary. This process maximizes computational resources while reducing complexity. The data can then be transformed into a Keras data frame for further preprocessing tasks or for merging with deep learning models.

High-level neural network API Keras offers extra functionality reserved for deep learning use cases. The conversion technique offers smooth interaction with deep learning models and compatibility with Keras operations. A variety of methods, including feature engineering, normalization, and data cleaning, can be applied throughout the data processing stage to enhance the relevance and quality of the data. To guarantee that the data is suitably prepared and suitable for training machine learning models, several procedures are essential. Both pandas and Keras data frames make it simple to organize and preprocess data, which sets the stage for additional analytic and modeling activities.

3.5. Visualization

Understanding and interpreting machine learning algorithms, such as XGBoost, uses visualization. Visualizations shed light on the decision-making process,

feature significance, and performance of the model. One method that can help us understand how the model performs better with more training data or iterations is to plot learning curves. Feature selection and interpretation are aided by the ability to visually represent the features that have the biggest influence on the model's predictions. Moreover, examining decision trees produced by XGBoost enables us to comprehend the fundamental reasoning behind the model's decision-making procedure. These illustrations not only aid in our understanding of the XGBoost algorithm but also facilitate the dissemination of the findings to interested parties, rendering complex machine-learning ideas more manageable and useful. Visualization plays a crucial role in optimizing the potential of XGBoost.

3.6. Feature Selection

Enhancing the effectiveness and efficiency of machine learning models, like XGBoost, requires careful consideration of feature selection. Numerous approaches may be taken to choose pertinent features and improve model accuracy. To reduce model complexity and overfitting, we can identify features that are highly related and eliminate duplicates using methods like correlation analysis. Second, by assigning computing power to the most pertinent variables, we may utilize XGBoost's feature importance scores to select the most important features for prediction. Moreover, subsets of features can be iteratively evaluated using methods like forward/backward selection and Recursive Feature Elimination (RFE) to determine the optimal feature set for model performance. Additionally, by choosing features that are most likely to affect the target variable based on subject matter expertise, domain knowledge can aid in feature selection. By employing these strategies, we may enhance the XGBoost models' interpretability, efficiency, and forecast accuracy, opening the door to more reliable and successful machine-learning applications.

3.7. Training and Testing

The training and testing stages of machine learning are essential for the development and assessment of models. To close the gap between expected and actual outcomes, the model iteratively modifies its parameters during training (80%) to identify patterns and relationships in the data. Using optimization methods like gradient descent, this strategy involves feeding labeled data (input-output pairs) into the model and adjusting its internal parameters. After training, the model is assessed against a different dataset—referred to as the testing set (20%), that it was not exposed to during training.

This lets us assess how well the model generalizes and how well it can produce accurate predictions on data that has not been seen before. The testing phase provides metrics such as accuracy, precision, recall, and F1 score that indicate how effective the model is; by dividing the dataset into subsets for training and testing, we may evaluate the model's reliability and performance in practical applications.

3.8. Webpage Generation

The code, after execution, creates a URL after all of the testing and training is complete, and when you paste that URL into a website, it creates a webpage. When a visitor enters, a home page with signup and sign-in buttons appears. Clicking on those buttons takes them to the registration and login pages, respectively.

Then an input screen appears, where you may enter variables like in-degree, out-degree, bitcoin in, bitcoin out, total bitcoin, mean out bitcoin, and maintain in bitcoin to determine the outcome or if the blockchain transaction is secure or not. "Safe Transaction" is displayed if it is safe; else, "Anomaly Transaction Detected" is shown.

3.9. Algorithms

3.9.1. Linear Regression

Linear Regression is an essential ML calculation that predicts mathematical qualities utilizing input qualities. Fitting a straight line to the information focuses on a direct connection between free factors (highlights) and a reliant variable (objective). Linear Regression [13] is frequently utilized for deal anticipation, stock price prediction, and pattern research. Straight Relapse, by concentrating on the connection between factors, gives experiences into the fundamental examples and patterns in information, considering more exact gauges of future results.

3.9.2. Naive Bayes

Naive Bayes is a probabilistic ML procedure that, for the most part, performs a grouping position. It will probably estimate examples' class names given the probability of events of different traits. Regardless of its effortlessness, Naive Bayes [13] is compelling in different certifiable applications, for example, message order, spam separating, and feeling examination. It infers that elements are autonomous of each other, consequently the name "naive," yet it now and again creates sufficient outcomes in any event when this supposition is broken. Naive Bayes is proficient, easy to execute, and particularly valuable for managing colossal, high-layered datasets.

3.9.3. XGBoost

Extreme Gradient Boosting, or XGBoost, is a sophisticated machine learning algorithm recognized for its unparalleled performance in characterization and relapse problems. It is likely to create strong points for a decision tree using inclination assistance, which improves hypothesis correctness and reduces errors. XGBoost [11] is widely used in several industries, such as banking, healthcare, and online advertising, because of its ability to handle large datasets and identify complex relationships between attributes and target parameters. It consistently produces state-of-the-art rivalries and certified applications, making it a well-known choice for sophisticated machine learning jobs requiring high predictive accuracy.

4. Results and Discussion

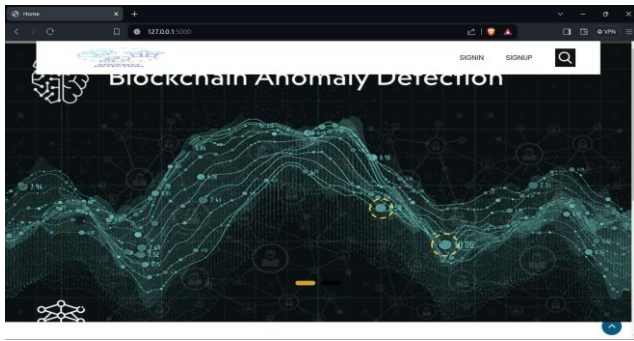


Fig. 2 Home page

A home page shown in Fig.2, is the main web page that a visitor will view when they navigate to a website via a search engine, and it may also function as a landing page to attract visitors.

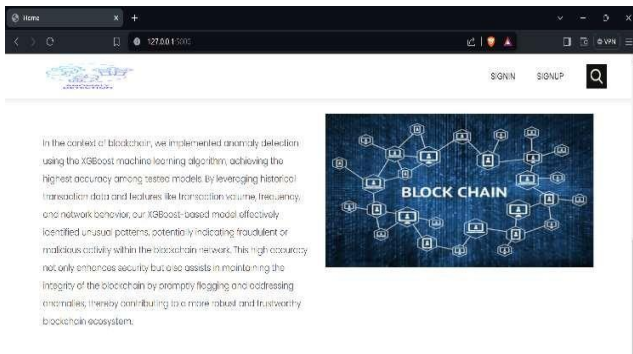


Fig. 3 Description page

A description page shown in Figure 3, which is obtained by scrolling down the home page, shows detailed information on the blockchain.

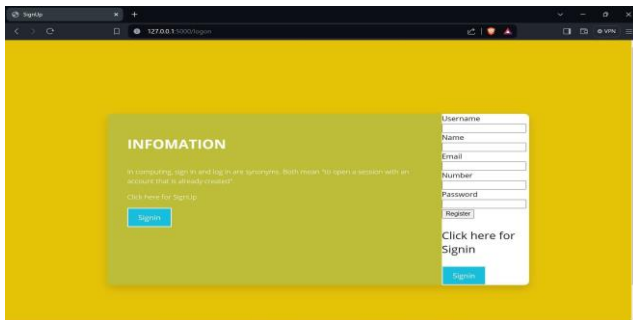


Fig. 4 Registration page

A registration page is shown in Figure 4, which is obtained by clicking the signup button on the home page that allows users to create an account or register for a service, website, or application. It is a crucial component of online platforms that require user authentication and personalized access.

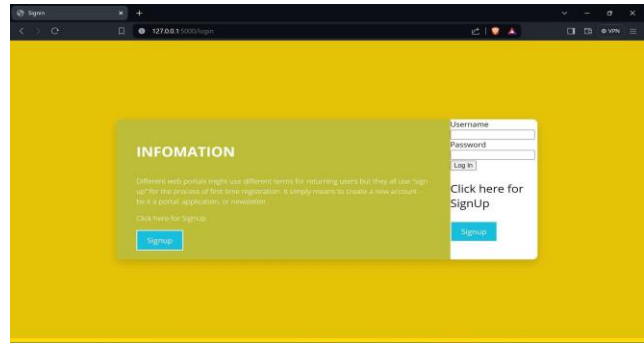


Fig. 5 Login page

A login page shown in Figure 5, which is displayed upon clicking the sign-in button on the home page/registration page, allows a user to access a website or web application by entering their username and password or by authenticating with a social network login.

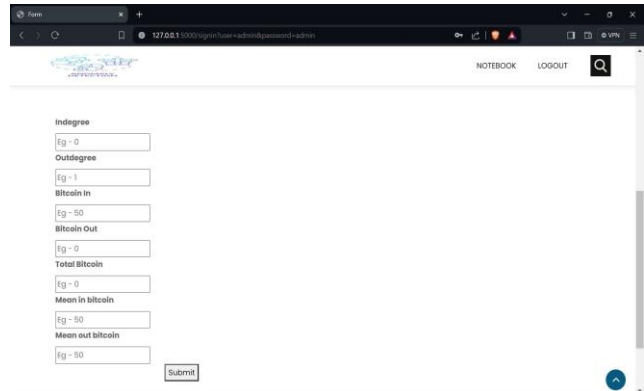


Fig. 6 Input page

An input page shown in Figure 6 is displayed when the user successfully login into the webpage, where the user will enter details according to the block requirements.

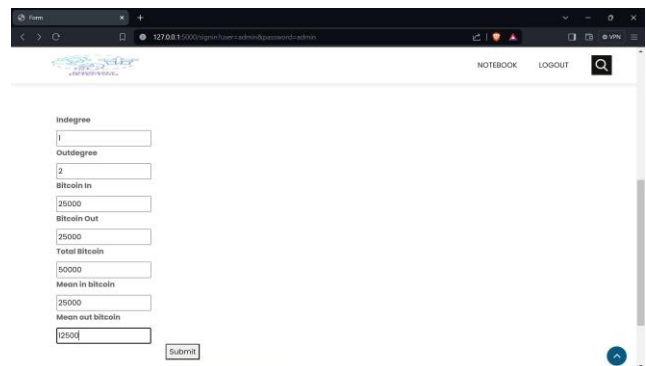


Fig. 7 Uploading input data

User has to enter the input data, as shown in Figure 7, according to their requirements and press the submit button to follow to the next page.

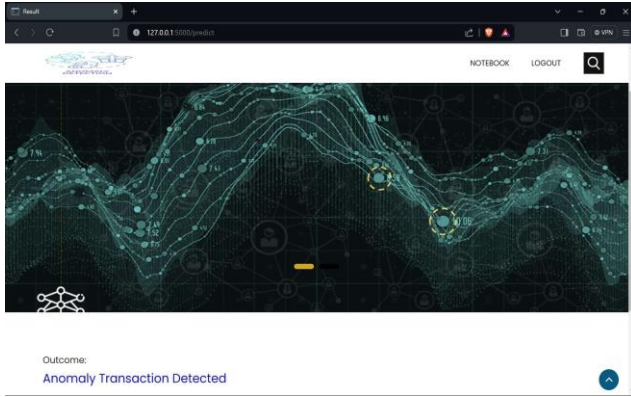


Fig. 8 Final outcome with anomaly

By clicking the submit button on the input page, the result for the above-entered input is visible in Figure 8 as an outcome where the transaction is detected as an anomaly(fraud).

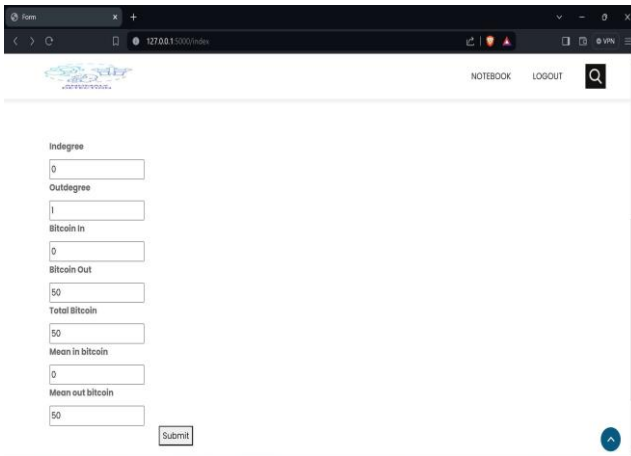


Fig. 9 Uploading another input data

User can enter another input data, as shown in Figure 9, according to their requirements and press the submit button to follow to the next page.

By clicking the submit button on the input page, the result for the above-entered input is visible in Figure 10 as an outcome where the transaction is detected as safe.

Figure 11 represents the values of the comparison table in the form of bar graphs of each machine-learning model. It

shows parameters such as accuracy, recall, precision, F1 score, and sensitivity for different machine learning models: Linear Regression, Naïve Bayes and XGboost.

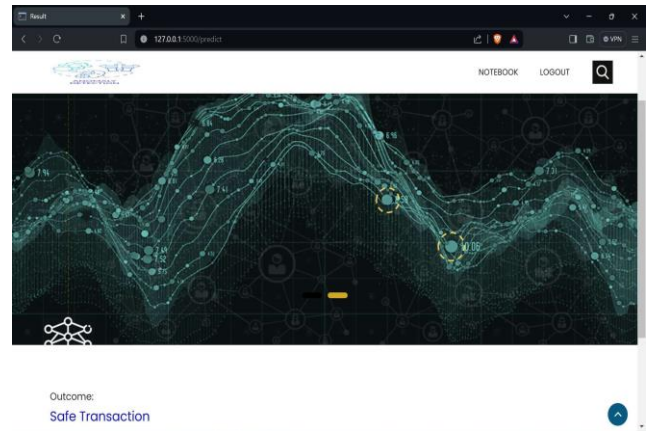


Fig. 10 Final outcome with safe transaction

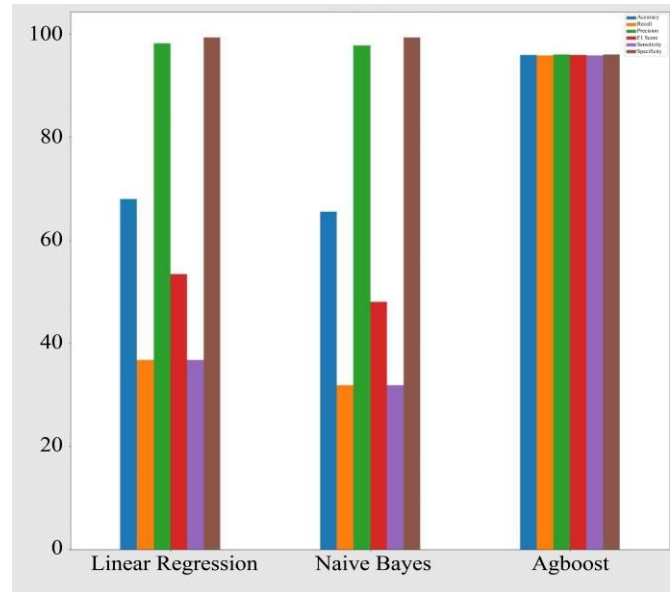


Fig. 11 Comparison graph

Table 1 shows the parameters like accuracy, recall, precision, F1 score, and sensitivity for different machine learning models: linear regression, naïve Bayes, and Xg boost. This table compares all the three-machine learning models and displays the result.

Table. 1 Comparison table

ML Algorithms	Accuracy	Recall	Precision	F1 score	Specificity	Sensitivity
Linear Regression	68.013237	36.704427	98.164037	53.430648	99.313700	36.704427
Naïve Bayes	65.539166	31.797775	97.762812	47.986293	99.272562	31.796775
XGBoost	95.913891	95.811747	96.006830	95.909190	96.016007	95.811747

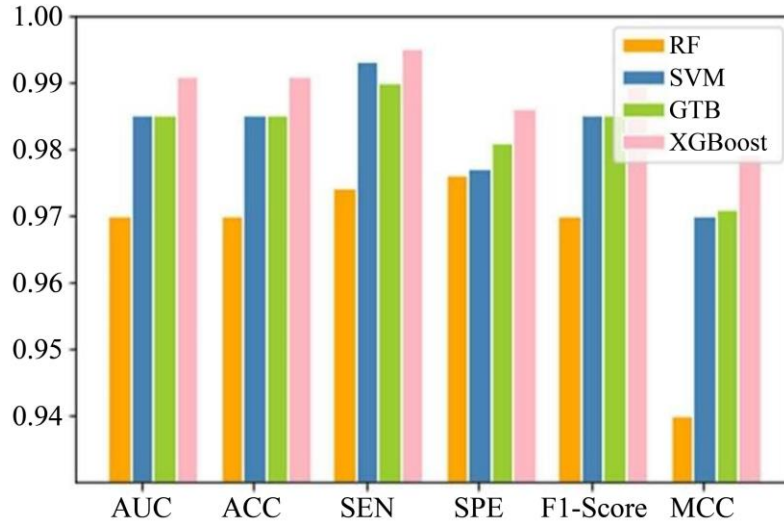


Fig. 12 Comparison with existing machine learning algorithms

Figure 12 shows different parameters such as Characteristic Curve (AUC), Accuracy (ACC), Sensitivity (SEN), Specificity (SPE), F1-Score and Mathews Correlation Coefficient (MCC) between the existing machine learning algorithms such as Random Forest (RF), Support Vector Machine (SVM), Gradient Tree Boosting (GTB) and XGBoost. Hence it is proved that the XGBoost algorithm is better in all aspects when compared to the existing machine learning techniques.

5. Conclusion

The proposed method offers a robust and multifaceted approach to enhancing security in Bitcoin transactions using various machine-learning techniques. The system uses the special qualities of XGBoost [11], Naive Bayes [13], and Linear Regression [13] to deliver the best fraud detection performance. The proposed method uses the XGBoost algorithm, which improves the accuracy by over 41.01% compared to the Linear Regression method and 46.34% when compared to the Naïve Bayes method. The F1 Score of the proposed method is also improved by 79.58% when compared to the Linear Regression method and 99.87% when compared to the Naïve Bayes method. Based on these results we can say that XGBoost is the most suitable method for the detection of fraudulent transactions on blockchain. XGBoost's ensemble learning technique is especially helpful for spotting fraudulent activity in Bitcoin transactions. The system's performance is also attributed to the ease of use and effectiveness of Naïve Bayes in probability estimation, as well

as the insights provided by Linear Regression into possible linear correlations between transaction data and fraudulent activity [14]. Customers can feel secure knowing that their Bitcoin assets are protected. Thanks to the suggested system's ability to detect and block fraudulent transactions in real-time, as proven by extensive testing and assessment [15]. The system's long-term accuracy and dependability are guaranteed by constant monitoring and response to new threats.

Figure 12 illustrates how the XGBoost approach outperforms the current machine learning algorithms in every way, including Accuracy, F1-Score, Specificity, Sensitivity, and more. Thanks to the use of the XGBoost algorithm, which can handle big datasets and find intricate correlations between qualities and target parameters, this research produced superior results than previous machine learning techniques. It is a well-known option for complex machine learning tasks needing high predicted accuracy since it continuously generates cutting-edge rivalries and validated applications.

In the future, the accuracy of fraud detection can be increased by merging sophisticated deep learning techniques like as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to identify temporal correlations and spatial patterns inside transactions. Investigating blockchain integration for safe and transparent transaction recording could also fortify the system against new threats in the cryptocurrency space by adding extra levels of security and transparency.

References

- [1] Nasrullah Sheikh, Zekarias Kefato, and Alberto Montesor, "GAT2VEC: Representation Learning for Attributed Graphs," *Computing*, vol. 101, no. 3, pp. 187-209, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Pranav Nerurkar et al., "Supervised Learning Model for Identifying Illegal Activities in Bitcoin," *Applied Intelligence*, vol. 51, no. 6, pp. 3824-3843, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [3] Damiano Di Francesco Maesa, Andrea Marino, and Laura Ricci, "The Graph Structure of Bitcoin," *Complex Networks and their Applications, COMPLEX NETWORKS 2018*, Cambridge, United Kingdom, pp. 547-558, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Fabio Aiolli et al., "Mind Your Wallet's Privacy: Identifying Bitcoin Wallet Apps and User's Actions through Network Traffic Analysis," *SAC '19: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pp. 1484-1491, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, and Muttukrishnan Rajarajan, "Detection of Bitcoin-Based Botnets Using a One-Class Classifier," *IFIP International Conference on Information Security Theory and Practice, WISTP 2018*, Brussels, Belgium, vol. 11469, pp. 174-189, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Angela S.M. Irwin and Adam B. Turner, "Illicit Bitcoin Transactions: Challenges in Getting to the Who, What, When and Where," *Journal of Money Laundering Control*, vol. 21, no. 3, pp. 297-313, 2018. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Guangcheng Li et al., "Predicting Global Computing Power of Blockchain Using Cryptocurrency Prices," *2019 International Conference on Machine Learning and Cybernetics (ICMLC), Kobe, Japan*, pp.1-6, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Huisi Jang, and Jaewook Lee, "An Empirical Study on Modeling and Prediction of Bitcoin Prices with Bayesian Neural Networks Based on Blockchain Information," *IEEE Access*, vol. 6, pp. 5427-5437, 2017. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Kevin Martin et al., "Combining Blockchain and Machine Learning to Forecast Cryptocurrency Prices," *2020 Second International Conference on Blockchain Computing and Applications (BCCA), Antalya, Turkey*, pp. 52-58, 2020. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Peter D. DeVries, "An Analysis of Cryptocurrency Bitcoin and the Future," *International Journal of Business Management and Commerce*, vol. 1, no. 2, pp. 1-9, 2016. [[Publisher Link](#)]
- [11] Ryan Farrell, "An Analysis of the Cryptocurrency Industry," *Wharton Research Scholars*, vol. 130, pp. 1-23, 2015. [[Google Scholar](#)]
- [12] Meduri V. N. S. S. R. K. Sai Somayajulu, and Bonthu Kotaiah, "A Survey on Cryptocurrency Price Prediction using Hybrid Approaches of Deep Learning Models," *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India*, pp. 1322-1327, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Karunya Rathan, Somarouthu Venkat Sai and Tubati Sai Manikanta, "Crypto-Currency price prediction using Decision Tree and Regression Techniques," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India*, pp. 190-194, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Sirine Sayadi, Sonia Ben Rejeb, and Zied Choukair, "Anomaly Detection Model Over Blockchain Electronic Transactions," *2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), Tangier, Morocco*, pp. 895-900, 2019. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Alex Greaves, and Benjamin Au, "Using the Bitcoin Transaction Graph to Predict the Price of Bitcoin," *No data*, pp. 1-8, 2015. [[Google Scholar](#)] [[Publisher Link](#)]