International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Enhancing Banking Security: A Blockchain and Machine Learning-Based Fraud Prevention Model

Dhruv Patel*

Independent Researcher

Received 01 Dec 2023, Accepted 24 Dec 2023, Available online 26 Dec 2023, **Vol.13, No.6 (Nov/Dec 2023)**

Abstract

Fraudulent activity detection within blockchain networks has become a critical concern due to the widespread adoption of decentralized technologies in financial and digital systems. The paper introduces a system that uses Blockchain and Machine Learning (ML)to strengthen the security of banks. Employing the services of the Ethereum blockchain dataset, the model applies a comprehensive methodology involving data preprocessing, feature engineering, Z-score normalization, and stratified data splitting. Genetic Algorithm-optimized Support Vector Machine (GA-SVM) and Artificial Neural Network (ANN) are constructed and tested, and their results are then compared with those from Generalized Autoregressive Conditional Heteroskedasticity (GARCH) and Convolutional Neural Network (CNN) models. Metrics of accuracy by using Mean Absolute Error (MAE) and Mean Absolute Percentage Error (MAPE) as measures. It was found that the GA-SVM model achieved the best results compared to other models, with MAE at 0.1032 and MAPE at 4.6938 on test data, which confirms its usefulness in real-time fraud detection. When the model connects with smart contracts, it helps prevent fraudulent activities and supports both transparency and good operations in blockchain-based finance.

Keywords: *Blockchain, fraud detection, banking security, GA-SVM, ANN, Ethereum dataset, machine learning, MAE, MAPE, classification.*

Introduction

Digitalization has caused a huge shift in banking, setting the stage for customers to access banking services from the comfort of their smartphones and computers. Because of digital banking, transactions are now quicker, customers enjoy better experiences, and many more people can use financial services. Even so, it has also made financial systems more susceptible to certain threats, the main one being digital fraud. [1][2]. Because digital banking is used more and more, criminals have responded by developing even more advanced fraud techniques. These days, people using financial platforms are experiencing higher rates of phishing attacks, identity theft and unauthorized transfers [3][4][5][6]. Such cases of fraud result in losing substantial amounts, reduce trust in companies and tarnish the reputation of financial firms. The fast rise in digital financial fraud proves that it is time for us to use more effective and active security methods.

Firewalls, multi-factor authentication and encryption have been used for a long time as important security measures in banking [7][8]. Even so, these procedures are mainly limited to border checks or a set of guidelines, so they notice fraud after it happens. Intelligent, real-time warning for threats is sorely missing, which puts security at great risk. Banking systems now need to use active, modern options that keep up with any new dangers and prevent unauthorized acts before they are carried out [9].

In this situation, blockchain is helping to make banking security stronger [10][11]. Since blockchain is not a single system but decentralized, immutable and transparent, it is a very secure environment for managing and recording financial transactions [12][13][14]. It limits the possibility of unauthorized changes since there are no key central points for attackers. On top of this, smart contracts take care of checking and executing transactions using rules, which leads to fewer errors or incidents of fraud because manual action is not needed [15][16][17][18].

The safety and reliability of transactions with blockchain are enhanced by ML, as it can spot fraud with improved intelligence. With historical transaction data, ML algorithms become capable of noticing regularities, unusual activities and strange behaviors [19][20][21]. Models working on a blockchain network can use quality data in real time, therefore detecting and preventing fraud more correctly and efficiently

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.13.6.10

[22][23][24]. Blockchain and ML are used in the model to ensure data safety and instant threat detection, turning usual banking protection into an active and efficient system for all [25][26][27][28].

Motivation and Contribution

The reason for this work is to improve how fraud is detected, as the amount and detail of data in Ethereum-like blockchains keeps rising. To find advanced fraudulent activities, manual analysis is not enough and automated approaches are required. This model is based on blockchain and ML to sort out and catch fraudulent transactions in the Ethereum blockchain. Its objective is to set up a system that automatically analyzes Ethereum transactions, identifies unusual cases and cuts down on misleading fraud detection signals. It relies on ML algorithms to make decisions more accurately and deliver a flexible approach that fits the requirements of live blockchain settings. The most important contributions are:

It is suggested that merging Ethereum blockchain information and ML approaches can help reduce fraud. Using advanced models to study Ethereum transactions is a strong and scalable way to detect fraud, as proposed by their model.

Preprocessing data consists of cleaning up, deleting outliers and normalizing Z-scores to maintain its high quality and consistency.

To validate the effectiveness, ML models like GA, SVM, ANN and CNN are used for classification and their performance is reviewed against GARCH.

The evaluation of the model uses MAPE and MAE measures which in turn helps develop a solid and usable fraud prevention framework..

Novelty with Justification

The study is innovative because data is prepared using advanced methods, class balancing techniques are included, and a combination of ML models is used for fraud detection in the Ethereum blockchain. The framework relies on several classifiers, like GA-SVM and ANN, which makes it strong at detecting different types of fraud. An assessment against GARCH and CNN models indicates that the suggested method is more accurate in predicting. This contribution advances the development of scalable, intelligent, and accurate fraud detection systems tailored for decentralized blockchain environments, enhancing both security and trust in digital financial ecosystems.

Structure of the Paper

Methodologically, this research is structured as follows: A thorough analysis of the body of research on blockchain fraud detection is given in Section II. Section III describes the approach that will be used. Section IV provides a study of the performance and outcomes of the experiments. Finally, Section V concludes and suggests avenues for further investigation into bolstering security and detecting fraud in decentralized banking and financial systems.

Literature Review

Here it go over the literature review on ML-based blockchain fraud detection. Table I also summarizes the literature reviews that will be covered later on:

Gedela and Karthikeyan (2022) identify instances of credit card theft. The Adaboost algorithm is employed, and its performance is evaluated by comparing it to other ML techniques. Metrics like accuracy, sensitivity, and performance of an algorithm are measured using specificity, precision, and F-score. AdaBoost, with detection accuracies of 99.43%, 90.93%, 95.35%, and 94.81%, respectively, LR, NB, ANN, and decision tree approaches perform well. The AdaBoost algorithm achieved a $p<0.05$ significance level and an F-score of 99.48%. According to the results of the qualitative study, compared to the NB, LR, ANN, and DT algorithms, the AdaBoost method was the most effective in identifying instances of credit card fraud [29].

Pranto et al. (2022) More and more cases of financial fraud are cropping up, even though technology has advanced recently. Concerns about privacy and a lack of cooperation between different organizations make it difficult to get accurate information on financial transactions. But data-driven technologies, such as ML, need valid data to facilitate collaboration across organizations, which is necessary to build a robust ML algorithm for e-commerce fraud detection, so these systems can operate properly in the real world. The difficulty of updating the ML model determines the incentives supplied to the organizations. Finally, the blockchain network is tested under different data amounts and difficulty levels to assess its performance. With a testing accuracy of 98.93%, the model showed that the volume of data correlates positively with the degree of difficulty of the blockchain in terms of mining time [30].

Amponsah, Adekoya and Weyori (2022) suggest integrating ML with blockchain technology to detect and prevent healthcare fraud, particularly in the context of claim processing. A decision tree classification technique is used to classify the initial claims dataset. An Ethereum blockchain smart contract is used to identify and prevent healthcare fraud using the recovered knowledge. In terms of classification accuracy (97.96%) and sensitivity (98.09%), the top tool outperformed the others in the comparative test. This indicates that the suggested solution improves the 97.96% accuracy of the blockchain smart contract's fraud detection [31].

Deng et al. (2021) the safety of international financial transactions and trade has been jeopardized by a method that detects fraudulent transactions using a combination of random forest and human detection. When tested on the IEEE CIS fraud dataset, their model outperforms industry standards like logistic regression

and support vector machines. Ultimately, their model achieved a 96.8% accuracy rate and an AUC ROC score of 92.5% [32].

Kim et al. (2021) through data collecting and anomaly detection, Blockchain technology provides a strong cryptographic defense mechanism that analyzes network traffic statistics to identify hostile events. Regularly, the data collection engine creates multi-dimensional data streams by sensing the underlying blockchain traffic. Using traffic data from blockchain networks, the findings demonstrated how well the suggested security system identifies online dangerous situations. Showcase further time complexity reduction with feature prioritization (up to 66.8% for training and 85.7% for testing) without compromising performance [33].

Boughaci and Alkhawaldeh (2020) banking system, focusing on its ability to enhance the protection of online banking operations. Banking industry, with a particular emphasis on its technical functionalities and consensus algorithms. To analyze and assess the technical features of blockchain technology and financial institutions, within the Bitcoin system, the public Elliptic dataset hosted by Kaggle is used. After that, four different ML approaches are used to classify the data, and they all show promise, particularly when k-means is coupled with the random forest classifier, which attains an accuracy of 85% [34].

Table 1 Overview of literature study for blockchain-based fraud detection for banking security

Author	Dataset	Methodology	Analysis	Limitations	Future Work
Gedela and Karthikeyan (2022)	Not specified	AdaBoost in comparison to ANN, Decision Trees, Logistic Regression, and Naive Bayes	AdaBoost achieved 99.43% accuracy and 99.48% F-score; statistically significant ($p < 0.05$)	Dataset not disclosed; lacks contextual or real-time evaluation	Could explore ensemble learning with real-time streaming fraud detection
Pranto et al. (2022)	Simulated cross-organizational financial data	Blockchain integration with ML for collaborative fraud detection	98.93% testing accuracy; 98.22% correlation between mining time and difficulty level/data volume	Real-world authentic datasets were not used due to privacy concerns	Development of privacy-preserving data-sharing frameworks using federated learning
Amponsah, Adekoya, and Weyori (2022)	Healthcare claims dataset	Decision Tree + Ethereum Blockchain Smart Contracts	97.96% accuracy, 98.09% sensitivity	Focused only on claims processing, lacks generalizability to other fraud types.	Expansion to other fraud domains like insurance, banking
Deng et al. (2021)	IEEE CIS Fraud Detection Dataset	Manual Detection + Random Forest	Achieved 96.8% accuracy and 92.5% AUC-ROC	Manual component may hinder scalability	Automation and integration with real-time fraud detection systems
Kim et al. (2021)	Blockchain network traffic data	Blockchain Traffic Monitoring + Feature Prioritization	Reduced training (66.8%) and testing (85.7%) time complexity without loss in performance	Specific to network traffic, not extended to transaction-level fraud	Extend the model to integrate transactional and behavioral analytics
Boughaci and Alkhawaldeh (2020)	Public Elliptic Dataset (Kaggle)	K-means + Random Forest, Blockchain architecture analysis	85% classification accuracy	Limited to Bitcoin transactions; lower accuracy compared to other studies	Integrate advanced ML models and expand to multi-currency/blockchain systems

Methodology

The proposed methodology for enhancing banking security through a Blockchain and ML-based fraud prevention model follows a structured pipeline, as illustrated in Figure 1. The process begins with data preprocessing on the Ethereum Blockchain dataset, including data cleaning, outlier removal, and standardization using Z-score normalization to ensure consistency and improve model performance. Feature engineering techniques are then applied to extract and construct informative attributes from transaction data, such as timestamps, transaction value, and network metrics, enhancing the model's learning capabilities. A fair evaluation of the model is made possible by splitting the dataset into sets for testing (20%) and training (80%). Several classification techniques, including GA, SVM, and ANN, are used.

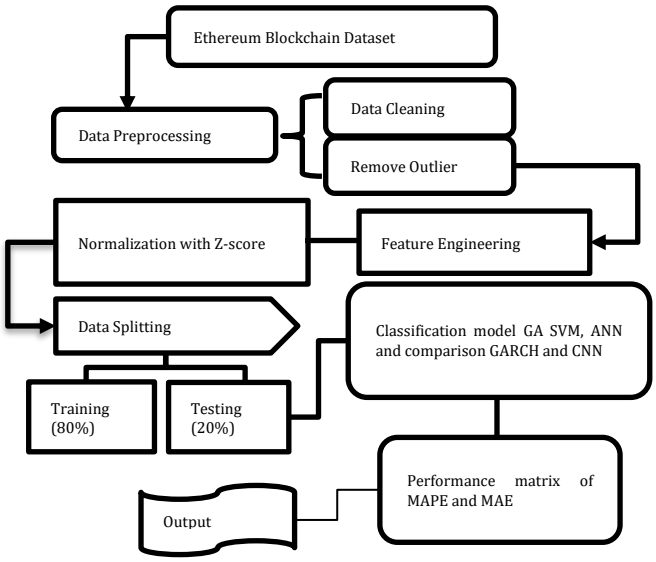

Fig.1 Flowchart for Blockchain-based fraud detection

To assess predicted accuracy, a comparison study is conducted using CNN models and GARCH. To measure the forecasting precision of the models, MAPE and MAE are used. The final model outputs are integrated into the blockchain system via smart contracts to enable fraudulent transaction detection in real time and automatic prevention, thereby improving transparency, security, and operational efficiency in digital banking infrastructures.

Data Collection

The Ethereum blockchain dataset is utilized due to its comprehensive representation of one of the most versatile blockchain networks. The Ethereum Virtual Machine (EVM) allows the execution of smart contracts, expanding blockchain capabilities beyond those of Bitcoin, which mainly records peer-to-peer transactions. Many different types of data are captured by the dataset, including transactional data, smart contract interactions, decentralized application (dApp) activities, and network-level events. This richness makes it highly suitable for developing and evaluating fraud detection models in blockchain-based financial systems.

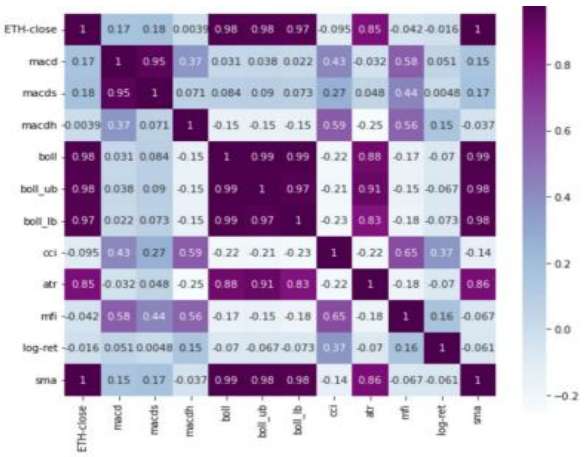

Fig.2 Correlation heatmap of Ethereum blockchain dataset

Figure 2 shows the correlation heatmap of the Ethereum blockchain dataset, highlighting relationships between technical indicators and financial variables. Strong positive correlations are observed between features like ETH-close, boll, sma, and atr, indicating their significance in market trend analysis. In contrast, indicators such as macdh, cci, and log-ret show weaker or negative correlations. This analysis supports effective feature selection for fraud detection and transaction forecasting models.

Figure 3 presents a pair plot visualization of key Ethereum blockchain features, including gas Limit, transaction Count, size, difficulty, burnt Fees ETH, and block Seconds. There is a scatter plot for each combination of features and the elements along the diagonal present the distribution of every single variable. Points marked as red and blue in the chart probably indicate different types of transactions such as fraudulent and normal ones. It supports the finding of patterns, special or unusual cases, relevant links and capability of features to stand out as categories important for blockchain fraud detection.

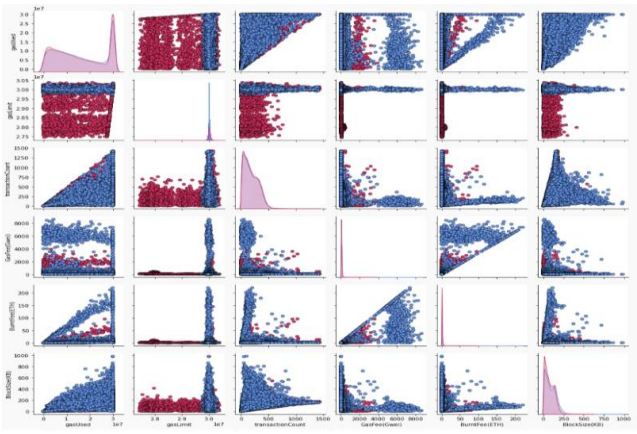

Fig.3 Pair plot of Ethereum blockchain feature

Data Preprocessing

The Ethereum Blockchain dataset is preprocessed to improve the accuracy and security of its data. In this stage, the researcher handles and cleans data with missing or wrong readings and deletes outliers that may negatively affect the model's outcome. Typically, the gathered data should be processed to support strong performance in blockchain fraud detection through its creation and training into models.

Data cleaning: A proper data cleaning process should be used to obtain high-quality input for fraud detection models. In terms of blockchain data, there can be lots of unnecessary entries, errors, missing parts, extra details and mismatched data in the raw transaction logs which can hamper the quality of the trained model.

Remove outlier: Extreme values in blockchain-based fraud detection features need to be identified and removed to prevent performance distortion of models. Common techniques include the Interquartile Range method outliers could also represent actual fraudulent activity.

Feature Engineering

Feature engineering in blockchain-based fraud detection involves creating meaningful features from raw data, such as transaction frequency, average value, and time gaps between transactions [35]. Categorical variables are encoded, and statistical or behavioral patterns are extracted Key techniques include extracting time-based features, transaction frequency, time gaps, statistical features average transaction value, variance, and behavioral patterns sudden spikes in activity or repeated transactions to the same address categorical data such as wallet type or transaction.

Normalization with Z-Score

The Z-score normalization process makes characteristics comparable by standardizing them to possess a standard deviation of 1 and a mean of 0. Because transaction amounts and frequency can vary greatly, this is particularly crucial in the identification of fraud. By applying Z-score normalization, models can better identify in Equation (1):

$$Z = \frac{x-\mu}{\sigma} \quad (1)$$

where σ is the standard deviation, μ is the mean, and x is the initial value. This technique helps scale features like transaction amount or frequency, making certain that every feature adds the same amount to the model. In terms of detecting fraud duties, Z-score normalization is very helpful.

Data Splitting

The train test split to divide the dataset in half, creating a training set and a testing set with a ratio of 80:20. The stratification of the data necessitates the separation of the training and testing sets.

Proposed Model of GA-SVM and ANN Model

The GA-SVM and ANN models are discussed in this section below:

Genetic Algorithm-Optimized SVM (GA-SVM)

The GA-SVM is a hybrid ML model that uses evolutionary computation to optimize SVM hyperparameters for enhanced classification performance. SVM is a statistical theory-based ML technique that has outstanding generalization and applicability [36]. This approach has special benefits for identifying patterns in tiny training sets.

The model found in Equations (2–5) corresponds to the hyperplane in the feature space.

$$y = w^T x + b (2)$$

In this scenario, x stands for the input set, y for the output set, w^T for the normal vector that dictates the hyperplane's orientation, and b for the offset.

$$\min_{w,b} \frac{1}{2}\|W\|^2 \quad (3)$$

subject to $yi(wTxi+b) \geq 1, i=1, \cdots, m$

The optimization challenge is resolved by mapping x to a higher-dimensional feature space using an appropriate kernel function.

$$\min_{\alpha} \frac{1}{2}\sum_{i=1,j=1}^{n} y_i\, y_j \alpha_i \alpha_j k(x_i, x_j) - \sum_{i=1}^{n} \alpha_j (4)$$

subject t $\sum_{i=1}^{n} y_i, \alpha_j = 0, i=1\cdots, l$ build the decision-making function:

$$f(x) = sgn\left(\sum_{i=1}^{l} \alpha_i\, y_i k(x_i, x_j) + b\right) \quad (5)$$

When SVM is used for classification, its performance is affected by both the kernel parameter and the error penalty parameter. GA-SVM, which to find the best values for the parameters c and g in a certain domain for support vector machines (SVM), which has the benefit of fitting large-scale parallel processes and improved overall optimizing potential. With GA-SVM, the classification accuracy was improved.

Artificial Neural Network (ANN)

In ML, an ANN is a nonparametric nonlinear model that is commonly used to circumvent the shortcomings of linear models. With no presumptions regarding the underlying model, ANN is suitably built using the features taken from the actual data. At least three layers make up an ANN as well: input, hidden, and output. Figure 4 displays the single hidden layer forecasting ANN:

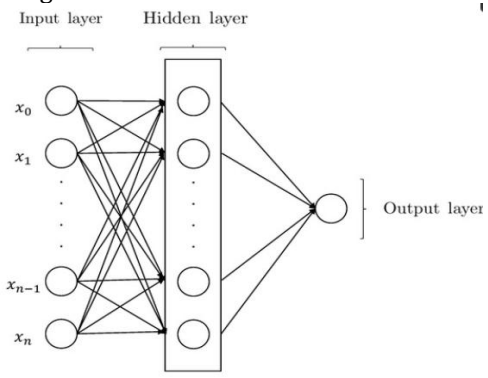

Fig.4 Structure of ANN model

The following is the typical output result from the input and hidden layers. It is shown in Equation (6)

$$output = f(\sum_{i=0}^{n} x_i w_i) \quad (6)$$

where xi and wi represent the weight attached to the connection to node I, the set of node I's input data, where f is a primary activation mechanism. The activation has been successful. There is a great deal of sensitivity to seemingly little changes to the input variables in the sigmoid function. Effective categorization results from the characteristics of this classifier function. The hyperbolic tangent function (Tanh) outperforms the sigmoid function among all activation functions. Because the derivative of the function produces a steep slope, learning and grading happen more quickly.

Performance Metrics

This segment presents an extensive examination of the performance metrics acquired from testing the fraud

prevention model, which integrates blockchain and ML. Particular attention is given to MAE and MAPE evaluation metrics. The prediction accuracy of the model with its fraud detection errors is measured using these parameters. The study demonstrates how blockchain technology combined with ML methods produces extremely precise, transparent, and dependable fraud prevention solutions. The next two evaluation metrics are presented in the discussion below:

Mean Absolute Percentage Error (Mape)

The scale dependency of absolute error makes it an inappropriate method to assess the predictive accuracy of forecasting models when applied to various time series [37]. As a result, the percentage error measurements are added to them, MAPE and formula is evaluated in Equation (7):

$$MAPE = \frac{100}{N}\sum_{t=1}^{N}\left|\frac{\hat{x}_t - x_t}{x_t}\right| \quad (7)$$

Mean Absolute Error (MAE)

The multiple norms serve as measurement standards for forecasting impreciseness. The L1 type MAE uses the mean of the absolute values that deviate between the predicted and actual values in order to compute the outcomes, while following the formula shown in Equation (8):

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|\hat{x}_t - \hat{x}_t| (8)$$

These matrices are utilized to determine the ML and DL models

Result Analysis and Discussion

This section provides result analysis for Blockchain-based fraud detection using ML and DL on the Ethereum blockchain dataset model across performance metrics including MAPE and MAE. The experimental setup was implemented using the Python programming language within environments such as Jupyter Notebook, data processing, and visualization. The computations were performed on a hardware platform equipped with an NVIDIA GTX 1660 Ti GPU (16 GB RAM), ensuring sufficient resources to handle the effective training and assessment of the suggested models. The following sections provide the results of the proposed model for Blockchain-based fraud using GA SVM and ANN model.

Table 2 GA-SVM and ANN model on Blockchain based fraud detection for Ethereum blockchain dataset

Technique	Training		Testing	
	MAE	***MAPE***	***MAE***	***MAPE***
GA-SVM	0.0945	4.4697	0.1032	4.6938
ANN	0.0978	4.5860	0.1076	4.7139

Table II uses error measures, such as MSE, MAPE, and MAE, to evaluate the effectiveness of ANN and GA-SVM models throughout the training and testing phases. The GA-SVM model demonstrates marginally better accuracy, with lower MSE (0.0945 vs. 0.0978), MAPE (4.4697 vs. 4.5860), and MAE (0.1032 vs. 0.1076) in training, as well as superior testing performance (MAPE: 4.6938 vs. 4.7139). These results suggest that GA-SVM exhibits slightly stronger predictive capability compared to ANN for the given task, blockchain-based fraud detection.

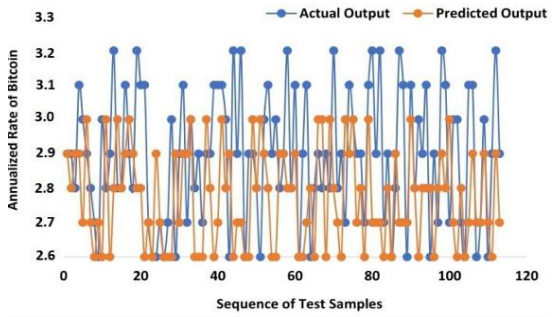

Fig.5 Prediction of GA-SVM

Figure 5 shows the prediction of the GA-SVM model, illustrating the comparison between actual and predicted outputs for a dataset, visualized as a fluctuating line plot. The test sequence exists along the x-axis and the Bitcoin annual rate exists along the y-axis. The actual output uses blue lines in this model but the predicted output utilizes orange lines. The model shows strong capability to capture actual data changes because both series present significant variations, even though some deviation points exist.

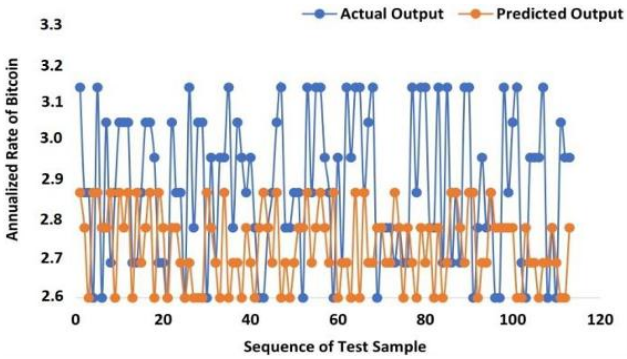

Fig.6 Prediction of ANN

The prediction results from an Artificial Neural Network (ANN) model appear in Figure 6. The figure includes Actual Output, Predicted Output, Annualized Rate of Bitcoin, and Test Sample Sequence data. This visual representation shows how well the ANN performs in Bitcoin metric prediction while displaying the matching or different values between forecasted and real outcomes. The visualization helps to measure the model's precision and performance for time-series prediction operations.

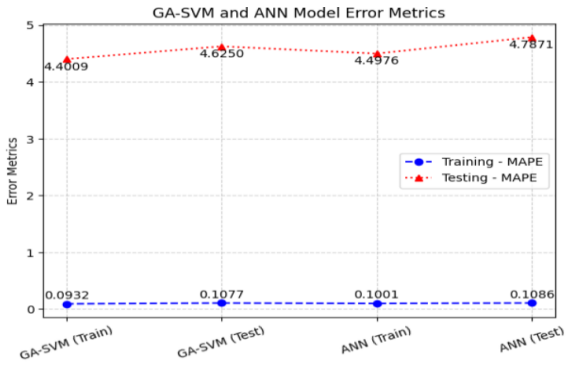

Fig.7 Error metrics of GA-SVM and ANN model

Figure 7. The graph displays the error performance of GA-SVM and ANN models through MAPE during the training and testing phases. The Testing-MAPE results reveal an overfitting issue because they surpass the Training-MAPE measurements for both GA-SVM and ANN models. The Training-MAPE for GA-SVM stands at 0.0932, and the Testing-MAPE reaches up to 4.4009, but the Training-MAPE for ANN checks in at 0.1001 with Testing-MAPE reaching 4.4976. The Testing-MAPE elevates from training to testing for both models, where GA-SVM achieved 4.6250 and ANN achieved 4.7871, indicating diminished performance of the models when operating on new data.

Discussion

This section includes an assessment of blockchain-based fraud detection methods. The analysis demonstrates a comparison between the developed GA SVM model and existing approaches, ANN, GARCH, and CNN, through performance metric evaluation using MAE and MAPE measurements presented in Table III. The GA SVM model achieves better results than other methods because it provides superior accuracy and efficiency when detecting fraud in blockchain systems.

Table 3 Comparison between GA SVM and ANN, Existing models for Blockchain-based fraud

Measure	Proposed Model		Comparison Model	
	GA SVM	***ANN***	***GARCH***[38]	***CNN***[39]
MAE	0.1032	0.1076	60.7172	29.61
MAPE	4.6938	4.7139	18.21	4.79

The research compares the proposed GA-SVM model to ANN alongside GARCH and CNN using Table III to assess their performance for fraud detection using blockchain technology. MAE and MAPE are crucial metrics for evaluating model correctness and dependability in predictive model evaluation. The GA-SVM model demonstrates superior performance compared to ANN because it produces the best results with an MAE of 0.1032 and an MAPE value of 4.6938. The GARCH model produces unsatisfactory results when processing complex blockchain data since it yields high error metrics of 60.7172 MAE and 18.21 MAPE. The CNN model, while competitive, records a higher MAE of 29.61 and a MAPE of 4.79. The GA-SVM model demonstrates better accuracy, together with the highest reliability in identifying fraudulent transactions in blockchain financial systems, according to these experimental findings.

High-quality predictions with low mistakes are due to the GA SVM model applied on blockchains, as seen in the MAE (0.1032) and MAPE (4.6938) values. It succeeds in reaching optimal results by analyzing detailed transactions and spotting data that does not follow normal patterns in blockchain records, despite having noisy or unorganized data. The use of evolutionary optimization in SVM through genetic algorithms allows it to improve its performance by adjusting hyperparameters for the best results while classifying.

Conclusion and Future Work

The use of Predictive analysis, artificial intelligence, blockchain technology, and risk mitigation techniques has revolutionized financial security systems. The implementation of these modern technologies allows for instant fraud control and automated compliance documentation as well as advanced forensic auditing, which minimizes business fraud risks. Moreover, it launches a blockchain ML-based fraud defense architecture to boost banking safety measures. In order to strengthen banking security measures, this study presents a novel fraud prevention system that combines blockchain technology with enhanced ML algorithms. The proposed GA-SVM model achieves top performance when used with Ethereum blockchain data to detect fraud, which surpasses traditional models, including ANN, GARCH, and CNN, because it shows better results according to MAE and MAPE. A Genetic Algorithm included for Support Vector Machine hyperparameter optimization produces higher classification precision while establishing strong abilities to detect abnormal transaction patterns. Experimental evaluations confirm the model's capability to handle feature complexity and data imbalance, thereby demonstrating its practical applicability for financial fraud detection in decentralized environments.

Future work will focus on expanding the framework to multi-chain environments for cross-platform fraud analysis, real-time deployment using smart contracts for autonomous prevention, and the incorporation of explainable AI techniques to improve automated decision-making systems' transparency and reliability.

References

[1] M. F. Mridha, K. Nur, A. K. Saha, and M. A. Adnan, "A New Approach to Enhance Internet Banking Security," *Int. J. Comput. Appl.*, vol. 160, no. 8, pp. 35–39, Feb. 2017, doi: 10.5120/ijca2017913093.
[2] D. D. Rao, A. A. Waoo, M. P. Singh, and F. Paul, "Breaking Down Barriers: Scalability and Performance Issues in Blockchain-Based Identity Platforms Achieving Scalable and High-Performance Blockchain-Based Identity Systems," 2021.

[3] F. Twum and K. Ahenkora, "Internet Banking Security Strategy: Securing Customer Trust," *J. Manag. Strateg.*, 2012, doi: 10.5430/jms.v3n4p78.
[4] S. Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.
[5] V. Kolluri, "A Detailed Analysis of AI as a Double-Edged Sword: AI-Enhanced Cyber Threats Understanding and Mitigation," *Int. J. Creat. Res. Thoughts*, vol. 8, no. 7, 2020.
[6] S. S. S. Neeli, "Leveraging Docker and Kubernetes for Enhanced Database Management," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, p. 5, 2022.
[7] A. Khelifi, M. Aburrous, M. A. Talib, and P. V. S. Shastry, "Enhancing Protection Techniques of E-Banking Security Services Using Open Source Cryptographic Algorithms," in *2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 2013, pp. 89–95. doi: 10.1109/SNPD.2013.47.
[8] N. Malali, "The Role of Devsecops in Financial AI Models: Integrating Security at Every Stage of AI/ML Model Development in Banking and Insurance," *Int. J. Eng. Technol. Res. Manag.*, vol. 6, no. 11, 2022, doi: 10.5281/zenodo.15239176.
[9] H. Guo and X. Yu, "A Survey on Blockchain Technology and Its Security," *Blockchain Res. Appl.*, vol. 3, no. 2, Jun. 2022, doi: 10.1016/j.bcra.2022.100067.
[10] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.
[11] V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," *Lib. Media Priv. Ltd.*, 2022.
[12] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.
[13] J. Thomas, P. Patidar, K. V. Vedi, and S. Gupta, "Predictive Big Data Analytics For Supply Chain Through Demand Forecasting," *Int. J. Creat. Res. Thoughts*, vol. 10, no. 06, pp. h868–h873, 2022.
[14] S. Tyagi, T. Jindal, S. H. Krishna, S. M. Hassen, S. K. Shukla, and C. Kaur, "Comparative Analysis of Artificial Intelligence and its Powered Technologies Applications in the Finance Sector," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, IEEE, Dec. 2022, pp. 260–264. doi: 10.1109/IC3I56241.2022.10073077.
[15] A. O. I. Hoffmann and C. Birnbrich, "The Impact of Fraud Prevention on Bank-Customer Relationships," *Int. J. Bank Mark.*, vol. 30, no. 5, pp. 390–407, 2012, doi: 10.1108/02652321211247435.
[16] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.
[17] S. Murri, "Data Security Environments Challenges and Solutions in Big Data," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 565–574, 2022.
[18] S. S. S. Neeli, "Key Challenges and Strategies in Managing Databases for Data Science and Machine Learning," *Int. J. Lead. Res. Publ.*, vol. 2, no. 3, p. 9, 2021.
[19] M. T. Oladejo and L. Jack, "Fraud Prevention and Detection in a Blockchain Technology Environment: Challenges Posed to Forensic Accountants," *Int. J. Econ. Account.*, vol. 9, no. 4, p. 1, 2020, doi: 10.1504/IJEA.2020.10032205.
[20] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.
[21] V. Kolluri, "An Innovative Study Exploring Revolutionizing Healthcare with AI: Personalized Medicine: Predictive Diagnostic Techniques and Individualized Treatment," *Int. J. Emerg. Technol. Innov. Res.*, vol. 3, no. 11, pp. 2349–5162, 2016.
[22] N. Malali, "Using Machine Learning to Optimize Life Insurance Claim Triage Processes Via Anomaly Detection in Databricks: Prioritizing High-Risk Claims for Human Review," *Int. J. Eng. Technol. Res. Manag.*, vol. 6, no. 6, 2022, doi: 10.5281/zenodo.15176507.
[23] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.
[24] A. Gogineni, "Multi-Cloud Deployment with Kubernetes: Challenges, Strategies, and Performance Optimization," *Int. Sci. J. Eng. Manag.*, vol. 1, no. 02, 2022.
[25] S. Hisham, M. Makhtar, and A. A. Aziz, "A comprehensive review of significant learning for anomalous transaction detection using a machine learning method in a decentralized blockchain network," *International Journal of Advanced Technology and Engineering Exploration*. 2022. doi: 10.19101/IJATEE.2021.876322.
[26] S. Pandya, "Innovative blockchain solutions for enhanced security and verifiability of academic credentials," *Int. J. Sci. Res. Arch.*, vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.
[27] M. Shah and A. Gogineni, "Distributed Query Optimization for Petabyte-Scale Databases," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 10, pp. 223–231, 2022.
[28] A. Polleri, R. Kumar, M. M. Bron, G. Chen, S. Agrawal, and R. S. Buchheim, "Identifying a Classification Hierarchy Using a Trained Machine Learning Pipeline," U.S. Patent Application No. 17/303,918, 2022
[29] B. Gedela and P. R. Karthikeyan, "Credit Card Fraud Detection using AdaBoost Algorithm in Comparison with Various Machine Learning Algorithms to Measure Accuracy, Sensitivity, Specificity, Precision and F-score," in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022. doi: 10.1109/ICBATS54253.2022.9759022.
[30] T. H. Pranto, K. T. A. M. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach," *IEEE Access*, vol. 10, pp. 87115–87134, 2022, doi: 10.1109/ACCESS.2022.3198956.
[31] A. A. Amponsah, A. F. Adekoya, and B. A. Weyori, "A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology," *Decis. Anal. J.*, 2022, doi: 10.1016/j.dajour.2022.100122.
[32] W. Deng, Z. Huang, J. Zhang, and J. Xu, "A Data Mining Based System for Transaction Fraud Detection," in *2021 IEEE International Conference on Consumer Electronics and Computer Engineering, ICCECE 2021*, 2021. doi: 10.1109/ICCECE51280.2021.9342376.
[33] J. Kim *et al.*, "Anomaly Detection based on Traffic Monitoring for Secure Blockchain Networking," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–9. doi: 10.1109/ICBC51069.2021.9461119.
[34] D. Boughaci and A. A. K. Alkhawaldeh, "Enhancing the security of financial transactions in Blockchain by using machine learning techniques: towards a sophisticated security tool for banking and finance," in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, 2020, pp. 110–115. doi: 10.1109/SMART-TECH49988.2020.00038.
[35] C. Jatoth, R. Jain, U. Fiore, and S. Chatharasupalli, "Improved Classification of Blockchain Transactions Using Feature Engineering and Ensemble Learning," *Futur. Internet*, vol. 14, no. 1, 2022, doi: 10.3390/fi14010016.
[36] Y. Zhang, J. Yu, C. Xia, K. Yang, H. Cao, and Q. Wu, "Research on GA-SVM Based Head-Motion Classification via Mechanomyography Feature Analysis," *Sensors*, vol. 19, no. 9, 2019, doi: 10.3390/s19091986.
[37] M. Kostmann and W. K. Härdle, "Forecasting in Blockchain-Based Local Energy Markets," *Energies*, vol. 12, no. 14, 2019, doi: 10.3390/en12142718.
[38] M. Seo and G. Kim, "Hybrid forecasting models based on the neural networks for the volatility of bitcoin," *Appl. Sci.*, vol. 10, no. 14, 2020, doi: 10.3390/app10144768.
[39] B. Aygun and E. K. Gunay, "Günlük Bitcoin Değerini Tahmin Etmek İçin İstatistiksel ve Makine Öğrenimi Algoritmalarının Karşılaştırılması," *Eur. J. Sci. Technol.*, 2021, doi: 10.31590/ejosat.822153.