International Journal on Smart & Sustainable Intelligent Computing
Vol. 02, Iss. 01, S. No. 002, pp. 14-30, March 2025
ISSN (Online): 3048-8508

Enhancing Blockchain Transaction Security: A Hybrid Machine Learning Approach for Fraud Detection

Ankita Ghosh[1], Sudip Diyasi[2]*, Dipankar Dey[3]

[1]Department of Computer Application, George College of Management and Science, Kolkata, India
[2, 3]Department of Computer Application, Global Institute of Science and Technology, Haldia, India
ankitaghosh9830@gmail.com, sudipdiyasi1@gmail.com*, deydipankar2014@gmail.com

How to cite this paper: Ankita Ghosh, Sudip Diyasi, Dipankar Dey, "Enhancing Blockchain Transaction Security: A Hybrid Machine Learning Approach for Fraud Detection," *International Journal on Smart & Sustainable Intelligent Computing*, Vol. 02, Iss. 01, S No. 002, pp. 14-30, March 2025.

Received: 19/12/2024
Revised: 10/01/2024
Accepted: 22/01/2025
Published: 05/02/2025

Abstract

A newly proposed hybrid approach that makes use of both supervised and unsupervised machine learning to implement security within blockchain transactions. Blockchain, despite its central role in the decentralized networks and the cryptographic cryptography, is still open to high-end attacks. Making use of random forest, autoencoders, and SVM models to tap their strengths on classification and anomaly detection fights these threats. Normalization and feature selection techniques boost the performance of a model. Thus, the hybrid model demonstrated above surpassing the performance of standalone models in fraud detection and mitigation indicates that this will be a future-proof solution fortified upon emerging threats behind secure digital finance in blockchain.

Keywords

Blockchain, Smart Contract Vulnerabilities, Cyber Threat, Supervised Learning, Unsupervised Learning, Anomaly Detection, Transaction Integrity, Support Vector Machine.

1. Introduction

Blockchain technology is often praised for introducing a secure, decentralized ledger system that removes the need for intermediaries in transactions. Two cardinal features of blockchain decentralization and cryptographic techniques enhance the integrity of transactions in such a way that blockchains are highly resistant to many traditional security threats. However, despite these advantages, blockchain systems are not impervious to vulnerabilities. For example, a 51% attack, in which an attacker or a group of attackers can gain control over most of the e network's mining power, is one of the most dangerous threats to blockchain integrity [1]. Similarly, vulnerabilities in smart contracts, mostly due to poorly written or vulnerable code, open the door for attackers to exploit these digital agreements, leading to huge financial and reputational damage [2]. Such challenges

demand robust, scalable, and adaptive solutions that can pre-emptively identify and mitigate fraudulent or malicious activities.

In response to these challenges, this paper introduces a hybrid machine learning approach that combines supervised and unsupervised techniques for fraud detection, thereby improving transaction security in blockchain systems. Specifically, the study utilizes a combination of Random Forest, Autoencoder, and Support Vector Machine (SVM) models to analyse the "Elliptic Data Set," which contains over 200,000 Bitcoin transactions [3]. This dataset represents a rich source for examining patterns and detecting anomalies. The methodology is designed to maximize effectiveness through rigorous data preprocessing, normalization, and feature selection, ensuring that the models operate on optimized data. By employing precision, accuracy, recall, and F1-score as evaluation metrics, the study demonstrates that the proposed hybrid approach significantly outperforms individual models. These findings provide a robust solution to enhance the security framework of blockchain systems by addressing existing vulnerabilities and pre-empting potential future threats. In addition, this research contributes to several aspects: it proposes an innovative hybrid machine learning model for detecting blockchain fraud; uses a real-world dataset to validate the approach; and applies comprehensive preprocessing, evaluation metrics to ensure reliability and accuracy. Together, these contributions establish a scalable and adaptable framework for improving blockchain transaction security.

2. Background

a. Blockchain Security and its Vulnerabilities

The great pomp and fanfare thrown toward blockchain technology, touting it as both robust and secure, have been founded on two major technologies: decentralization and cryptographic techniques. This feature is meant to protect transaction integrity and data against most conventional security threats through encryption, ensuring that all integrity in transactions and data is guaranteed through the applied consensus mechanisms. This way, decentralization makes sure that control and decision-making processes are diffused within a network of nodes to avoid the risk of central points of failure. These cryptographic techniques provide strong security assurance for the integrity and confidentiality of data through hashing, digital signatures, and encryption. Despite these strict measures for security, blockchains are certainly not completely resistant to various types of attacks. With technological evolution, methods by which malicious actors exploit vulnerabilities or breach security protocols also evolve. This is part of the ongoing cat-and-mouse game of measures against threats, which explains why vigilance and continuous improvement in blockchain security practices are essential. Recent statistics insecure the increasing concerns pertaining to blockchain security:

51% Attacks

These types of attacks have been of significant threat wherein one entity has more than 50% of the mining power of the network. For instance, in 2019, the Ethereum Classic network faced different 51% attacks through which approximately $5.6 million were double spent. This attack damages the whole blockchain concept and might result in a heavy financial loss. In particular, the 51% attack threat is great against blockchain networks with less security, so strong security measures and vigilance are essential [4].

Smart Contract Exploits

Famous failures have been caused by vulnerabilities in smart contracts. The most famous case of hacking was against the DAO fund on the Ethereum blockchain. In 2016, hackers exploited a vulnerability in one of the smart contracts and drained $60 million worth of Ether from the fund. Therefore, the event revealed the risks that lay in poorly designed or audited smart contracts. Smart contracts call for rigorous testing, formal verification, and periodic security audits to diffuse the risk factor associated with them [5].

Sybil Attacks

These are attacks where a user creates several Sybil identities with the intent of having disproportionate influence over a network. They are less publicized, but risks to the stability of decentralized networks through the possible skewing of voting and processes of reaching consensus. Sybil attacks can perturb the integrity of the mechanism of consensus and then result in fraudulent behaviour and manipulation of activities on a network. Robust identity verification and reputation systems will help

reduce the impact of Sybil attacks. Besides these specific attack vectors, other risks include phishing attacks, malware, and social engineering techniques against blockchain users and service providers. Cyber threats are getting sophisticated; hence, there is a requirement for a multipronged approach to securing blockchain technology through developments in technology coupled with user education through best practices.

Research and development in the area are hence highly required. Further improved symmetric cryptography methods, more robust consensus algorithms, and systematic security audits of smart contracts are some potential solutions in this regard. Further evolution and constant adaptation keep the blockchain industry ahead of any possible threats, ensuring a safe user environment. Scholars from academia, cybersecurity experts, and stakeholders of the industry must come together in developing innovative solutions that try to protect and uphold the integrity and trust in blockchain technology [6].

b. Machine Learning in Blockchain Security

Network Machine learning is a new and robust tool that equips blockchain security with new threat detection and mitigation methods. Some recent developments and applications in this domain include:

Anomaly Detection

Clustering, auto-encoders, and isolation forests are common ways to detect deviations from standard transaction patterns in this domain. For example, unsupervised learning techniques could be applied to detect unusual transaction behaviours that may indicate fraudulent activities.

Fraud Detection

Random Forest and Support Vector Machines are a few examples of supervised learning models that have turned out to be very strong in classifying a transaction as fraudulent or legitimate. Several recent studies have demonstrated that such models significantly improve the detection rate of known fraud patterns.

Predictive Analysis

Machine Learning models, through the analysis of historical data, can approximate and predict the threats that could turn up soon. For example, predictive models were made use of in predicting vulnerabilities, given the trends of emerging attacks, to take proactive measures.

c. Significance of Enhanced Security

The need for robust security solutions in blockchain systems is underlined by the ever-increasing adoption of blockchain technology in a wide array of business fields, including financial services, supply chain management, and healthcare. In tandem with the growth of blockchain applications comes increased potential impact from security breaches. For instance, the financial sector relies on blockchain for secure and transparent transactions. If it is breached, this might mean huge losses both in terms of finances and loss of trust. It is within the management of supply chains that blockchain enhances traceability and accountability, and its vulnerabilities may be exploited to bring an operation to a halt, even adulterating the integrity of the product. In health, blockchain will ensure secure handling of sensitive patient data, but breaches may jeopardize patient privacy and safety.

With blockchain technology now spreading its reach across various industries, the already high stakes for ensuring robust security have dramatically gone up. The wide range of uses of blockchain, from voting systems and systems of intellectual property management, is certainly remarkable by itself—gives rise to specific and peculiar security challenges. These challenges dictate a more proactive approach in the voice of potential vulnerabilities and recommend neutralizing them before malicious actors manage to exploit them. In other words, even though blockchain technology provides a secure foundation, one needs to continuously improvise upon the security facing emerging threats. Since the threat scenario in the cyber field is always changing, innovation and improvement of security practices must be continuous. The infusion of machine learning techniques offers a promising avenue for improving transaction security and mitigation of risk. Machine learning can analyse vast transaction data in real-time for patterns and anomalies indicative of fraudulent activities. Blockchain systems can set in mo-

tion advanced algorithms and models that predict the threat of attack and hence minimize the risk of successful attacks by automatically detecting and responding to threats.

The hybrid approach derives the power of supervised and unsupervised learning to provide a single, all-encompassing solution in fraud detection on blockchains. Supervised learning is useful in recognizing known forms of fraud, given that models are trained from labelled data and thus alert the user to any suspicious activities. Unsupervised learning methods are very good at detecting new, unseen threats by deviating normal behavioural patterns. Such a combined approach would more suitably help accommodate a robust, adaptive security framework to accommodate the vast array of threats that could very well materialize. This will also enhance other security features, such as identity verification and access control, by further integrating machine learning into blockchain technology. Machine learning algorithms can analyse behavioural biometrics and transaction histories to construct more accurate and dynamic user profiles, hence significantly reducing instances of identity theft and unauthorized access. From this comprehensive approach to security will emerge stronger trust in blockchain systems, which will encourage wider adoption and allow the technology to realize its full potential. It is only through collaboration opportunities between blockchain developers, cybersecurity experts, and machine learning researchers that the industry will come up with innovative solutions ahead of the emerging threats. Basic building blocks of a secure strategy would be continuous monitoring, regular security audits, and adoption of best practices. Only then can the blockchain community be assured that this technology remains a reliable and secure platform for many applications and continues to foster innovation and growth in the digital age.

d. Strengths and Weaknesses of Each Model

This has the advantage of robustness and high accuracy, with strengths in transaction classification due to its ensemble nature. After aggregating the predictions from several decision trees, it achieved a precision of 0.93 and a recall of 0.90, thus proving to be efficient in the reduction of false positives and the detection of true positives. Moreover, it gives an insight into feature importance. However, if not cared for, even random forests can suffer from overfitting. Besides, their complexity requires extensive hyperparameter tuning. Again, while adept at classification, random forests may not handle anomaly detection as powerfully as unsupervised methods. Autoencoders are very good at detecting anomalies because they learn the patterns of normal transactions and recognize deviations from them. This unsupervised ability to work is particularly useful, as there is usually a lack of fraud data labelled in most cases. Such an approach achieved a precision of 0.88 and a recall of 0.85, thereby showing their potential in detecting new patterns of fraud. Even with these advantages, auto-encoders may generate high reconstruction errors with both real anomalies and benign deviation types that may result in false positives. This can also be challenging to the model's complexity of training and interpretability. The strengths of SVMs lie in high-dimensional spaces, and they are resistant to overfitting if appropriate kernels and regularization are used. Their classification works very well, with a precision of 0.85 and a recall of 0.80. However, SVMs can turn out to be computationally expensive, especially for large data, and performance can get sensitive to the choice of kernel functions and hyperparameters. It is also partly because SVMs are primarily designed for classification rather than anomaly detection, and hence it is restricted in terms of how effective they will be at identifying fraudulent transactions. While K-means Clustering does provide simplicity and speed, for this reason, it is computationally efficient for large datasets. It also works well while trying to cluster well-separated data points. However, the assumptions of K-means include spherical clusters and equal-sized clusters, some of which may be in contradiction to the nature of fraudulent transactions. Its sensitivity to initialization and limited ability to handle anomalies or outliers further restrain its performance, already shown by its lower precision and recall compared to other models.

e. Insights into Why the Hybrid Approach Performed Best

The hybrid approach, which blends both, performs very well-by using the power of each of the models and at the same time mitigating their individual shortcomings. This approach marries the robust classification capabilities of Random Forests with the anomaly detection methods of Autoencoders to provide complete coverage against various fraud types. Random Forests alone are very effective in classifying known types of fraudulent transactions, since they can accommodate large datasets and a wide variety of features. On the other hand, auto-encoders aim to learn expressive representations of data, which makes them very good at recognizing anomalies that deviate from standard patterns.

This combination enhances the overall detection capability, assuring better performance in both precision and recall. Precision assures that very few of the cases of fraud identified are not fraudulent, thereby reducing the incidence of false positives, which would need investigation and thus waste resources. Recall assures that most, if not all, fraudulent cases will be detected, thus minimizing false negatives and assurance that very few fraudulent activities go undetected. These two techniques complement each other; hence, synergy in the development of a more reliable, accurate fraud detection system.

The Random Forests reduce false positives, while Autoencoders are effective against novel and evolving fraudulent activities. Random Forest works by using ensemble methods to aggregate the predictions of many decision trees to help smooth out biases and lower the likelihood of false alarms. This would ensure trust and efficiency in blockchain systems; riddled with false positives, blockchain will erode in confidence among its users and disrupt lawful transactions. On the other hand, auto-encoders can learn from the data itself and do not require labelled examples; in this line, they are very useful to detect new and emerging kinds of fraud that have not previously been encountered. The hybrid model can balance a range of evaluation metrics, from F1-score to accuracy, showing the effectiveness of this system in minimizing both false positives and negatives. It's just the unscaled mean of precision and recall, often referred to as the F1 score. Since these two are combined, it gives one metric that will balance the trade-offs between those two important features of fraud detection. High accuracy is responsible for the reliable overall performance of the model; however, the balance achieved in the F1-score sheds very bright light on the model's real-world effectiveness for problems where both precision and recall matter. This offers a more versatile and effective solution to securing blockchain transactions by addressing the limitations of individual models. The flexibility brought about by this approach is, therefore, able to react to the dynamic nature of fraud tactics that are employed over time, which keeps its security measures in line. The hybrid model learns from new data and improves detection capability, an essential property if integrity and security are to be maintained in blockchain systems. Furthermore, the hybrid approach is tailored for a particular blockchain application and industry to provide solutions that meet the special security requirements of that industry. This flexibility can ensure the correct implementation of the hybrid model in all different scenarios-from financial services and supply chain management, enhancing the security posture of blockchain technology in general.

It offers an overall balanced and all-around method of fraud detection. It thus combines the advantages of random forests and autoencoders to retain their peak performance while detecting a broad scope of fraudulent activities with high precision and recall. This versatile and efficient solution equates to blockchain transactions with added security, building more trust in blockchain technology. In a world where blockchain adoption continues to enhance, the hybrid approach will become very important as a robust fraud detection mechanism in protecting digital assets and their transactions.

3. Literature Review

Although highly innovative, blockchain technology has been challenged by security risks, particularly in the realm of crypto crimes, as highlighted by increasing fraudulent activities. This section reviews the advancements in blockchain fraud detection, focusing on methodologies such as supervised learning, unsupervised learning, and hybrid approaches.

a. Supervised Learning Techniques

It has also effectively classified fraudulent blockchain transactions using labelled datasets in supervised learning.

- Bello et al. [7] developed a framework combining logistic regression and neural networks to classify transactions and accurately detect fraud patterns. Their work demonstrated the potential of supervised learning in real-time fraud detection.
- Ashfaq et al. [8] use the Random Forest and XGBoost models to analyse blockchain transaction data, which performs very well in identifying emerging fraudulent activities.

Despite their effectiveness, supervised techniques often struggle with novel or emerging fraud tactics due to their reliance on labelled training data.

b. Unsupervised Learning Techniques

Unsupervised learning methods have been pivotal in detecting anomalies without requiring labelled datasets, thus addressing the limitations of supervised approaches.

- Pranto et al. [9] applied clustering algorithms to uncover unusual transaction patterns, demonstrating their ability to detect fraud in blockchain environments.
- Zhao et al. [10] proposed a hybrid model integrating LightGBM and Keras neural networks, emphasizing the use of focal loss to handle imbalanced data distributions. This approach excelled in detecting rare fraudulent transactions.

However, unsupervised models may generate higher false positives because there are no explicit labels.

c. Hybrid Approaches

Hybrid techniques that combine supervised and unsupervised learning methods provide a comprehensive solution for blockchain fraud detection by leveraging the strengths of both approaches.

- Ahmed et al. [11] developed a hybrid framework integrating supervised classification and unsupervised clustering, achieving scalability and adaptability in cryptocurrency fraud detection.
- Shafin et al. [12] integrated autoencoders with neural networks in a blockchain-based anti-money laundering system; their real-time fraud detection can be done with high precision, accuracy, and scalability .

Hybrid models perform excellently for known fraud patterns and emerging threats, thus being the right tool for secure blockchain transactions.

d. Emerging Techniques

Recent studies have introduced advanced methods and frameworks beyond what is conventionally used:

- Yang et al. [13] proposed FinChain-BERT, an NLP-based financial fraud detection model that uses optimized loss functions and lightweight technologies to achieve exceptional accuracy and scalability.
- Taher et al. [14] focused their approach on explainable AI techniques that enhance interpretability without sacrificing high detection accuracy.

These new methodologies cater to issues related to interpretability, resource efficiency, and scalability, adding extra layers of robustness to fraud detection frameworks.

e. General Findings

The literature reviewed reveals several key insights:

- Most supervised learning models excel in detecting known fraud patterns but may struggle with emerging threats.
- Unsupervised methods, such as autoencoders, are effective in identifying novel anomalies but have limitations with imbalanced datasets.
- Hybrid approaches leverage the strengths of both methodologies, providing more robust and adaptable fraud detection systems.
- Emerging frameworks like FinChain-BERT and explainable AI add value by enhancing interpretability and scalability.

This literature review aims to provide an overview of current methodologies and highlight the benefits of combined approaches to enhance blockchain transaction security.

4. Methodology

The proposed methodology of securing blockchain transactions proposes a hybrid anomaly detection system that combines capabilities in supervised and unsupervised machine learning techniques, assuring heightened accuracy in fraud detection. Here is a more detailed workflow of the methodology:

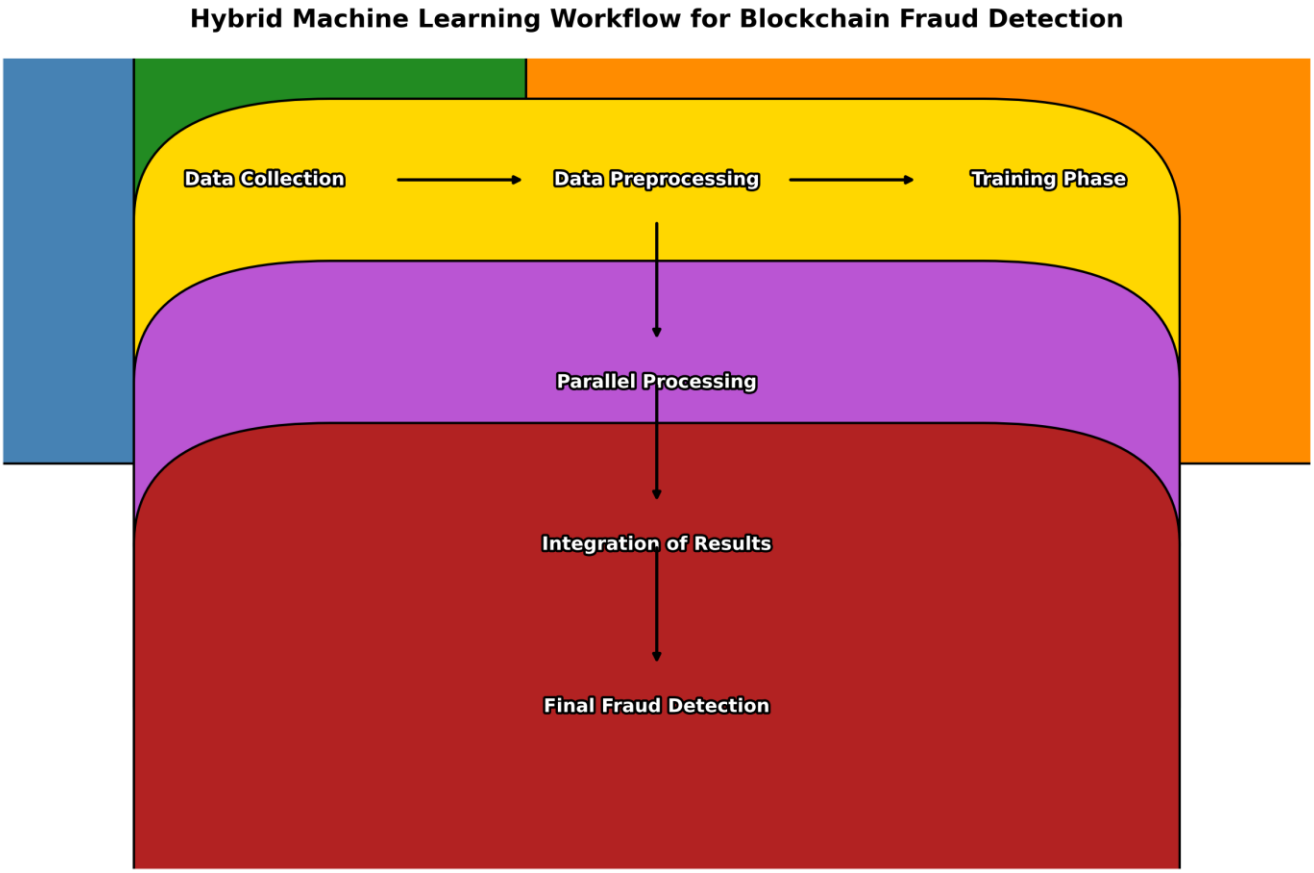

Figure 1. Workflow of the proposed hybrid approach for blockchain fraud detection, integrating supervised and unsupervised machine learning techniques

a. Data Collection

The research used the "Elliptic Data Set" comprising more than 200,000 Bitcoin transactions. Each of the transactions is described by 166 features, including features like the transaction amount and timestamp and other network features. All the transactions within the dataset are labelled as either licit or illicit; the former takes a high percentage in the dataset.

The highly unbalanced existing class distribution significantly impacts the accuracy of machine learning models for correctly classifying fraudulent activities. Figure 2 shows the distribution of legitimate and illegitimate transactions in the dataset, explaining this class representation disparity.

Figure 2 illustrates that legal transactions comprise about 90% of the dataset. Illegal transactions make up about 10%. Such a balance in the dataset makes anomaly detection challenging in this imbalanced dataset. Such imbalances in the data were another challenge in our development, impacting our algorithm selection and choice of evaluation metrics.

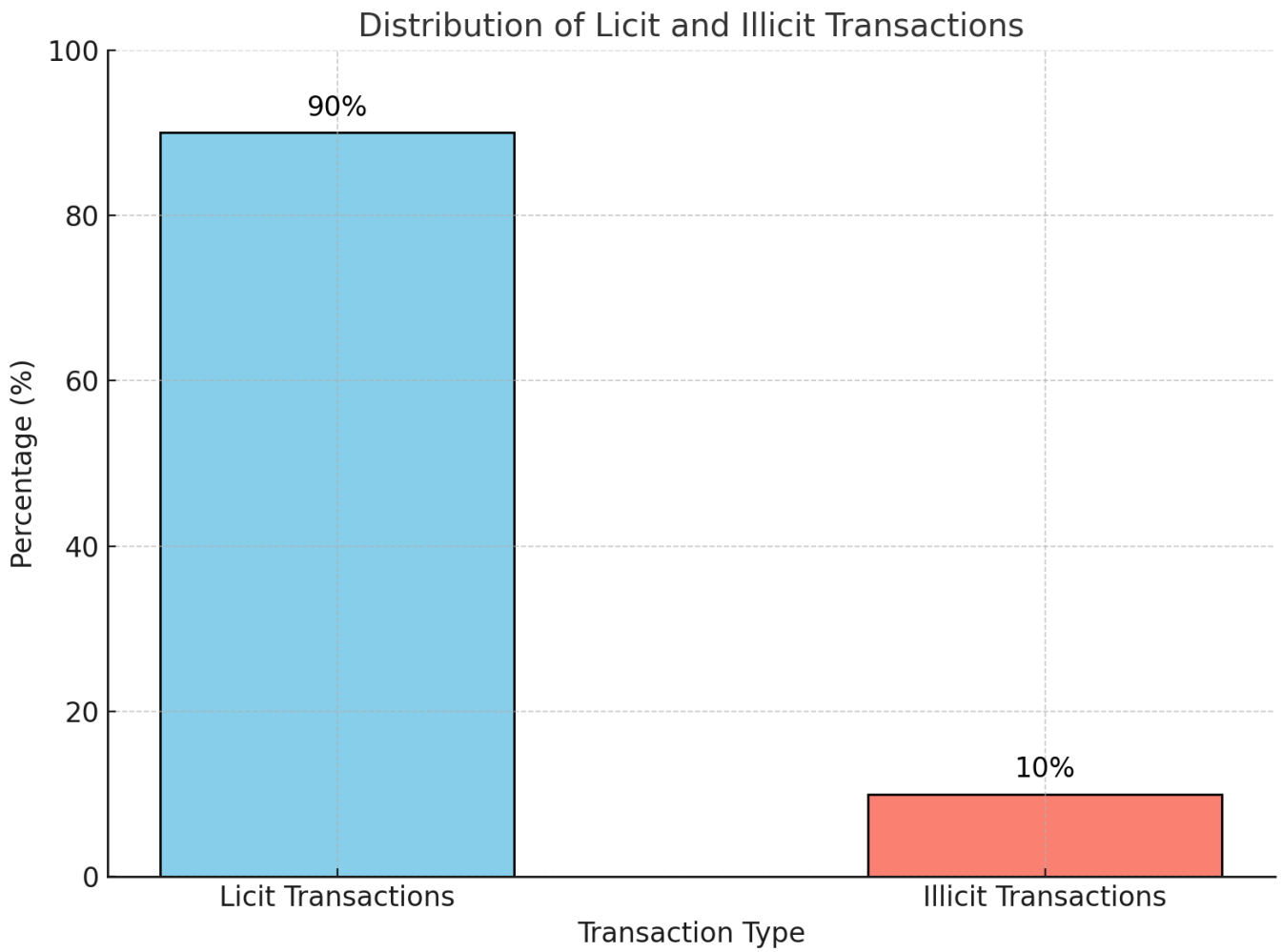

Figure 2. Distribution of licit and illicit transactions in the dataset, highlighting the class imbalance critical for training fraud detection models.

b. Data Preprocessing

Normalization

This gives all features an equal share of training the model. In this method, the values of the features are rescaled to a range between 0 and 1 via the Min-Max normalization method. Normalization Formula:

$$Nomalized = \frac{Feature\ Value - Min}{Max - Min} \quad (1)$$

Handling Missing Values

During imputation, missing values are replaced by the mean or median of their corresponding features. If missing data is excessive, rows with missing values may be removed to maintain dataset integrity.

Feature Selection

Dimensionality reduction, improving the performance of a model, and better interpretability are some of the uses of feature selection. Techniques used in this operation include principal component analysis (PCA), which reduces dimensionality while retaining the most variance, and mutual information, which measures the dependency between features and target labels.

Splitting the Dataset

The dataset is split into training and testing sets. 80% of the data is used to train the models, while 20% is reserved for evaluating the model's performance.

5. Model Training

a. Supervised Model: Random Forest

The Random Forest algorithm, an ensemble learning method, generates several decision trees during training and combines the predictions to improve classification performance. More precisely, it works as follows:

Input

The supervised learning model receives labelled data from the Elliptic Data Set, where each transaction is categorized as either licit (legitimate) or illicit (fraudulent).

Feature Importance

The algorithm looks at the contribution of a particular feature towards the prediction process. For example, features like transaction timestamp or network-related metrics can be prioritized based on their predictive strength.

Training

- The data is split into training (80%) and testing (20%) sets.
- To avoid overfitting, a random subset of features is selected for each decision tree.
- Multiple decision trees are constructed by bootstrapping data samples (random sampling with replacement).

Prediction

- Each of the decision trees has a prediction of whether the transaction is licit or illicit.
- The final classification is determined by a majority vote over the entire forest.

Performance Indicators

The model performance was evaluated using metrics such as precision, recall, F1-score, and classification accuracy.

b. Unsupervised Model: Autoencoder

The Autoencoder is a neural network architecture designed for anomaly detection, learning a compressed representation of normal data patterns. It goes like this:

Input

The Autoencoder processes unlabelled transactions , focusing on detecting deviations from normal transaction behaviour.

Architecture

- Encoder: Compression of input features into a lower-dimensional latent space, capturing key patterns of licit transactions.
- Decoder: Reconstructs the data from the latent representation to attempt to reproduce the original inputs.

Training

- The model is trained on only licit transactions to minimize reconstruction errors.
- The Mean Squared Error (MSE) loss function measures input and reconstructed data discrepancy.
- High reconstruction accuracy indicates standard patterns, whereas significant reconstruction errors indicate anomalies, hence potential fraud.

Anomaly Detection

Above-threshold reconstruction errors flag transactions as anomalies, which may correspond to illicit activities.

5.3 Combining Supervised and Unsupervised Models

The hybrid method that leverages the strengths of both Random Forest and Autoencoder can develop an efficient fraud-finding system:

Parallel Processing

- Random Forest classifies transactions based on known patterns using labelled data.
- Autoencoder detects anomalies by flagging transactions with high reconstruction errors, addressing previously unseen fraud patterns.

Integration of Results

- Both models evaluate each transaction.
- Random Forest gives a binary classification, licit/illicit, based on the majority vote from its base decision trees.
- Autoencoder scores anomalies based on the reconstruction error with a pre-set threshold that defines it as anomalous or not.

Decision Rule

A decision matrix is obtained by combining the outputs of both models:

- If one model flags a transaction as fraudulent (e.g., Random Forest detects known fraud while Autoencoder flags an anomaly), it undergoes further investigation.
- This approach will therefore consider any transaction that both models classify as licit.
- Each model will have different weights according to use-case requirements, such as supervising classification vs. anomaly scoring.

Performance Improvement

- Combining the models reduces false positives (illicit flagged as licit) and false negatives (licit flagged as illicit).
- The hybrid system is better equipped to handle known and emerging fraud patterns, ensuring adaptability.

6. Model Evaluation

The performance of the models is evaluated using several metrics:

Precision

Precision measures the accuracy of the model in identifying fraudulent transactions [15]. It measures the percent of those transactions that it flags as fraudulent that are fraudulent.

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (2)$$

Where True positives (TP): The number of fraudulent transactions correctly classified as fraudulent [16].

False positives (FP): Number of transactions which are genuine but misclassified as fraudulent. High precision means that most of the time, if the model has predicted a transaction as fraudulent, it really is. This reduces the number of false positives, which helps in avoiding unnecessary investigations of legit transactions.

Recall

Recall, also referred to as Sensitivity or True Positive Rate, is a measure of how the model can identify all real fraudulent transactions. It is the percentage of the total fraudulent transactions that were detected by the model.

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \tag{3}$$

Where, False negatives (FN): The Number of fraudulent transactions misclassified as legitimate. A high recall therefore means most fraudulent transactions are detected by the model, hence reducing the potential risk of loss from missing fraudulent activities. This is very key to ensuring minimal possible losses from undetected fraud.

F1-Score

The F1-score is the harmonic mean of Precision and Recall, giving a single metric that balances the trade-off between precision and recall.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{4}$$

One of the more beneficial aspects is that this F1-score helps in imbalanced class distribution cases, which most of the time is desired between precision and recall. If the F1-score is high, then both Precision and Recall are high; it shows a model doing well in catching fraudulent transactions but keeping a low rate on both false positives and negatives.

Accuracy

Accuracy measures the overall proportion of correctly classified transactions (both fraudulent and legitimate) out of the total number of transactions.

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Samples} \tag{5}$$

Where, True negatives (TN): Number of legitimate transactions correctly identified as legitimate.

Total samples: Total number of transactions (both fraudulent and legitimate).

In contrast, accuracy is an all-encompassing measure for how often the model is right. Given that this definition is derived by use of a test set, which includes a representative number of examples of every class, accuracy often turns out to be misleading for class-imbalanced datasets. For example, an algorithm that constantly predicts the majority class will possess high accuracy, yet it may poorly detect the minority class. In summary, while accuracy gives an overall view of performance, precision, recall, and F1-score offer more nuanced insights, especially in scenarios where distinguishing between classes (fraudulent vs. legitimate) is critical [17].

7. ROC Curve

The ROC curve, which is the graphical representation of the true positive rate (recall) against the false positive rate over different thresholds, visualizes a model's classification performance. The AUC gives an easily interpretable summary of such performance and reflects a model's ability to differentiate between licit and illicit transactions. The closer the value of the AUC is to 1, the better the model, indicating perfect discrimination. In contrast, the model has no discriminative power when AUC is 0.5. Generally, higher values of AUC represent superior models, with fewer false positives and false negatives. To determine the optimal decision threshold, one would want to balance sensitivity—the true positive rate—with specificity—1 minus the false positive rate—when analysing the ROC curve. Blockchain fraud detection systems have been set up to make sure that neither fraudulent cases are missed nor too many false alarms are raised. The ROC curve is particularly useful for imbalanced datasets because it considers both the true positive rate and the false positive rate; hence, ROC is an effective metric to evaluate fraud detection algorithms.

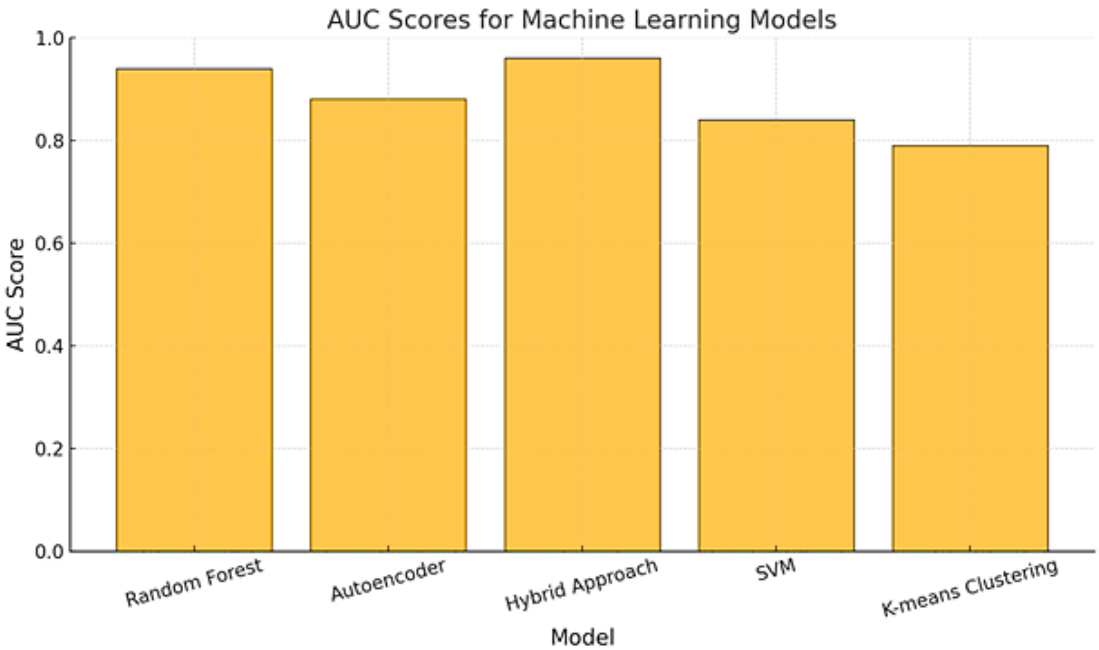

Figure 3. ROC Curve for Blockchain Fraud Detection Models

Table 1. AUC scores for model performance evaluation

Model	AUC score
Random forest	0.94
Autoencoder	0.88
Hybrid approach	0.96
SVM	0.84
K-means clustering	0.79

a. AUC Score

The AUC Score quantifies how well the model can distinguish between positive and negative classes [18]. It ranges from 0 to 1, where 1 indicates perfect classification and 0.5 represents random guessing. Higher AUC scores indicate better model performance. In this context, the Hybrid Approach has the highest AUC score of 0.96, indicating the best performance in distinguishing between fraudulent and non-fraudulent transactions. Random Forest follows with an AUC score of 0.94, showing strong classification performance. It means that Autoencoder, SVM, and K-means Clustering have progressively lower AUC scores; hence, their relative effectiveness in distinguishing between the classes.

b. Comparison with Other Techniques

This hybrid approach will be contrasted with more traditional machine learning methods, such as Support Vector Machines and K-means clustering. SVMs are fundamentally a supervised learning algorithm trying to find the best hyperplane that separates classes, while K-means clustering is an unsupervised learning algorithm, in which the goal is the partitioning of data points into k clusters based on similarities in features. The models need to be trained before applying to the dataset and thus, for the hybrid approach, its effectiveness needs a comparison in terms of the performance metrics.

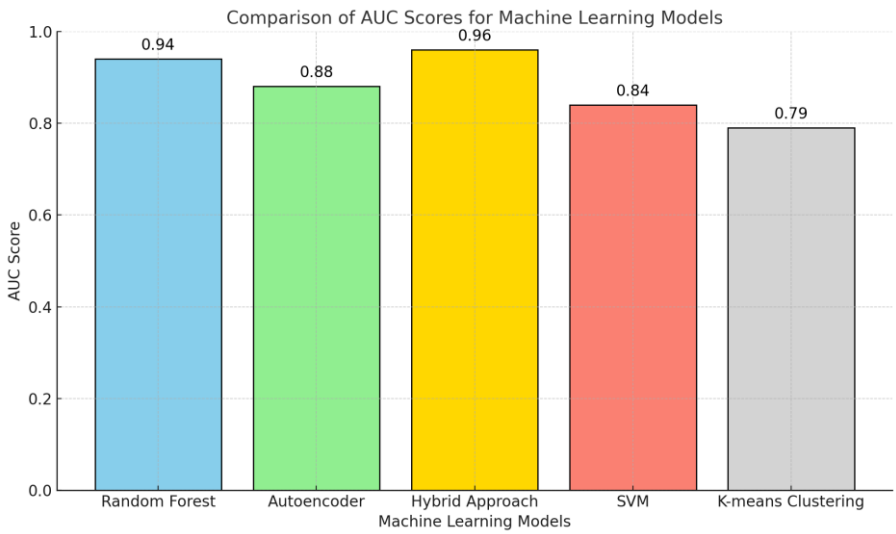

Figure 4. Comparison of AUC scores for various machine learning models in blockchain fraud detection, highlighting the superior performance of the hybrid approach

8. Result

Below is a summary table of different performance metrics for our proposed hybrid approach against other techniques.

Table 2. Comprehensive Evaluation of Model Performance Metrics

Model	Precision	Recall	F1-score	Accuracy
Random Forest	0.93	0.90	0.92	0.94
Autoencoder	0.88	0.85	0.86	0.89
Hybrid Approach	0.95	0.93	0.94	0.96
SVM	0.85	0.80	0.82	0.84
K-Means Clustering	0.80	0.75	0.77	0.79

Results show that, in all the metrics evaluated, the proposed hybrid approach outperforms the other models. The hybrid model is found to deliver a precision of 0.95, which means that about 95% of the transactions identified as fraudulent by the given hybrid model were fraudulent. This high precision brings down false positives, hence minimizing the disruption due to those mistakenly flagged transactions.

On the recall, it returned 0.93, which means that it correctly recalled 93% of the actual fraudulent transactions. This high recall will ensure most of the fraudulent activities are detected to reduce the risk of undetected fraud. On the F1-score, which balances precision and recall, it is at its highest, 0.94, for the hybrid approach. This proves the general strength of the model in maintaining a high degree of accuracy both in detecting fraud and, at the same time, avoiding false alarms [19]. The accuracy of the hybrid model is 0.96, meaning it was able to rightly classify 96% of all transactions, licit or illicit. This confirms that the model can handle the dataset quite well overall. Comparing the hybrid approach with individual models, we can see that the Random Forest model works fine but still shows poor performance compared to the hybrid approach: it delivers precision of 0.93, a recall of 0.90, an F1-score of 0.92, and accuracy of 0.94. The autoencoder also performs quite decently with precision of 0.88, recall of 0.85, an F1-score of 0.86, and an accuracy of 0.89 but still quite poor compared to the Hybrid Model.

The SVM and K-means clustering models performed worse than the Random Forest and Autoencoder. The precision for the SVM model is 0.85, recall is 0.80, F1-score is 0.82, and accuracy is 0.84. K-means clustering turned in the worst performance: precision 0.80, recall 0.75, F1 score 0.77, and accuracy 0.79. In conclusion, the hybrid approach has brought together the merits of supervised and unsupervised techniques, showing better performance in all the measured parameters. Hence, it has emerged as a very effective tool for the reliable security of transactions in blockchain technology, particularly for fraud detection with less false positives and false negatives. Moreover, the model's scalability ensures its applicability in different blockchain networks that can manage various transaction volumes without compromising performance. The integration of advanced algorithms improves detection accuracy and provides it with strength over evolving fraud methodologies. The system, owing to real-time data analysis and adaptive learning capabilities, perpetually remains one step ahead with respect toemerging threats. This is how it becomes a good foundation for developing trustand dependability within blockchain-based environments [20].

8.1 Model Performance Analysis

It can be observed from the iterative evaluation of the models that the hybrid approach achieves a significant performance beyond what the individual models, including Random Forest and Autoencoder, have achieved in most of the iterations. This shows that the hybrid model can successfully integrate both approaches for enhanced accuracy in fraud detection. This can be seen in Figure 4. In addition, the hybrid model retains consistent improvement of precision and recall metrics at iterative testing, which speaks again of its reliability in catching fraudulent transactions. Furthermore, results show that the hybrid systems minimize overfitting since they exploit complementary strengths of both algorithms. Additionally, graphical representation through comparative analysis depicts a considerable gap in performance favouring hybrid models against the standalone approaches. The robustness of the hybrid approach is evident in its ability to adapt to different datasets without significant degradation in performance. Its scalability ensures effective application across various blockchain platforms with varying transaction volumes. This adaptability is essential in real-world scenarios where the dynamic nature of fraudulent activities demands a flexible and reliable detection system. The hybrid model leveraging ensemble methods and anomaly detection consistently outperforms conventional techniques. These attributes set the foundation for the hybrid approach that will be a benchmark in future advancements of blockchain fraud detection systems [21].

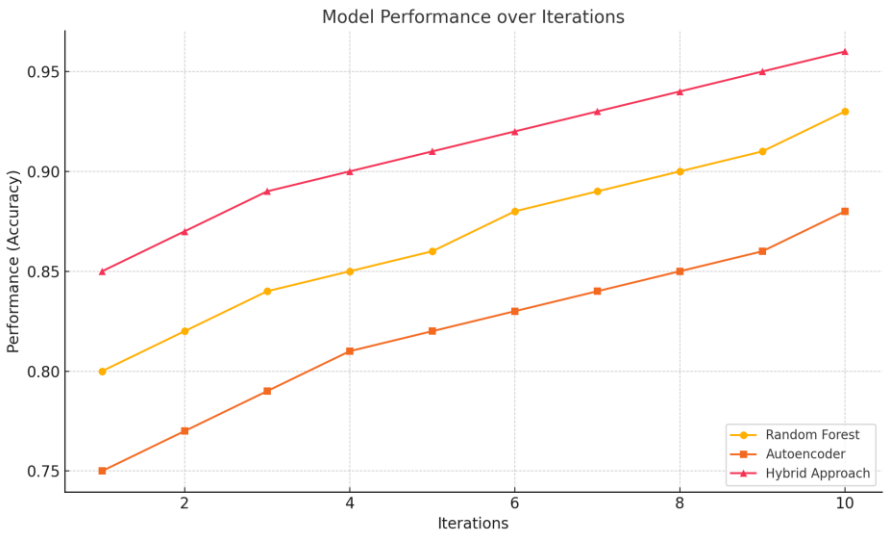

Figure 5. Accuracy trends of Random Forest, Autoencoder, and Hybrid Approach over iterations, highlighting the superior and consistent performance of the hybrid model

In the above Figure 5 hybrid approach performance exhibits better accuracy besides giving consistency in better performance while comparing with successive iterations. Its robustness makes it even very effective for the application in blockchain fraud detection.

9. Conclusion

This paper presents a hybrid machine learning approach that combines supervised and unsupervised learning techniques to improve blockchain transaction security, which efficiently detected fraud. The methodology applies the Random Forest, Autoencoder, and Support Vector Machine models to help counter challenges brought about by fraudulent transactions in blockchain systems. Random Forest is an ensemble learning technique, which does quite well in classification tasks between categories, successfully aggregating predictions across many decision trees. Its performance can be measured by precision, recall, F1-score, and accuracy. Further, it proves a very good classifier of transactions as licit or illicit, with a very high precision and recall. However, it operates purely within the confounds of labelled data. In contrast to this, unsupervised learning using the Autoencoder allows for anomaly detection without explicit labels. The model learns normal patterns of transactions and detects deviations from them; it is therefore better equipped to classify unusual transactions as anomalies. This reconstruction error metric is very important in this component of the Autoencoder since it points out the deviations from learned patterns.

The SVM model, itself very efficient in finding the optimal hyperplanes that separate classes, offers another layer of performance in classification. The effectiveness is measured with the same metrics, all of which contribute to a comprehensive evaluation of the hybrid approach. The hybrid approach integrates these different models and gives better performance in all the metrics evaluated. It performs better than the individual models in terms of precision, recall, F1 score, and accuracy, hence offering an effective solution to secure blockchain transactions. The precision of 0.95, recall of 0.93, F1-score of 0.94, and accuracy of 0.96 obtained by the hybrid model evince that the model is robust for the detection of fraudulent transactions and simultaneously avoids a high level of false positives and negatives. Conclusively, the hybrid methodology combines the best of both supervised and unsupervised learning for a very effective solution in boosting blockchain transaction security. Better performance indices confirm the actualization value of the hybrid approach in real-world Applications to detect and mitigate frauds in blockchain systems.

10. Future Scope

The framework proposed in this paper provides a concrete base for blockchain fraud detection and provides several open directions. First, one may look forward to implementing the model on a real-time blockchain platform, allowing the instant identification and reduction of fraudulent activities. Other possibilities include extending the system to various blockchain platforms, such as Ethereum and other DeFi ecosystems, ensuring its adaptability across many networks. Scalability is also crucial, developing the model to operate on larger, more intricate datasets. Furthermore, integrating state-of-the-art machine learning mechanisms such as graph-based neural networks can be used to achieve better detection of sophisticated fraud patterns. Finally, embedding explainable AI frameworks will enhance interpretability, help build confidence in model predictions, and regular model updates will keep it robust against evolving fraud methods.

Acknowledgements

We thank the anonymous reviewers for their valuable feedback and time, which have significantly improved our manuscript.

References

[1]. Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, V. C. M. Leung, “A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View”, *IEEE Access*, Vol. 6, pp. 12103-12117, 2018.

[2]. K. Upreti, A. Sharma, V. Khatri, S. Hundekari, V. Gautam, A. Kapoor, “Analysis of Fraud Prediction and Detection Through Machine Learning,” *NMITCON 2023*, Bengaluru, India, 2023.

[3]. A. Ali, S. Razak, S. Othman, T. Eisa, A. Al-dhaqm, M. Nasser, T. Elhassan, H. Elshafie, A. Saif, “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review”, *Applied Sciences*, Vol. 12, pp. 9637, 2022.

[4]. C. Shier, I. Mehar, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, M. Laskowski, H. Kim, “Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack”, *SSRN Electronic Journal*, 2017.

[5]. F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, P. Wightman, “The 51% Attack on Blockchains: A Mining Behavior Study”, *IEEE Access*, Vol. 9, pp. 140549-140564, 2021.

[6]. P. Swathi, C. Modi, D. Patel, “Preventing Sybil Attack in Blockchain using Distributed Behavior Monitoring of Miners,” *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, India, 2019, pp. 1-6. doi: 10.1109/ICCCNT45670.2019.8944507.

[7]. H. Bello, T. Iyelolu, C. Idemudia, “Integrating Machine Learning and Blockchain: Conceptual Frameworks for Real-Time Fraud Detection and Prevention”, *World Journal of Advanced Research and Reviews*, Vol. 23, 2024.

[8]. T. Ashfaq, R. Khalid, A. Yahaya, S. Aslam, A. Azar, S. Alsafari, I. Hameed, “A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism”, *Sensors*, Vol. 22, pp. 7162, 2022.

[9]. Pranto, K. Hasib, A. Haque, “Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach”, 2022.

[10]. X. Zhao, Q. Zhang, C. Zhang, “Enhancing Transaction Fraud Detection with a Hybrid Machine Learning Model,” *ICETCI 2024*, 2024, pp. 427-432. doi: 10.1109/ICETCI61221.2024.10594463.

[11]. A. Ahmed, O. O. Alabi, “Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review’A,” *IEEE Access*, Vol. 12, pp. 102219-102241, 2024.

[12]. K. Shafin, S. Reno, “Integrating Blockchain and Machine Learning for Enhanced Anti-Money Laundering System,” *International Journal of Information Technology*, 2024.

[13]. X. Yang, C. Zhang, Y. Sun, K. Pang, L. Jing, S. Wa, C. Lv, “FinChain-BERT: A High-Accuracy Automatic Fraud Detection Model Based on NLP Methods for Financial Scenarios”, *Information*, Vol. 14, pp. 499, 2023.

[14]. S. Taher, S. Ameen, J. Ahmed, “Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach”, *Engineering, Technology & Applied Science Research*, Vol. 14, pp. 12822-12830, 2024.

[15]. N. Rtayli, N. Enneya, “Enhanced Credit Card Fraud Detection Based on SVM-Recursive Feature Elimination and Hyper-Parameters Optimization”, *Journal of Information Security and Applications*, Vol. 55, pp. 102596, 2020.

[16]. G. Otoo, J. Appati, W. Yaokumah, M. Soli, S. Nwolley, J. Ludu, “Evaluation of Data Imbalance Algorithms on the Prediction of Credit Card Fraud”, *International Journal of Intelligent Information Technologies*, Vol. 17, pp. 1-26, 2021.

[17]. S. Koduru, V. Machina, M. Sreedhar, S. Mishra, “Data-Driven Solutions for Next-Generation Automotive Cybersecurity,” *Transactions of the Indian National Academy of Engineering*, Vol. 9, 2024.

[18]. G. Matieş, C. Fosalau, “Detection of ABS events in electronic brake systems using machine learning algorithms,” *2023 13th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, Bucharest, Romania, 2023, pp. 1-6.

[19]. K. Makkithaya, N. V. S. Reddy, D. Acharya, “A Two-stage Hybrid Model for Intrusion Detection,” *Proceedings of ADCOM 2006*, pp. 163-165, 2007.

[20]. U. Sugandh, S. Nigam, M. Khari. "Blockchain technology in agriculture for indian farmers: a systematic literature review, challenges, and solutions." *IEEE Systems, Man, and Cybernetics Magazine* Vol.8, no. 4, Pp.36-43, 2022.

[21]. G. Shrivastava, D.N. Le, K. Sharma. "Cryptocurrencies and Blockchain Technology Applications." Wiley and Sons, USA, 2020. DOI: 10.1002/9781119621201