Journal of Information Systems and Informatics
Vol. 7, No. 1, March 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i1.1047 Published By DRPM-UBD

Advanced Techniques for Anomaly Detection in Blockchain: Leveraging Clustering and Machine Learning

Ferdiansyah[1], Usman Ependi[2,*], Tasmi[3], Muhammad Haikal[4], Mikko[5]

[1,3,4,5] Faculty of Computer and Science, Universitas Indo Global Mandiri, Palembang, Indonesia
[2]Informatics Department, Bina Darma University, Palembang, Indonesia
Email: [1]ferdi@uigm.ac.id, [2,*]u.ependi@binadarma.ac.id, [3]tasmi@uigm.ac.id,
[4]2022310006@student.uigm.ac.id, [5]202231070@student.uigm.ac.id

Abstract

Blockchain technology has revolutionized data security and transaction transparency across various industries. However, the increasing complexity of blockchain networks has led to anomalies that require further investigation. This study aims to analyze anomalies in blockchain systems using machine learning approaches. Various anomaly detection techniques, including supervised and unsupervised methods, are evaluated for their effectiveness in identifying irregularities. The results indicate that machine learning models can detect anomalies with high accuracy, providing insights into potential threats and system vulnerabilities. The findings of this research contribute to improving blockchain security and developing more robust monitoring systems.

Keywords: Blockchain Security, Anomaly Detection, Machine Learning, Fraud Detection.

1. INTRODUCTION

Blockchain has emerged as one of the most revolutionary technologies in the past decade, with wide-ranging applications from cryptocurrency to supply chain management[1]. The technology has revolutionized data security and transaction transparency across various industries [2], [3]. However, the increasing complexity of blockchain networks has led to anomalies that require further investigation. Traditional anomaly detection techniques often fall short in identifying hidden anomaly patterns within large and diverse datasets due to the distributed and encrypted nature of blockchain data. This inadequacy poses significant risks, including potential fraud, security breaches, and system vulnerabilities[4].

The security and integrity of data stored within blockchain networks are crucial to ensuring the trust and reliability of these systems [5]. However, with the increasing adoption of this technology, the threats to blockchain network security have also escalated, including suspicious transactions and other anomalous activities [6]. Anomaly detection in blockchain networks is a complex and challenging process due to the distributed and encrypted nature of the data[7]. Traditional techniques

often fall short in identifying hidden anomaly patterns within large and diverse datasets. Therefore, more sophisticated approaches are required to effectively detect anomalies.

A recent study successfully detected anomalies within blockchain transactions using machine learning classifiers and explainability analysis. The integration of eXplainable Artificial Intelligence (XAI) techniques with tree-based ensemble classifiers, such as the Shapley Additive exPlanation (SHAP) method, enhanced the detection of anomalous Bitcoin transactions[8]. This approach improved the True Positive Rate (TPR) and ROC-AUC scores, demonstrating the effectiveness of advanced machine learning techniques in anomaly detection [9]. there have been instances where anomaly detection in blockchain has failed. For example, traditional methods struggled to detect anomalies in complex blockchain networks due to the infrequent occurrence of illicit transactions and the lack of explanations for model predictions. This limitation underscores the need for more sophisticated and interpretable models to accurately identify and explain anomalies.

Despite the advancements in blockchain technology, there is a notable gap in effective anomaly detection methods tailored for blockchain networks[1]. Existing techniques struggle with the unique challenges posed by blockchain's decentralized and encrypted structure. The need for more sophisticated approaches that can accurately detect and analyze anomalies in blockchain transactions is evident. This gap highlights the necessity for innovative solutions that leverage advanced machine learning and clustering algorithms to enhance anomaly detection capabilities.

This study aims to analyze anomalies in blockchain systems using machine learning approaches by evaluating various anomaly detection techniques, including both supervised and unsupervised methods, to determine their effectiveness in identifying irregularities within blockchain networks. By employing clustering algorithms such as K-Means and anomaly detection algorithms like Random Forest, the research seeks to enhance the accuracy and efficiency of detecting suspicious transactions. Ultimately, the goal is to develop a robust monitoring system capable of providing insights into potential threats and system vulnerabilities, thereby contributing to improved blockchain security.

In this study, we propose the use of clustering algorithms and machine learning-based anomaly detection to enhance the capability of detecting anomalies in blockchain networks [10]. Clustering algorithms, such as K-Means, are employed to group transactions based on feature similarities, while anomaly detection algorithms, such as Random Forest, are utilized to identify suspicious transactions [11].

This approach not only enables the identification of anomalies with higher accuracy but also aids in understanding the patterns and characteristics of normal and anomalous transactions. Consequently, this research aims to make a significant contribution to the field of blockchain security by offering a more effective and efficient solution for anomaly detection.

2. METHODS

2.1. Research Framework

The flowchart Figure 1 illustrates a machine learning pipeline for anomaly detection in transactions.

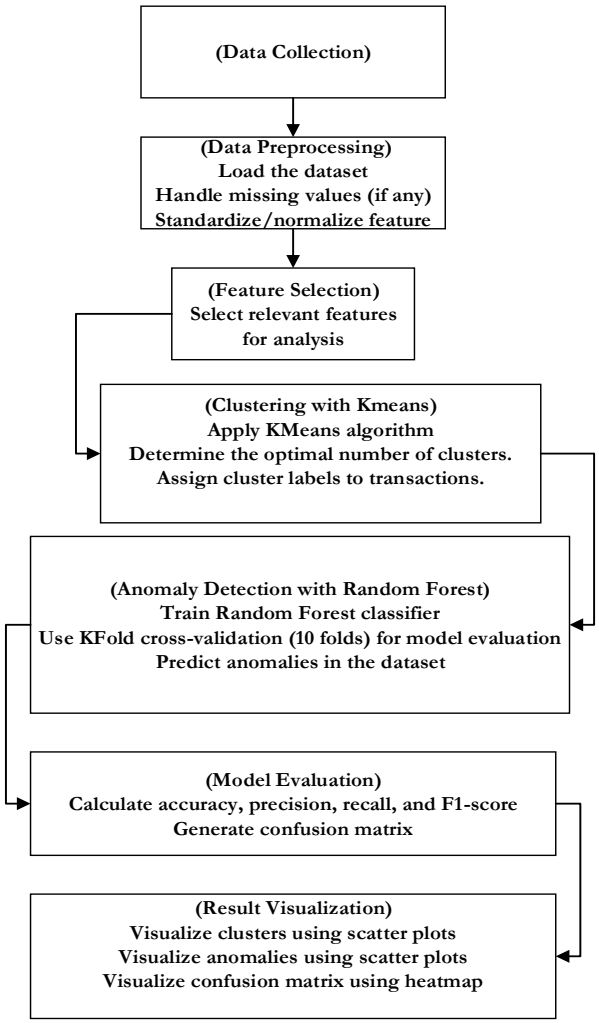

Figure 1. Research Framework

It begins with data collection, followed by preprocessing, where missing values are handled, and features are standardized. Feature selection involves identifying and using the most relevant features from blockchain transaction data to improve anomaly detection. Machine learning algorithms like Random Forest and K-Means Clustering are suitable for this task due to their ability to handle high-dimensional data, robustness to noise and outliers, and scalability. These algorithms can effectively group similar transactions, identify outliers, and classify transactions as normal or anomalous, making them ideal for enhancing blockchain security and detecting fraudulent activities. Clustering with K-Means determines the optimal number of clusters and assigns labels to transactions. Next, Random Forest is trained for anomaly detection, using 10-fold cross-validation for evaluation. The model is assessed based on accuracy, precision, recall, and F1-score, with results visualized through scatter plots for clusters and anomalies, alongside a confusion matrix heatmap for performance evaluation.

2.2. Machine Learning in Anomaly Detection

Machine learning has become a pivotal tool in the field of anomaly detection , offering a range of techniques to analyze large volumes of complex data and identify anomalous patterns that are difficult to detect using traditional methods[12], [13]. Anomaly detection is crucial in various domains, including cybersecurity, fraud detection, and healthcare, where identifying unusual patterns can prevent significant losses and enhance system security[14], [15], [16]. Machine learning techniques, both supervised and unsupervised, have been extensively researched and applied to improve the accuracy and efficiency of anomaly detection systems[12].

2.3. KMeans Clustering for Anomaly Detection

KMeans clustering is one of the most widely used unsupervised learning algorithms for anomaly detection. It partitions data into K clusters based on feature similarities, making it easier to identify outliers that do not fit well into any cluster. The algorithm works by minimizing the variance within each cluster, which helps in grouping similar data points together while isolating those that are significantly different [17][14].

Several studies have demonstrated the effectiveness of KMeans in anomaly detection. For instance, Mani Mehrotra and Nakul Joshi proposed an algorithm using KMeans clustering combined with the C5.0 decision tree to improve clustering accuracy and classify anomalous instances [18][17]. Another study by Krishna Prajapati and Hitesh Patel introduced a two-tier KMeans clustering algorithm to enhance anomaly detection in various datasets. These advancements

highlight the robustness of KMeans in handling large datasets and its adaptability to various anomaly detection scenarios [19].

2.3.1. Random Forest for Classification

Random Forest is a powerful ensemble learning method used for classification and regression tasks. It constructs multiple decision trees during training and outputs the mode of the classes for classification[20][21]. The algorithm's ability to handle large datasets with higher dimensionality and its robustness to overfitting make it an ideal choice for anomaly detection. Leo Breiman's seminal work on Random Forests laid the foundation for its widespread adoption in machine learning[21]. The algorithm's generalization error converges as the number of trees in the forest increases, making it highly reliable for classification tasks[22]. Additionally, Random Forests provide internal estimates of error, strength, and correlation, which are used to measure variable importance and improve model performance. In the context of anomaly detection, Random Forests have been used to classify transactions as normal or anomalous based on various features. The algorithm's ability to handle imbalanced datasets and its interpretability through feature importance scores make it a valuable tool for detecting anomalies in complex datasets[23].

2.3.2. Combining KMeans and Random Forest for Enhanced Anomaly Detection

Combining KMeans clustering with Random Forest classification offers a robust approach to anomaly detection. KMeans can be used to group similar transactions and identify potential outliers, which are then classified using Random Forest to determine their likelihood of being anomalous. This hybrid approach leverages the strengths of both algorithms, providing a comprehensive solution for detecting and classifying anomalies in large datasets[24]. Studies have shown that this combination improves the accuracy and efficiency of anomaly detection systems. By clustering data points first, the model can focus on the most relevant features for classification, reducing noise and improving overall performance. This approach has been successfully applied in various domains, including financial fraud detection and network security[24].

2.4. Dataset

The dataset used in this study is sourced from GitHub [25], The transaction dataset used in this study consists of 1000 rows of transaction data. Each row represents a unique transaction with various features relevant for clustering and anomaly detection analysis. The details of features in the Dataset as follow.

1) Transaction_ID: A unique identifier for each transaction.

2) Transaction_Amount: The amount of money transacted.
3) Transaction_Volume: The volume of transactions conducted.
4) Average_Transaction_Amount: The average amount of transactions.
5) Frequency_of_Transactions: The frequency of transactions conducted by the user.
6) Time_Since_Last_Transaction: The time since the last transaction was conducted.
7) Day_of_Week: The day of the week when the transaction was conducted.
8) Time_of_Day: The time of day when the transaction was conducted.
9) Age: The age of the user conducting the transaction.
10) Gender: The gender of the user (Male/Female).
11) Income: The income of the user.
12) Account_Type: The type of account (Savings/Current).

2.5. Challenges Faced

There several of challenges faced in this research as follow.

1) Anomaly Detection: One of the main challenges is detecting suspicious or unusual transactions. Anomalies in financial transactions can indicate fraudulent activities or system errors.
2) Clustering Transactions: Grouping transactions based on feature similarities to understand normal transaction patterns and identify potentially suspicious transaction clusters.
3) Large Volume of Data: The dataset contains a large number of transactions, making manual analysis impractical. Therefore, machine learning techniques are required to efficiently analyze the data.
4) Feature Variability: The features in the dataset exhibit high variability, such as transaction amounts, transaction frequencies, and transaction times. This adds complexity to detecting anomaly patterns.

2.6. Research Objectives

This study aims to enhance the capability of detecting anomalies in blockchain networks using clustering and machine learning-based anomaly detection algorithms. This approach is expected to identify suspicious transactions with higher accuracy and understand the patterns of normal and anomalous transactions. The approach uses by using Clustering with KMeans, the KMeans algorithm is used to cluster transactions based on feature similarities. This helps in identifying groups of similar transactions and isolating significantly different transactions. Anomaly Detection with Random Forest, the Random Forest algorithm is used to classify transactions as normal or anomalous. Random Forest is chosen for its ability to handle large and complex datasets and provide interpretative results through feature importance scores.

3. RESULTS AND DISCUSSION

3.1. Experimental Results

The clustering results reveal three main transaction patterns, with most transactions concentrated around Transaction Amount ≈ 1000, while high-value transactions (>2500) form a distinct cluster. KMean effectively differentiates regular transactions (Clusters 0 & 1) from high-value transactions (Cluster 2), which may indicate either premium customers or potential anomalies. Further analysis is required to assess the alignment of these clusters with Isolation Fores anomaly detection and to incorporate additional factors such as transaction frequency and user demographics for a more comprehensive evaluation.

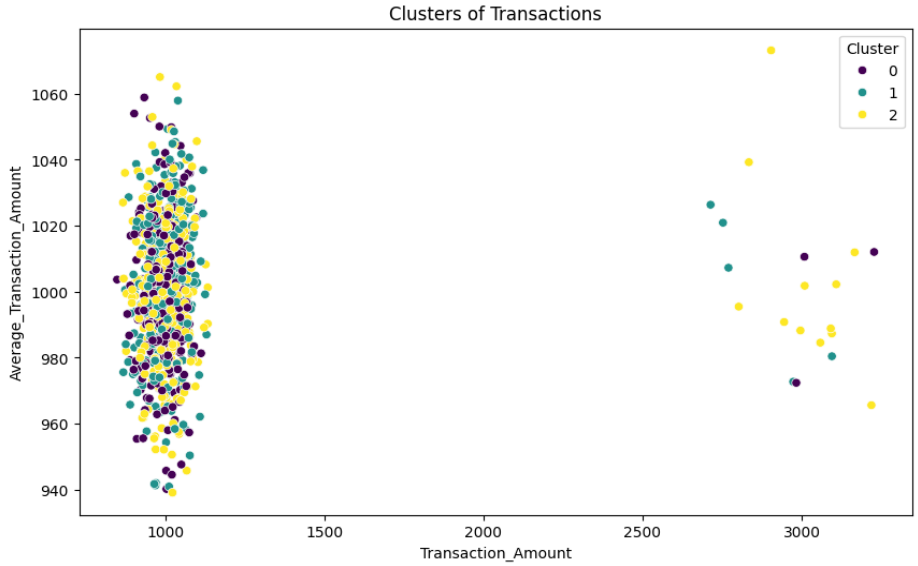

Figure 2. Clustering Visualization

The scatter plot presents a visualization of transaction clustering based on Transaction Amount and Average Transaction Amount, as shown in Figure 2, revealing three distinct groups. The majority of transactions are concentrated around 1000, while a smaller subset with significantly higher values (~2500-3200) suggests the presence of high-value transactions or potential anomalies. The color-coded clusters represent different transactional behaviors, which may correspond to distinct user segments such as regular users, premium users, or anomalous transactions. Identifying these clusters is crucial for applications such as fraud detection, customer segmentation, and transaction pattern analysis. The presence of outliers may indicate suspicious financial activities, including money laundering, fraudulent transactions, or unauthorized access, warranting further investigation.

This clustering approach enables financial institutions to enhance risk management strategies, improve fraud prevention mechanisms, and develop adaptive financial models based on user behavior patterns. Furthermore, the ability to detect and classify anomalous transactions can contribute to enhancing the security and trustworthiness of financial and blockchain-based systems. The dataset contains 50 detected anomalies based on the Isolation Forest algorithm. These anomalies represent transactions that significantly deviate from the normal pattern, potentially indicating fraudulent activities, unusual spending behavior, or errors in transaction records, as shown in Figure 3.

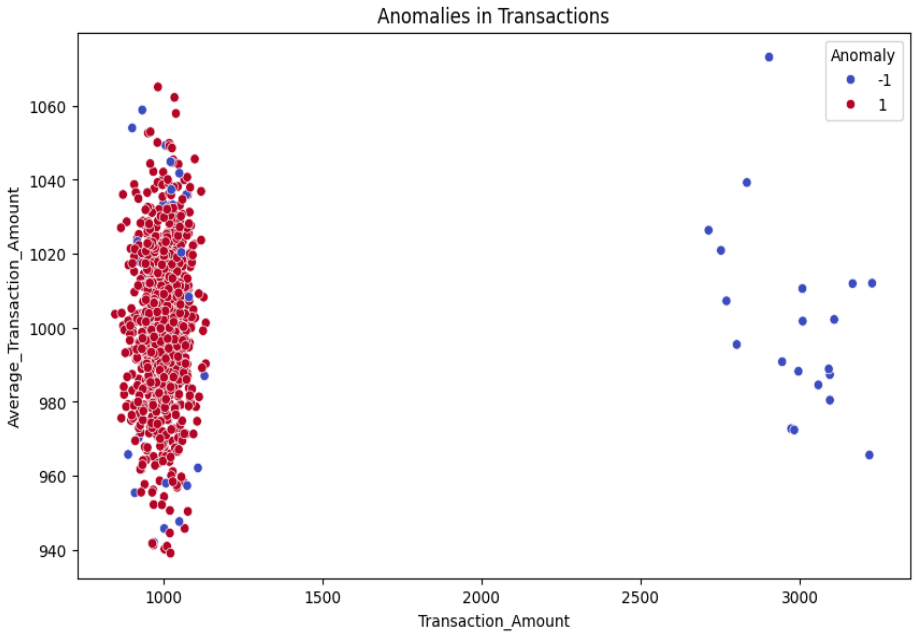

Figure 3. Anomalies in Transactions

The anomaly detection results using Isolation Forest indicate that most transactions (red points, labeled as "1") are classified as normal, while a small subset (blue points, labeled as "-1") are detected as anomalies. The anomalies are primarily concentrated in two areas:

1) High-value transactions (>2500): These transactions deviate significantly from the majority and could indicate fraudulent activity, VIP customers, or unusual spending behavior.
2) Scattered anomalies within the normal range (~1000 transaction amount): These may result from subtle irregularities in transaction patterns, such as sudden changes in frequency or user spending behavior.

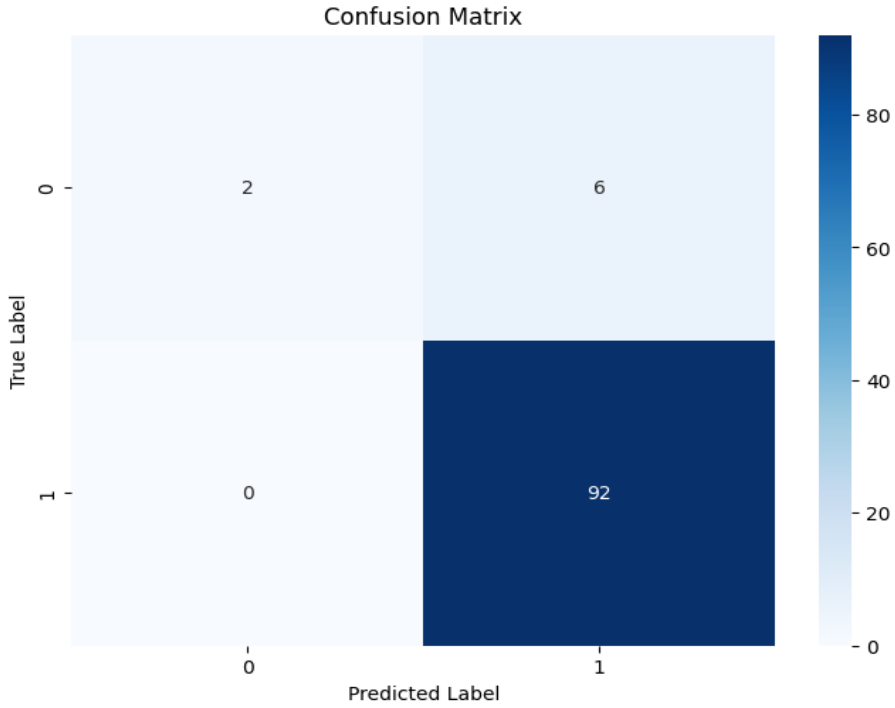

Figure 4. Anomalies in Transactions

The confusion matrix evaluates the performance of a classification model, as shown in Figure 4. It shows 92 true positives (correctly classified class 1 instances) and 2 true negatives (correctly classified class 0 instances). However, there are 6 false positives (class 0 misclassified as class 1) and 0 false negatives (class 1 misclassified as class 0). This suggests the model has high recall (no false negatives) but may have some false positives, potentially favoring class 1 predictions. The model performs well in detecting class 1 but may need improvements in distinguishing class 0 accurately.

Table 1. Classification Report

Classification Report:				
	precision	recall	f1-score	support
-1	1.00	0.25	0.40	8
1	0.94	1.00	0.97	92
accuracy			0.94	100
macro avg	0.97	0.62	0.68	100
Weighted avg	0.94	0.94	0.92	100

The classification report as shown in Table 1 provides a detailed evaluation of the model's performance.

1) Class -1 (Anomalies): The precision is 1.00, meaning all predicted anomalies were actually anomalies. However, recall is only 0.25, indicating that the model only detected 25% of actual anomalies, missing many true cases. The F1-score (0.40) suggests poor overall performance in identifying anomalies due to low recall.
2) Class 1 (Normal transactions): The model has 0.94 precision and 1.00 recall, meaning nearly all normal transactions were correctly identified. The F1-score (0.97) indicates excellent classification for this class.
3) Overall Performance: The accuracy is 94%, but the macro average recall (0.62) highlights imbalanced performance, as anomalies are often missed. The weighted average F1-score (0.92) suggests the model is optimized for detecting normal transactions rather than anomalies.

3.2. Discussion

The experimental results of the clustering and anomaly detection processes provide valuable insights into transaction behavior and potential risks within the dataset. The application of the KMeans clustering algorithm successfully revealed three distinct transaction patterns, with the majority of transactions clustering around a transaction amount of approximately 1000. This indicates a concentration of regular or average transactions, possibly representing typical user behavior. Notably, a separate and clearly defined cluster, encompassing high-value transactions exceeding 2500, stands out. This cluster could represent a segment of premium users or, more concerningly, a group of potential anomalies requiring further examination.

The visualization in Figure 2 enhances the interpretability of the clustering output, where color-coded clusters illustrate variations in user behavior. The presence of a high-value cluster highlights the model's sensitivity to differentiating typical from exceptional behavior, which is essential for customer segmentation, premium service targeting, or anomaly detection. However, the interpretation of this cluster is twofold—it may indicate a valuable user segment or raise red flags related to suspicious activities, such as fraudulent transactions or attempts at money laundering. Therefore, clustering alone is insufficient for definitive conclusions; a cross-analysis with anomaly detection models like Isolation Forest is necessary.

When integrated with the Isolation Forest anomaly detection results, the picture becomes more complex. As shown in Figure 3, the Isolation Forest algorithm identified 50 anomalous transactions within the dataset. These anomalies fall into two key categories: high-value outliers and irregular transactions within the normal transaction range (~1000). The former aligns with KMeans Cluster 2, reinforcing

the hypothesis that high-value transactions may not follow regular patterns. The latter, however, is more nuanced—such scattered anomalies might reflect abrupt behavioral shifts in otherwise typical users, possibly due to contextual or external factors such as promotions, seasonal spending, or technical errors. This layered detection is instrumental for financial institutions that aim to flag not only overtly suspicious activities but also subtle and evolving risks.

The classification performance, as evaluated by the confusion matrix and detailed in Table 1, reveals both the strengths and limitations of the current model. The confusion matrix shows that while the model achieves excellent recall (1.00) for normal transactions (class 1), indicating that it successfully identifies almost all regular behavior, its ability to detect anomalies (class -1) is significantly limited. Although precision for anomalies is perfect (1.00), meaning all predicted anomalies were correct, the recall is only 0.25. This implies that 75% of actual anomalies remain undetected, which is a serious concern in high-stakes applications like fraud detection where missing even a single fraudulent transaction can have costly implications.

The F1-score for class -1, standing at 0.40, reinforces the model's weakness in capturing a substantial portion of actual anomalies, highlighting the need for improvement in recall. In contrast, the model performs admirably on class 1, with high precision, recall, and F1-score values, demonstrating a bias toward identifying normal behavior. While the overall accuracy is 94%, and the weighted F1-score is 0.92, these metrics mask the imbalance in class performance. The macro average recall (0.62) reflects this skewed performance, emphasizing the need for rebalancing through techniques such as anomaly-focused training data augmentation or cost-sensitive learning.

In practical terms, this imbalance is critical. Financial institutions and security systems must prioritize reducing false negatives in anomaly detection, even at the expense of a few false positives. In real-world applications, a model that detects every anomaly—even with some over-flagging—is more valuable than one that fails to identify significant threats. Therefore, the next iteration of model refinement should explore ensemble methods, advanced anomaly-aware algorithms, or hybrid approaches that combine unsupervised clustering with supervised anomaly labeling. Ultimately, the combined insights from clustering, anomaly detection, and classification performance highlight the model's potential in understanding transaction behavior, segmenting user types, and detecting risks. However, improvements are necessary to enhance anomaly recall and balance performance across all transaction classes. Addressing these challenges will significantly bolster fraud detection capabilities, reinforce financial security protocols, and enable more intelligent data-driven decision-making in transaction analysis systems.

4. CONCLUSION

This study successfully applied machine learning techniques to detect anomalies in blockchain transactions, leveraging K-Means clustering and Random Forest classification. The approach combining K-Means clustering and Random Forest classification effectively identified high-value transactions and frequent transactions, showcasing the models' ability to handle large datasets and detect outliers. Behavioral anomalies, such as unusual spending patterns and irregular transaction times, were also successfully flagged. However, the models faced limitations in detecting low-frequency but high-impact anomalies due to their rarity and subtlety. The anomaly detection model identified 50 anomalous transactions, as visualized in the scatter plots. The classification results achieved an overall accuracy of 94%, with a precision of 1.00 for anomalies and 0.94 for normal transactions. The recall values indicate that the model detected 100% of normal transactions correctly but only 25% of anomalies, suggesting a need for further optimization in identifying rare fraudulent patterns. The confusion matrix highlights that 92 normal transactions were correctly classified, while 6 normal transactions were misclassified as anomalies, and 2 anomalies were correctly identified. These findings demonstrate that while the model is highly accurate in detecting normal transactions, improvements are necessary for better anomaly detection. Future work should focus on refining feature selection, incorporating deep learning approaches, and implementing real-time detection to enhance blockchain security and fraud prevention.

REFERENCES

[1] Z. Liu, H. Gao, H. Lei, Z. Liu, and C. Liu, "Blockchain anomaly transaction detection: An overview, challenges, and open issues," in *Int. Conf. Inf. Sci., Commun. Comput.*, 2023, pp. 126–140.

[2] E. P.-E. George, C. Idemudia, and A. B. Ige, "Blockchain technology in financial services: Enhancing security, transparency, and efficiency in transactions and services," *Open Access Res. J. Multidiscip. Stud.*, 2024, doi: 10.53022/oarjms.2024.8.1.0042

[3] A. Judmayer, N. Stifter, K. Krombholz, and E. Weippl, *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms. Synth. Lect. Inf. Secur. Priv. Trust*, 2017, doi: 10.2200/s00773ed1v01y201704spt020.

[4] K. Croman *et al.*, "On scaling decentralized blockchains: (A position paper)," in *Int. Conf. Financial Cryptography Data Secur.*, 2016, pp. 106–125.

[5] Y. Ikeda, R. Hadfi, T. Ito, and A. Fujihara, "Anomaly detection and facilitation AI to empower decentralized autonomous organizations for secure crypto-asset transactions," *AI Soc.*, pp. 1–12, 2025.

[6] Ł. Apiecionek and P. Karbowski, "Fuzzy neural network for detecting anomalies in blockchain transactions," *Electronics*, vol. 13, no. 23, p. 4646, 2024.
[7] G. S. Rai, S. B. Goyal, and P. Chatterjee, "Anomaly detection in blockchain using machine learning," in *Comput. Intell. Eng. Manag. Appl.: Sel. Proc. CIEMA 2022*, Springer, 2023, pp. 487–499.
[8] J. Bonneau *et al.*, "SOK: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Proc. 2015 IEEE Symp. Secur. Privacy*, 2015, pp. 104–121.
[9] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," *Blockchain Res. Appl.*, vol. 5, no. 3, p. 100207, 2024.
[10] S. Siddamsetti, C. Tejaswi, and P. Maddula, "Anomaly detection in blockchain using machine learning," *J. Electr. Syst.*, vol. 20, pp. 619–634, 2024.
[11] M. T. R. Laskar *et al.*, "Extending isolation forest for anomaly detection in big data via K-means," *ACM Trans. Cyber-Phys. Syst.*, vol. 5, no. 4, pp. 1–26, 2021.
[12] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021.
[13] X. Ugarte-Pedrero *et al.*, "On the adoption of anomaly detection for packed executable filtering," *Comput. Secur.*, vol. 43, pp. 126–144, 2014, doi: 10.1016/j.cose.2014.03.012.
[14] J. Akoto and T. Salman, "Machine learning vs deep learning for anomaly detection and categorization in multi-cloud environments," in *Proc. 2022 IEEE Cloud Summit*, 2022, pp. 44–50.
[15] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.
[16] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annu. Int. Cryptol. Conf.*, 2017, pp. 357–388.
[17] Q. Kong, H. Gong, X. Ding, and R. Hou, "Classification application based on mutual information and random forest method for high dimensional data," in *2017 9th Int. Conf. Intell. Human-Machine Syst. Cybern. (IHMSC)*, 2017, pp. 171–174.
[18] M. Mehrotra and N. Joshi, "Anomaly detection in temporal data using KMeans clustering with C5.0," *Int. J. Eng. Sci.*, vol. 6, no. 5, pp. 77–81, 2017.
[19] A. Sreenivasulu, "Evaluation of cluster based anomaly detection," 2019.
[20] D. R. Cutler *et al.*, "Random forests for classification in ecology," *Ecology*, vol. 88, no. 11, pp. 2783–2792, 2007.

[21] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001, doi: 10.1023/A:1010933404324.
[22] H. S. Galal, Y. B. Mahdy, and M. A. Atiea, "Behavior-based features model for malware detection," *J. Comput. Virol. Hacking Tech.*, vol. 12, no. 2, pp. 59–67, 2016, doi: 10.1007/s11416-015-0244-0.
[23] M. Staron, H. O. Hergés, L. Block, and M. Sjödin, "Comparing anomaly detection and classification algorithms: A case study in two domains," in *Int. Conf. Softw. Qual.*, 2023, pp. 121–136.
[24] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "Combining k-means and XGBoost models for anomaly detection using log datasets," *Electronics*, vol. 9, no. 7, p. 1164, 2020.
[25] B. Apurva, "Anomaly detection in transactions." Accessed: Feb. 17, 2025. [Online]. Available: https://github.com/NebeyouMusie/Anomaly-Detection-in-Transactions