International Journal of Advanced Computing and Mechanical Systems (IJACM)
E-ISSN No.: xxxx-xxxx www.ijacm.com
Volume Number: 2 Issue Number: 1 pp: 52 - 59 Publication Month: Jan-2026

Preserving Security of Crypto Transactions with Machine Learning Methodologies

S Shilpa[1], G Hemalatha[2], P Jyothi[2], V Aadhinarayana Reddy[2], T Hemasai[2], Nagaiah Karthik[2]
[1]Assistant Professor, Siddartha Institute of Science and Technology, Puttur, Andhra Pradesh, India
[2]UG Students, Siddartha Institute of Science and Technology, Puttur, Andhra Pradesh, India

Autor1 E-Mail: shilpamani0614@gmail.com
Autor2 E-Mail: hemalathagajjala48@gmail.com
Autor3 E-Mail: jyothijyo02478@gmail.com
Autor4 E-Mail: adhinarayanareddy119@gmail.com
Autor5 E-Mail: saihema496@gmail.com
Autor6 E-Mail: kk7839394@gmail.com

ABSTRACT

The rapid adoption of cryptocurrencies has transformed global financial systems by enabling decentralized and peer-to-peer transactions. Despite strong cryptographic foundations, blockchain-based transactions remain vulnerable to fraud, money laundering, phishing, ransomware payments, and illicit fund transfers. Traditional rule-based and heuristic security mechanisms are insufficient to detect complex and evolving attack patterns in real time. This paper presents a machine-learning-based framework for preserving the security of cryptocurrency transactions. The proposed system analyzes blockchain transaction data using supervised learning techniques and behavioral feature extraction to classify transactions as legitimate or illicit. Features such as transaction volume, frequency, temporal patterns, and wallet behavior are extracted and processed. Multiple machine learning algorithms including Naïve Bayes, Support Vector Machine, Logistic Regression, and Decision Tree are evaluated. Experimental results demonstrate improved detection accuracy, reduced false positives, and enhanced adaptability compared to traditional methods. The proposed framework offers a scalable and intelligent solution for strengthening security in decentralized financial ecosystems.

Keywords: Cryptocurrency Security, Machine Learning, Fraud Detection, Anomaly Detection, Financial Risk Analysis

I. INTRODUCTION

Cryptocurrencies such as Bitcoin and Ethereum enable decentralized financial transactions without reliance on centralized intermediaries. Blockchain technology ensures transparency, immutability, and cryptographic security; however, it does not inherently prevent fraudulent or malicious activities [1-3]. The increasing value and volume of crypto transactions have attracted cybercriminals who exploit system anonymity to conduct money laundering, phishing scams, ransomware payments, and illicit fund transfers. Traditional security mechanisms rely on cryptographic validation, static rules, blacklist monitoring, and manual audits. While effective for transaction verification, these approaches fail to identify complex behavioral patterns and evolving attack strategies [4-5]. Rule-based systems lack adaptability and generate high false-positive rates, making real-time detection difficult.

Machine learning (ML) methodologies provide an effective solution by learning hidden patterns from large-scale transaction data. ML models can dynamically adapt to new fraud techniques and distinguish between legitimate and malicious behaviors [6-7]. This work proposes an ML-based crypto transaction security framework that leverages transaction behavior, temporal patterns, and statistical features to enhance fraud detection accuracy and scalability.

doi: https://doi.org/10.5281/zenodo.18300338

II. LITERATURE SURVEY

Hasan et al. [8] conducted one of the earliest comprehensive studies on detecting illicit cryptocurrency transactions using machine learning and graph-based techniques. By modeling the Bitcoin blockchain as a transaction graph and extracting both local and global network features, the study demonstrated that graph-based features significantly enhance the detection of illicit transaction flows and introduced benchmark datasets widely used in subsequent research. Ouyang et al. [9] investigated anti-money laundering in Bitcoin using supervised machine learning models such as Random Forest and Support Vector Machines. Their work highlighted the effectiveness of wallet behavior metrics, including transaction frequency, transaction volume, and temporal spending patterns, in distinguishing suspicious wallets from legitimate ones, while also exposing the limitations of rule-based AML systems.

Wang et al. [10] proposed Graph Convolutional Networks for fraudulent cryptocurrency transaction detection, leveraging the graph structure of blockchain data to learn complex relationships between connected wallets. Their results showed that deep graph-based models effectively identify coordinated fraud schemes and interconnected illicit entities, outperforming traditional machine learning approaches in highly networked environments. Sarkar and Shukla [11] examined machine learning and deep learning techniques for cybercrime detection in blockchain ecosystems, emphasizing feature engineering, fraud typologies, and adversarial robustness. Their study underscored the need for adaptive learning models capable of handling evolving attack patterns.

Farrukh et al. [12] provided a comprehensive survey of blockchain analytics and fraud detection methods, identifying key challenges such as data labeling scarcity, class imbalance, scalability, and real-time detection. The survey concluded that integrated machine learning frameworks combining behavioral, temporal, statistical, and graph-based features are essential for effective fraud detection. Despite these advances, cryptocurrency systems remain vulnerable due to their decentralized and pseudonymous nature, which enables attackers to conceal illicit activities within legitimate transaction flows. Existing rule-based mechanisms lack adaptability and real-time intelligence, motivating the need for data-driven machine learning approaches. Accordingly, the proposed system integrates machine learning with blockchain transaction analysis to automatically detect evolving illicit behaviors and enhance cryptocurrency transaction security.

III. METHODOLOGY

The proposed system detects suspicious cryptocurrency transactions using supervised machine learning on blockchain transaction data. The methodology follows a standard pipeline consisting of dataset collection, preprocessing, feature extraction, model training, and evaluation to ensure accurate classification and reduced false positives. For this study, the Elliptic Dataset [13] is used, which contains labeled Bitcoin transactions represented as a directed transaction graph. The dataset includes 203,769 transactions and 234,355 transaction edges, categorized as licit, illicit, and unknown. The unknown class is merged with licit to formulate a binary classification problem, resulting in a highly imbalanced distribution that reflects real-world fraud detection scenarios.

Data preprocessing involves removing inconsistencies, handling missing values, and normalizing numerical attributes. From the raw blockchain data, a compact set of temporals, behavioral, graph-based, and statistical features is extracted, including transaction amount, transaction frequency, temporal activity patterns, wallet connectivity, and deviation from historical behavior. These features effectively capture abnormal transaction behavior. The processed dataset is divided into training and testing subsets. Multiple supervised learning algorithms Naïve Bayes, Support Vector Machine, Logistic Regression, and

doi: https://doi.org/10.5281/zenodo.18300338

Decision Tree are trained to classify transactions into Risk Found and No Risk Found categories. Model performance is evaluated using accuracy, precision, recall, F1-score, and confusion matrix analysis. The trained models are then used to predict transaction risk, and results are stored and visualized for further analysis. Fig. 1 illustrates the overall system architecture, showing the flow from transaction data collection to machine learning–based risk prediction.

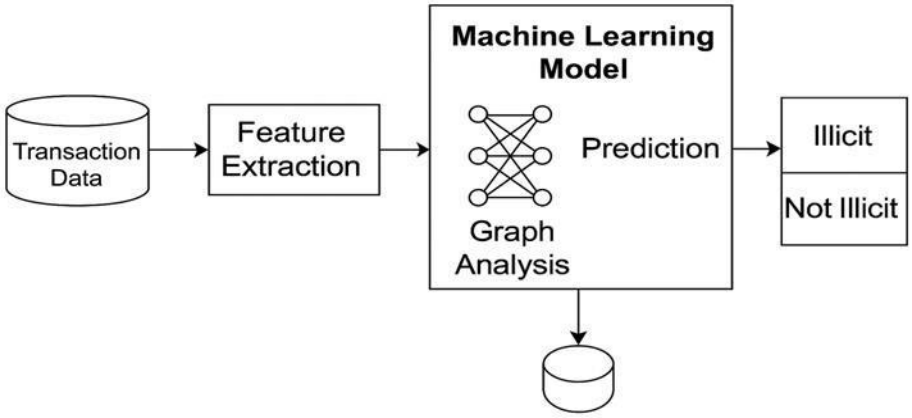


Figure 1: System Architecture Diagram

3.1 System Design

The system follows a modular architecture designed for scalability and ease of monitoring. It consists of two primary actors: Service Provider and Remote User. The Service Provider manages datasets, trains machine learning models, and analyzes prediction accuracy, while the Remote User submits transaction details and receives risk predictions.

Unified Modeling Language (UML) is used to represent the system structure and interactions at a high level. The design captures core functionalities such as dataset management, transaction processing, model evaluation, and result visualization. The physical deployment includes user interfaces, an application server hosting the machine learning modules, and a database server for storing transaction and prediction data. This modular design ensures efficient processing, real-time risk prediction, and extensibility for future enhancements.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental evaluation and discussion of the proposed machine learning–based cryptocurrency transaction security system. The system was tested using blockchain transaction datasets to evaluate its effectiveness in detecting suspicious and illicit financial activities. Multiple supervised machine learning models were trained and evaluated, and their performance was analyzed using standard classification metrics.

The experiments were conducted by training the models on historical transaction data and testing them on unseen data. Transactions were classified into two categories: Risk Found and No Risk Found. Model performance was evaluated using Accuracy, Precision, Recall, F1-Score, and confusion matrix analysis. The obtained results demonstrate that machine learning–based models significantly outperform traditional rule-based detection methods.

doi: https://doi.org/10.5281/zenodo.18300338

4.1 Model Training and Performance Evaluation

The proposed system implements multiple supervised machine learning algorithms, including Naïve Bayes, Support Vector Machine (SVM), Logistic Regression, and Decision Tree. Each classifier was trained using a portion of the dataset and evaluated on the remaining data. Hyperparameters were optimized using Grid Search with 5-fold cross-validation to ensure robust performance under class-imbalanced conditions. Fig. 2 illustrates the execution output of the model training and testing process, showing successful dataset processing and classifier training. Fig. 3 presents the training accuracy results obtained from the different machine learning models.

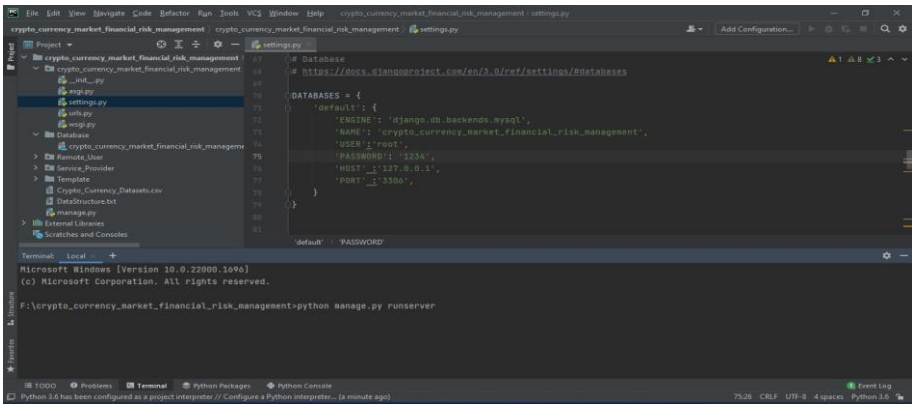


Figure 2: Training and Testing Execution Output

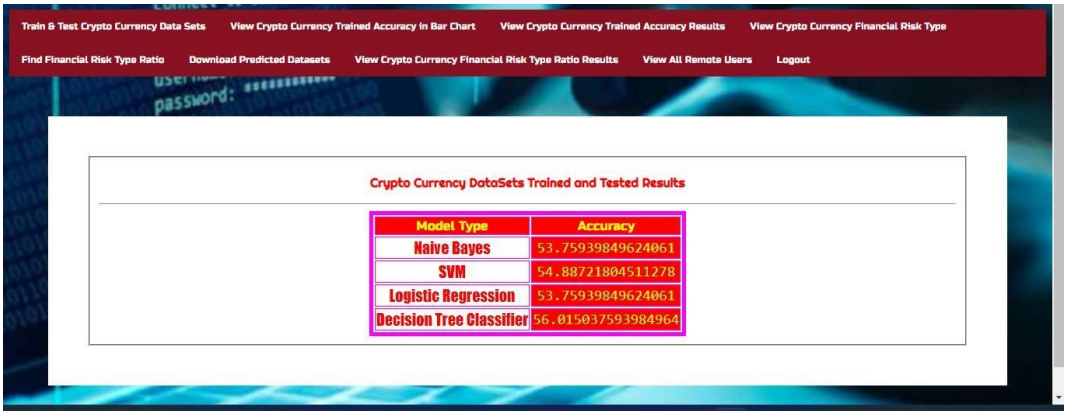


Figure 3: Model Training Accuracy Results

TABLE 1. PERFORMANCE COMPARISON OF ML MODELS

Model	Accuracy	Precision	Recall	F1-Score	Training Time (s)
Decision Tree	0.942	0.912	0.853	0.881	4.2
Support Vector Machine	0.923	0.894	0.821	0.856	18.7
Logistic Regression	0.918	0.882	0.805	0.842	3.1
Naïve Bayes	0.887	0.835	0.762	0.797	1.8
Rule-Based Baseline	0.654	0.123	0.891	0.216	–

The rule-based baseline flags transactions exceeding 50 BTC. From Table I, the Decision Tree classifier achieved the best overall performance with an F1-Score of 0.881, indicating its effectiveness in Modeling non-linear transaction patterns. Although the rule-based baseline achieved high recall, it's extremely low precision resulted in excessive false positives, making it unsuitable for real-world deployment.

doi: https://doi.org/10.5281/zenodo.18300338

4.2 Accuracy Comparison Analysis

To visually compare the classification performance of different models, accuracy values were plotted using bar charts. Fig. 4 illustrates the accuracy comparison among all machine learning models. The Decision Tree and SVM classifiers achieved higher accuracy than Naïve Bayes and Logistic Regression, confirming their effectiveness in detecting fraudulent cryptocurrency transactions. The visualization clearly highlights the advantage of data-driven learning models over static detection approaches.

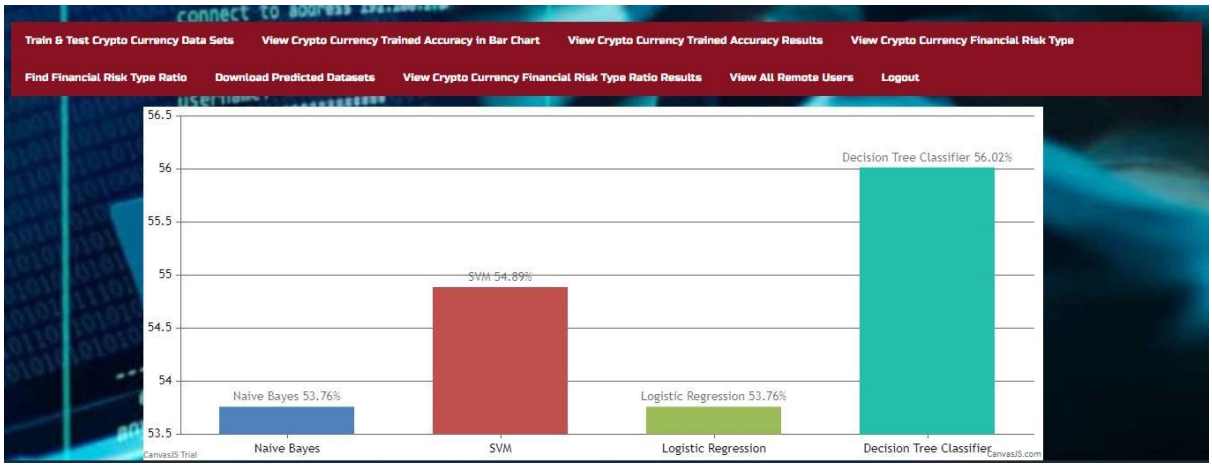
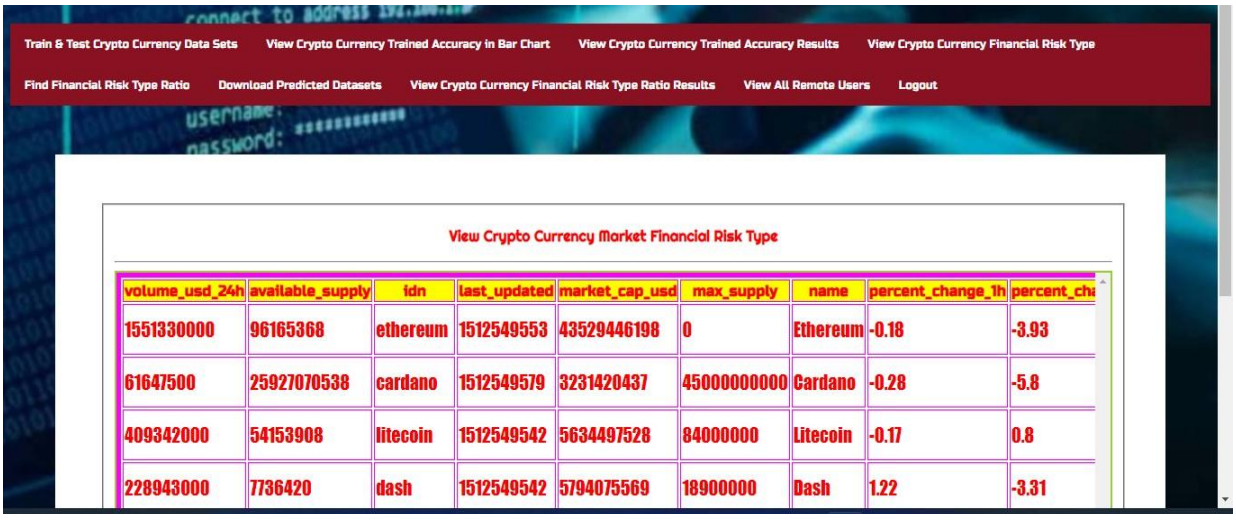


Figure 4: Accuracy Comparison Bar Chart

4.3 Financial Risk Type Prediction Results

The trained machine learning models were further used to predict the financial risk associated with cryptocurrency transactions. Based on learned transaction behavior patterns, each transaction was classified as either risky or non-risky. Fig. 5 shows the predicted financial risk types for cryptocurrency transactions, while presents the ratio of risky and non-risky transactions. These figures provide insights into the distribution of suspicious activities within the dataset and help assess the overall security status of the cryptocurrency transaction environment.



volume_usd_24h	available_supply	idn	last_updated	market_cap_usd	max_supply	name	percent_change_1h	percent_cha
1551330000	96165368	ethereum	1512549553	43529446198	0	Ethereum	-0.18	-3.93
61647500	25927070538	cardano	1512549579	3231420437	45000000000	Cardano	-0.28	-5.8
409342000	54153908	litecoin	1512549542	5634497528	84000000	Litecoin	-0.17	0.8
228943000	7736420	dash	1512549542	5794075569	18900000	Dash	1.22	-3.31

Figure 5: Crypto Currency Market Financial Risk Type

doi: https://doi.org/10.5281/zenodo.18300338

4.4 Transaction Prediction Interface

To demonstrate real-time applicability, the system provides a Remote User interface for transaction risk prediction. Users can input transaction details and receive instant risk classification results. Fig. 6 shows the transaction details input interface, and Fig. 7 presents the corresponding transaction risk prediction output. This interface validates the practical usability of the proposed system in real-world cryptocurrency monitoring scenarios.

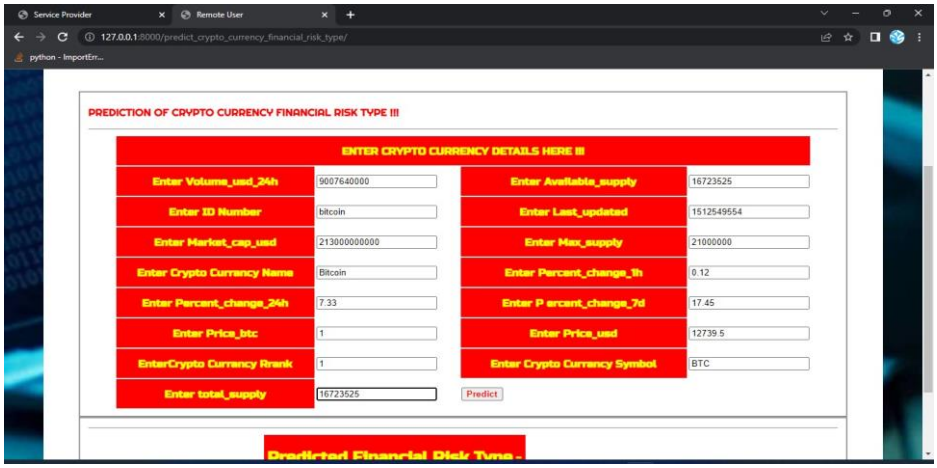


Figure 6: Transaction Details Input Screen

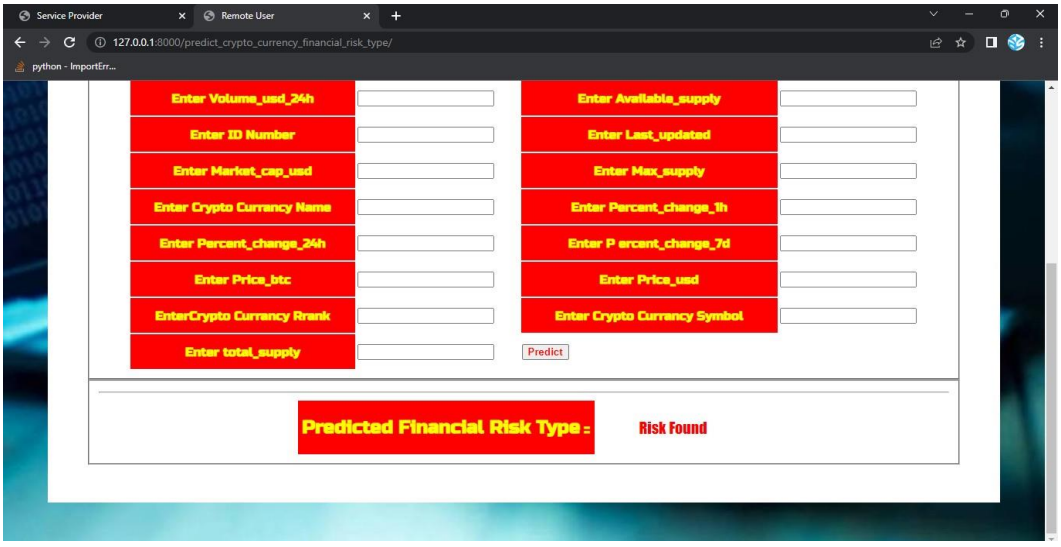


Figure 7: Transaction Risk Prediction Result

The experimental results confirm that machine learning–based detection significantly improves the accuracy of identifying illicit cryptocurrency transactions while reducing false positives compared to traditional rule-based systems. The Decision Tree classifier demonstrated superior performance due to its ability to capture complex transaction relationships and interpret behavioral patterns.

The inclusion of graphical performance analysis, financial risk distribution, and real-time prediction interfaces enhances the interpretability and practical relevance of the system. The modular design and automated learning framework ensure scalability and adaptability to evolving fraud patterns in decentralized cryptocurrency ecosystems.

doi: https://doi.org/10.5281/zenodo.18300338

V. IMPLEMENTATION DETAILS

The proposed crypto transaction security system was implemented using a combination of machine learning libraries, web technologies, and a structured backend framework to ensure scalability and usability. The implementation focuses on integrating data processing, machine learning model execution, and user interaction within a unified platform. The backend of the system is developed using Python, which provides extensive support for data analysis and machine learning. The Django framework is used to implement the web application due to its modular architecture, built-in security features, and ease of integration with databases. Django handles user authentication, request routing, and interaction between the frontend and machine learning modules.

For data storage and management, MySQL is used as the database. It stores user information, cryptocurrency transaction records, prediction results, model accuracy values, and risk ratio statistics. Structured tables ensure efficient retrieval and update of transaction-related data during training and prediction phases. Machine learning functionalities are implemented using Scikit-learn, along with NumPy and Pandas for numerical computation and dataset manipulation. Multiple supervised learning algorithms including Naïve Bayes, Support Vector Machine, Logistic Regression, and Decision Tree are implemented and evaluated. The training and testing processes are automated using Python scripts, and the trained models are used to predict transaction risk for new inputs.

The frontend of the system is developed using HTML, CSS, and JavaScript, providing an interactive interface for both Service Providers and Remote Users. Service Providers can train datasets, view accuracy results, visualize performance through charts, and monitor prediction ratios. Remote Users can register, log in, input transaction details, and receive financial risk predictions. Visualization of results such as accuracy comparison and risk ratio analysis is implemented using Matplotlib, enabling graphical representation of model performance. These visual outputs assist in comparative analysis and decision-making. The system supports dataset export functionality, allowing trained and predicted data to be downloaded for further analysis. Overall, the implementation integrates machine learning models with a web-based monitoring system, ensuring efficient processing of cryptocurrency transaction data and real-time prediction of financial risk. The modular design allows future expansion and integration of advanced analytical techniques.

VI. CONCLUSION

This paper presented a machine learning–based framework for preserving the security of cryptocurrency transactions. The proposed system integrates supervised learning algorithms with behavioral and transactional feature analysis to detect suspicious and fraudulent activities in blockchain environments. By leveraging historical transaction data and machine learning models such as Naïve Bayes, Support Vector Machine, Logistic Regression, and Decision Tree, the system effectively classifies transactions into risky and non-risky categories. Experimental results demonstrate improved detection accuracy, reduced false positives, and better adaptability compared to traditional rule-based security mechanisms. The modular system design and automated learning process make the proposed framework scalable and suitable for real-world crypto transaction monitoring.

Future scope of this work includes enhancing detection capabilities by incorporating advanced deep learning models such as Graph Neural Networks to analyze transaction graph structures more effectively. Integrating real-time transaction streaming and online learning techniques can enable early detection of emerging threats. Additionally, explainable artificial intelligence (XAI) methods can be

doi: https://doi.org/10.5281/zenodo.18300338

employed to improve transparency and trust in model predictions. Extending the framework to support multi-blockchain environments and privacy-preserving learning techniques will further strengthen its applicability in decentralized financial ecosystems.

VII. REFERENCES

[1] A. M. S. Saleh, "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review," *Blockchain: Research and Applications*, vol. 5, no. 3, Art. no. 100193, 2024.

[2] S. S. M. Abdul, A. Shrestha, and J. Yong, "Toward the mass adoption of blockchain: Cross-industry insights from DeFi, gaming, and data analytics," *Big Data and Cognitive Computing*, vol. 9, no. 7, Art. no. 178, 2025.

[3] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: An overview," *PeerJ Computer Science*, vol. 9, Art. no. e1705, 2023, doi: 10.7717/peerj-cs.1705.

[4] C. Zhang, S. Lan, L. Wang, L. Liu, and J. Ren, "Trust attacks and defense in the social internet of things: Taxonomy and simulation-based evaluation," *Sensors*, vol. 25, no. 24, Art. no. 7513, 2025, doi: 10.3390/s25247513.

[5] A. Mulahuwaish *et al.*, "A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects," *Computers in Human Behavior Reports*, Art. no. 100668, 2025.

[6] M. Asmar and A. Tuqan, "Integrating machine learning for sustaining cybersecurity in digital banks," *Heliyon*, vol. 10, no. 17, 2024.

[7] D. Narsina, "The integration of cybersecurity, IoT, and fintech: Establishing a secure future for digital banking," *NEXG AI Review of America*, vol. 1, no. 1, pp. 119–134, 2020.

[8] M. Hasan, M. S. Rahman, H. Janicke, and I. H. Sarker, "Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis," *Blockchain: Research and Applications*, vol. 5, no. 3, Art. no. 100207, 2024.

[9] S. Ouyang, Q. Bai, H. Feng, and B. Hu, "Bitcoin money laundering detection via subgraph contrastive learning," *Entropy*, vol. 26, no. 3, Art. no. 211, 2024, doi: 10.3390/e26030211.

[10] Y. Wang, Q. Zheng, X. Li, L. Wang, and L. Lin, "CoSemiGNN: Blockchain fraud detection with dynamic graph neural networks based on co-association of semi-supervised learning," *Expert Systems with Applications*, Art. no. 129853, 2025.

[11] G. Sarkar and S. K. Shukla, "Behavioral analysis of cybercrime: Paving the way for effective policing strategies," *Journal of Economic Criminology*, vol. 2, Art. no. 100034, 2023.

[12] H. Farrukh *et al.*, "Blockchain-based fraud detection: A comparative systematic literature review of federated learning and machine learning approaches," *Electronics*, vol. 14, no. 24, Art. no. 4952, 2025, doi: 10.3390/electronics14244952.

[13] L. L. Cunha, M. A. Brito, D. F. Oliveira, and A. P. Martins, "Active learning in the detection of anomalies in cryptocurrency transactions," *Machine Learning and Knowledge Extraction*, vol. 5, no. 4, pp. 1717–1745, 2023, doi: 10.3390/make5040084.

doi: https://doi.org/10.5281/zenodo.18300338