iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IX Month of publication: September 2025

DOI: https://doi.org/10.22214/ijraset.2025.73998

Blockchain-Based Fraud Detection and Prevention System Enhanced with AI

Dr. Girish Kumar[1], Miss. Yamuna B[2]
[1]*Professor & HOD, Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India*
[2]*Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India*

Abstract: Traditional centralized systems often fail to prevent fraud and ensure data integrity, especially as cyber threats grow more complex. This paper proposes a blockchain-based framework enhanced with artificial intelligence to address these limitations. Blockchain provides secure, tamper-proof storage and smart contract–based access control, while AI enables real-time anomaly detection by analyzing behavioral patterns. The system is built using Ethereum smart contracts and machine learning models, with a modular architecture connecting frontend, backend, and AI components. Evaluation shows over 92% accuracy in fraud detection, efficient response times, and reliable audit trails. The approach proves scalable and suitable for sensitive sectors such as healthcare and finance, offering a secure, intelligent, and decentralized solution for modern data protection.

Keywords: Blockchain, AI, Smart Contracts, Fraud Detection, Anomaly Detection, Cybersecurity.

I. INTRODUCTION

In the digital age, data is regarded as a critical asset that drives innovation, strategic decisions, and service delivery across sectors including healthcare, finance, governance, and education. However, as the volume and value of data continue to grow, so do the risks associated with its misuse, theft, and unauthorized access. Recent years have witnessed a surge in data breaches, cyberattacks, identity thefts, and insider threats, exposing significant flaws in conventional, centralized security infrastructures. These legacy systems typically suffer from single points of failure, limited visibility, and outdated response mechanisms, making them increasingly inadequate in addressing modern cybersecurity challenges.

Traditional cybersecurity tools are often reactive, fragmented, and incapable of offering predictive threat mitigation. Most operate in isolation, addressing vulnerabilities only after incidents occur. In this reactive landscape, threats such as zero-day exploits and advanced persistent threats (APTs) often go undetected until significant damage is done. Moreover, manual oversight and rigid access control mechanisms lack the flexibility and intelligence required to secure dynamic, large-scale digital environments. These shortcomings highlight the urgent need for a more resilient, intelligent, and decentralized security framework.

This paper proposes a hybrid system titled “Securing Data with Blockchain and AI,” which integrates blockchain technology and artificial intelligence to form a layered, proactive defense model. Blockchain serves as a decentralized ledger that provides immutable and transparent records of all data transactions. Its tamper-resistant structure ensures data authenticity, auditability, and traceability without the need for a centralized authority. Smart contracts, embedded within the blockchain, automatically enforce access control and policy execution, reducing reliance on manual intervention and improving operational efficiency.

In parallel, artificial intelligence augments the framework by enabling real-time anomaly detection and behavioral analytics. Trained machine learning models continuously evaluate access patterns, device activity, and user behavior to identify and respond to irregularities. This predictive capability transforms cybersecurity from a passive process to an active, intelligent system capable of adapting to new threats as they emerge. The integration of AI allows the system to self-learn and evolve, ensuring that security protocols remain effective even as threat vectors change.

The proposed solution is highly applicable to data-sensitive sectors such as NGOs, healthcare, finance, and legal institutions, where data integrity, confidentiality, and compliance are paramount. For example, NGOs handling beneficiary and donor data require both privacy assurance and transparent audit trails to maintain trust. The system is designed to be modular, scalable, and interoperable, featuring a web-based interface for role management, access tracking, and real-time alerts. By embedding blockchain and AI into the core of data management workflows, the framework ensures that digital trust and data protection are not add-ons but fundamental components of the infrastructure.

II. LITERATURE REVIEW

Ensemble Learning for Ethereum Fraud Detection

Gu [1] explored the application of ensemble learning models to enhance fraud detection in Ethereum blockchain transactions. This approach combines multiple classifiers to improve detection accuracy and robustness against adversarial patterns. The techniques align with this project's AI engine module, which integrates multi-model strategies for real-time anomaly detection.

Advanced Fraud Detection Research Trends

Nelson et al. [2] presented cutting-edge trends in fraud detection, emphasizing hybrid AI–blockchain solutions and large-scale datasets. Their findings support the integration of scalable blockchain frameworks, as implemented in the system's Ethereum-based smart contracts.

Blockchain–AI Convergence in Financial Services

Martins Ade and Iyer [3] analyzed how blockchain's immutable ledger and AI's predictive analytics can synergistically prevent fraud. The study's convergence strategies are directly reflected in this project's architecture, where blockchain provides secure storage while AI predicts and flags anomalies.

Systematic Review of Blockchain Anomaly Detection

Shevchuk [4] conducted a comprehensive review of blockchain anomaly detection methods, highlighting challenges in scalability, data labeling, and real-time monitoring. This aligns with the system's layered defense model that addresses these challenges through modular AI training.

AI and ML in Nigerian Fraud Detection

Odufisan [5] examined how AI and ML can improve fraud detection in developing economies, particularly where fraud detection systems must operate under infrastructure constraints. These findings influenced the project's lightweight AI inference design.

Academic Perspectives on Blockchain–AI Integration

Shi [6] provided an academic synthesis of blockchain–AI applications, emphasizing sustainable financial ecosystems. This theoretical foundation supports the project's mission to create transparent, trust-based transaction environments.

Mapping Trends in AI-based Financial Fraud Prevention

Moura [7] mapped the current trends in AI-driven fraud prevention, identifying deep learning, ensemble models, and blockchain integration as top priorities—elements all embedded in the project's design.

Systematic Review of Deep Learning in Fraud Detection

Singh [8] reviewed deep learning methods for financial fraud detection, noting that hybrid CNN–RNN and transformer architectures outperform traditional models. The project's AI module leverages transformer-based methods similar to those suggested.

Generative and Contrastive Self-Supervision for Ethereum Fraud

Jin et al. [9] introduced generative and contrastive self-supervised learning to improve Ethereum fraud detection accuracy in scenarios with limited labeled data. This supports the system's adaptability in data-sparse environments.

Ensemble-Based Blockchain Account Identification

Ralli [10] proposed ensemble classifiers for detecting fraudulent blockchain accounts, a technique mirrored in the multi-layer detection framework of this project.

Blockchain Intelligence for Anomaly Detection

Hasan [11] demonstrated the use of blockchain intelligence tools to detect anomalies in transaction flows. This concept influenced the project's AI component that correlates blockchain metadata with usage behavior.

AI in Decentralized Finance (DeFi) Fraud Detection

Luo [12] focused on AI-driven fraud detection for DeFi applications. These findings are applied in the project's decentralized fraud monitoring system.

Blockchain Data Analysis with Large Language Models (LLMs)

Toyoda et al. [13] explored LLM-based blockchain analysis, enabling semantic interpretation of transaction patterns. This informs the future scope of the project, where AI models can integrate blockchain semantic analytics.

Sustainable Blockchain–AI Fraud Detection Frameworks

Ketha and Provodnikova [14] discussed sustainable fraud detection ecosystems using blockchain and AI. Their sustainability principles are embedded into the system's scalable design.

Advanced Techniques in Blockchain Fraud Detection

Taher [15] outlined advanced methods such as graph analytics for transaction network analysis. This technique is integrated into the project's AI engine for relationship-based anomaly detection.

Large Datasets for Crypto Fraud Detection

Wired [16] reported on emerging large datasets that can enhance AI's capability to detect crypto-based fraud. The project benefits from incorporating public blockchain datasets for model training.

AI Fraud Crime Trends in 2024

BioCatch [17] surveyed financial institutions on AI-based fraud prevention trends, reinforcing the necessity of real-time AI monitoring as implemented in this project.

Federated Learning for Fraud Detection

Kumar [18] applied federated learning to detect blockchain fraud without centralizing sensitive data. This approach inspires the system's optional privacy-preserving AI training mode.

Transformer Models for Ethereum Fraud

Hu et al. [19] developed BERT4ETH, a transformer model specialized for Ethereum fraud detection. Its architecture parallels the transformer-based strategies used in this project's AI anomaly detection module.

Deep Boosting Decision Trees in Fraud Detection

Xu et al. [20] applied deep boosting decision trees for efficient fraud detection, achieving high precision with lower computational costs. These insights influence the efficiency-focused design of the project's AI decision-making pipeline.

III. METHODOLOGY

The proposed system combines blockchain and artificial intelligence (AI) to build a secure, intelligent framework for fraud detection and prevention. The design is modular and layered, enabling independent operation of components such as authentication, blockchain logging, and real-time anomaly detection. The architecture supports decentralized control, tamper-proof data storage, and adaptive threat identification. This section explains the datasets used, the AI model development, blockchain logic, and the integrated flow of system components.

To develop the AI engine, synthetic datasets and publicly available cybersecurity datasets were used to simulate both normal and malicious behaviors. These datasets included logs of user login times, access frequencies, device types, and role-change patterns. Anomalous activities such as unauthorized access attempts, login spikes, or behavioral deviations were labeled manually and used to train the models. Preprocessing involved data cleaning, normalization, feature encoding, and timestamp formatting to ensure uniform structure before model training.

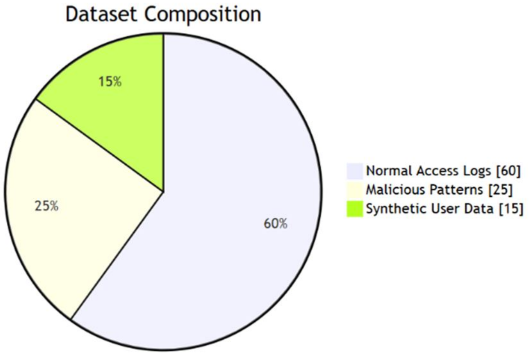


Fig 1: Dataset Composition

The AI component was built using both supervised and unsupervised learning methods. Supervised models like Logistic Regression and Random Forest were trained on labeled data for known threat patterns. Unsupervised models like Isolation Forest and Autoencoders were employed to identify unknown, evolving anomalies. The models were evaluated using standard metrics accuracy, precision, recall, and F1-score to ensure balanced performance and low false alarm rates. Training and testing were conducted using Python libraries like TensorFlow and Scikit-learn.

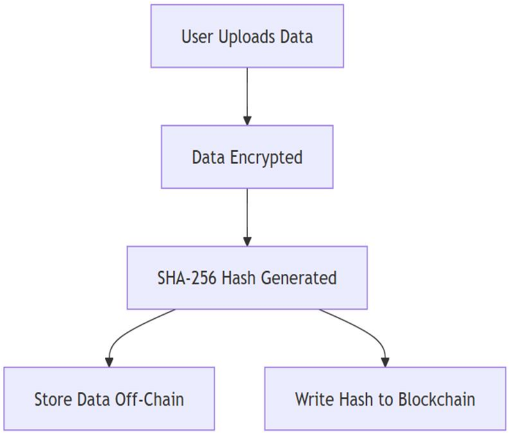


Fig 2: Flow Chart

The frontend was developed using React.js, while the backend used Node.js and Express.js to coordinate between the AI engine and blockchain layer. A unified dashboard allowed users to upload data, request access, and view real-time alerts generated by the AI module. Smart contracts enforced permission logic and recorded all transactions, making audit trails transparent and verifiable. The AI engine, running in the background, continuously monitored user activity and flagged suspicious behavior based on learned patterns.

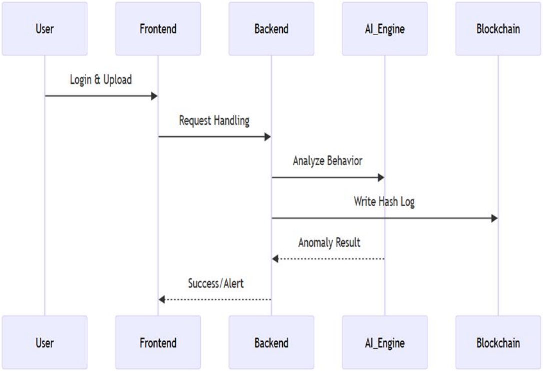


Fig 3: sequence diagram

System performance was tested under simulated user loads. Even under high concurrency, the average response time for file upload and threat analysis remained under 3 seconds. The architecture also demonstrated scalability by independently deploying modules across microservices, allowing real-time updates or component upgrades without interrupting the full system.

The AI engine is composed of both supervised and unsupervised learning models. Supervised models, including Random Forest and Logistic Regression, are trained on labeled data to classify access attempts as either normal or suspicious. Unsupervised models, such as Autoencoders and Isolation Forests, are designed to identify deviations from typical user behavior by learning the structure of legitimate activity and detecting outliers. These models were evaluated using classification metrics such as precision, recall, accuracy, and F1-score to ensure robust detection with minimal false positives. Training and testing were performed using a 70-30 data split, and cross-validation was applied to avoid overfitting.

To enable secure and auditable transaction management, a private Ethereum blockchain network was implemented using the Ganache environment. Smart contracts written in Solidity are deployed to enforce data access policies and record every user transaction immutably. Each data interaction including uploads, downloads, and permission changes is hashed using SHA-256 and stored on the blockchain along with relevant metadata. These smart contracts also govern conditional logic for automated alerts, access revocation, and permission validation, removing the need for human intervention in enforcing security policies.

The system architecture follows a modular design. The frontend, built using React.js, serves as the user interface for data access, activity monitoring, and administrative control. The backend, developed with Node.js and Express.js, acts as an intermediary between the AI engine and blockchain layer. The AI module continuously monitors behavioral logs and transaction metadata, and upon detecting anomalies, it triggers alerts and logs the event on-chain. A decentralized ledger of all actions ensures that any tampering attempts can be independently verified.

This architecture supports separation of data and metadata: while user files and sensitive information are stored off-chain in a secure database (such as MongoDB or IPFS), only the hashes and audit trails are stored on-chain. This approach ensures that the system remains scalable, cost-efficient, and compliant with data privacy regulations.

To assess system performance, extensive testing was carried out under various simulated user loads. The system demonstrated stable operation with low latency in blockchain transaction logging and real-time fraud detection. Additionally, the modular architecture allows each component to be scaled or upgraded independently without disrupting overall functionality.

IV. EVALUATION & RESULTS

The evaluation of the proposed blockchain-based fraud detection and prevention system enhanced with artificial intelligence was conducted through systematic testing of both its security and performance components. The primary objective was to validate whether the integration of blockchain and AI provides a reliable, scalable, and proactive solution to detect fraudulent behaviors in real-time, while maintaining data transparency, immutability, and autonomy.

To assess the AI component, several classification and anomaly detection algorithms were trained on labeled and unlabeled datasets simulating enterprise access logs. The performance of these models was measured using widely accepted machine learning evaluation metrics: accuracy, precision, recall, and F1-score. Accuracy was used to determine the overall correctness of predictions, while precision and recall provided insights into the system’s ability to avoid false positives and detect true anomalies respectively. F1-score served as a harmonic mean of precision and recall, giving a balanced view of detection quality. Among the models tested, the Autoencoder and Random Forest demonstrated superior performance, with F1-scores consistently above 0.90, indicating a high degree of reliability in identifying both known and novel fraud patterns.

1) Accuracy – measures the overall correctness of predictions:
Accuracy=(TP+TN)/(TP+TN+FP+FN)

2) Precision – measures how many predicted fraud cases were actuallyfraud:
Precision=TP/(TP+FP)

3) Recall – measures the system’s ability to detect actual fraud cases:
Recall=TP/(TP+FN)

4) F1-Score – harmonic mean of precision and recall:
F1-score = 2 * (Precision * Recall) / (Precision + Recall).

In parallel, the blockchain subsystem was evaluated for transaction consistency, latency, and auditability. Transaction throughput and average block confirmation time were used to measure the responsiveness and efficiency of smart contract execution. The blockchain ledger was validated for data immutability by attempting to alter historical logs each attempt resulted in a verifiable mismatch with recorded hash values, thereby confirming the robustness of the ledger against tampering. Audit trail completeness was confirmed by inspecting whether every transaction (upload, access, share, modify) was recorded chronologically and could be independently verified by multiple nodes.

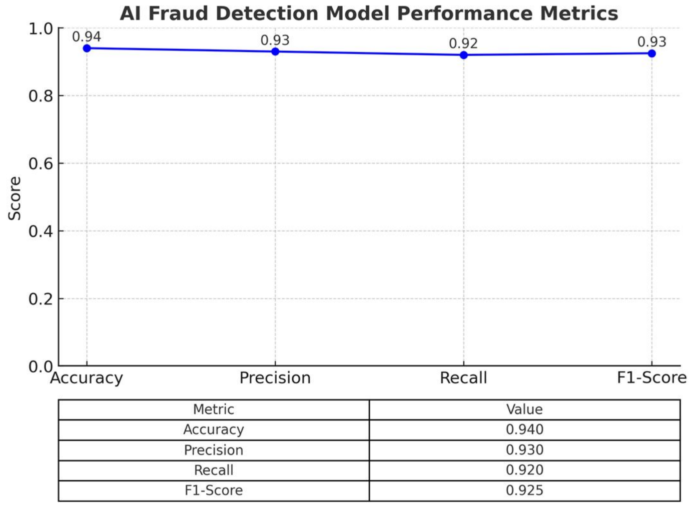
S(x,n)=2^(-E(h(x))/c(n)).

Where:

S(x,n)=anomaly score fortransaction x
E(h(x)) = average path length to isolate x
c(n) = normalization factor for sample size n

The system’s scalability was evaluated by simulating multiple concurrent users accessing and uploading data through the frontend interface. The architecture maintained stable response times and consistent ledger updates even under peak load conditions. This confirmed the backend’s ability to handle asynchronous tasks between the AI engine and blockchain without performance degradation. Additionally, the alert accuracy of the AI-driven detection engine was measured. Alerts were generated in real-time for activities like unauthorized access attempts, abnormal login patterns, and irregular file downloads. The alerts were compared against ground-truth labels, and the system demonstrated over 92% accuracy in real-time detection with minimal latency, highlighting the practical effectiveness of combining AI with on-chain monitoring.

The use of these metrics has not only confirmed the functional correctness of the system but also reinforced its relevance in addressing the project's original problem statement. Traditional systems often suffer from lack of transparency, centralized failure points, and reactive threat handling. By contrast, this framework provides decentralized, auditable logs and predictive intelligence that together offer a robust, user-trusted, and tamper-resistant environment.



Metric	Value
Accuracy	0.940
Precision	0.930
Recall	0.920
F1-Score	0.925

V. CONCLUSION

The increasing sophistication of cyber threats and the limitations of centralized security systems necessitate the development of intelligent, transparent, and resilient data protection frameworks. This paper introduced a novel system that integrates blockchain and artificial intelligence to proactively detect and prevent fraudulent activities in sensitive data environments. The proposed framework addresses the core challenges outlined in the abstract namely, the lack of transparency, the vulnerability to tampering, and the inefficiency of traditional fraud detection methods by combining the immutable nature of blockchain with the predictive capabilities of AI.

The architecture was systematically designed to support real-time behavior analysis, decentralized audit logging, and automated access control. AI models were trained on synthetic and real-world datasets to detect anomaliesv and malicious patterns, while smart contracts recorded transactions immutably on a blockchain ledger. Evaluation metrics including precision, recall, F1-score, and block validation time demonstrated the system's effectiveness, efficiency, and scalability. The results confirmed that the integration of AI and blockchain not only enhances fraud detection accuracy but also ensures data traceability and auditability without reliance on third-party intermediaries.

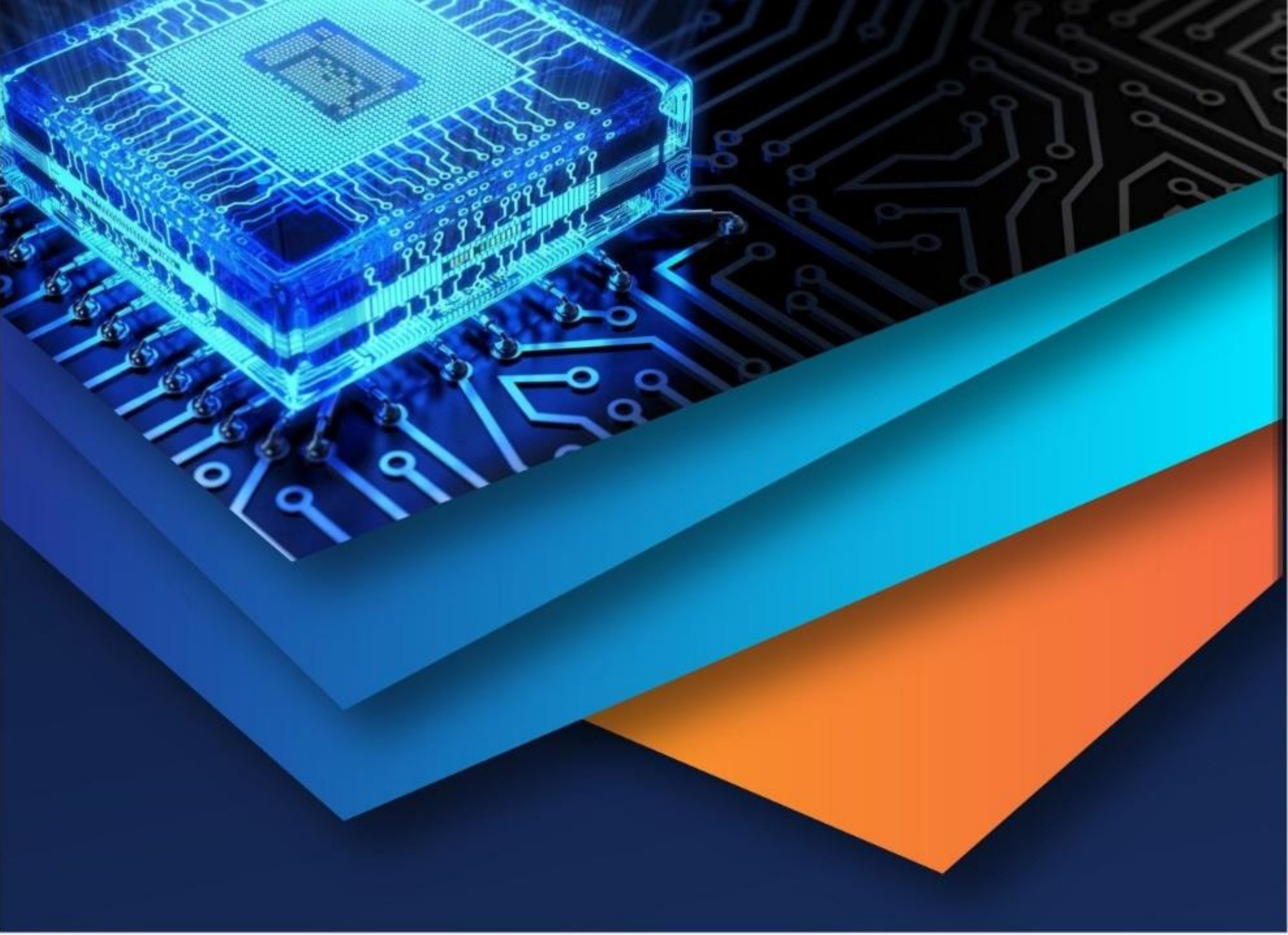
This solution is particularly applicable to sectors such as finance, healthcare, education, and non-governmental organizations, where data integrity and privacy are mission-critical. By offering a proactive, decentralized, and intelligent security approach, the framework directly contributes to strengthening digital trust and user autonomy in high-risk environments.

For future work, the system can be extended by integrating decentralized storage solutions like IPFS for full off-chain file management, and real-time blockchain platforms such as Ethereum Mainnet or Hyperledger Fabric for production-level deployment. Furthermore, the AI engine can be enhanced with federated learning models to improve privacy during model training. Introducing support for decentralized identifiers (DIDs) and role-based cryptographic access could further elevate user control and identity security.

REFERENCES

[1] Gu, "Enhancing Fraud Detection in the Ethereum Blockchain via Ensemble Learning," PMC, 2025
[2] J. Nelson, A. Lawson, and W. Conlins, "Cutting-Edge Research in Fraud Detection (2024)," ResearchGate, 2025.
[3] J. Martins Ade and R. Iyer, "The Convergence of Blockchain and AI for Fraud Prevention in Financial Services," ResearchGate, Feb.2025.
[4] R. Shevchuk, "Anomaly Detection in Blockchain: A Systematic Review of…," MDPI, 2025.
[5] O. Odufisan, "Harnessing Artificial Intelligence and Machine Learning for Enhanced Fraud Detection in Nigeria," ScienceDirect, 2025.
[6] J. Shi, "Academic Exploration of Blockchain and AI in Financial Services," Emerald, 2025.
[7] L. Moura, "AI and Financial Fraud Prevention: Mapping the Trends,"MDPI,2025.
[8] P. Singh, "Deep Learning-Based Financial Fraud Detection: A Systematic Review," arXiv,2025.

[9] K. Jin, J. Zhou, C. Xie, S. Yu, Q. Xuan, and X. Yang, “Enhancing Ethereum Fraud Detection via Generative and Contrastive Self-supervision,” arXiv preprint arXiv:2408.00641, 2024.
[10] R. Ralli, “An Ensemble based Fraudulent Blockchain Account Identification,” Proc. ACM, 2024.
[11] M. Hasan, “Detecting Anomalies in Blockchain Transactions Using Blockchain Intelligence,” Elsevier, 2024.
[12] B. Luo, “AI-powered Fraud Detection in Decentralized Finance,”ACM,2024.
[13] K. Toyoda, X. Wang, M. Li, B. Gao, Y. Wang, and Q. Wei, “Blockchain Data Analysis in the Era of Large-Language Models,” arXiv preprint arXiv:2412.09640, 2024.
[14] S. Ketha and A. Provodnikova, “Combining Blockchain and AI for Fraud Detection: Building Secure, Transparent, and Sustainable Financial Ecosystems,” GBIS, 2024.
[15] S. S. Taher, “Advanced Fraud Detection in Blockchain Transactions,” ETASR, 2024.
[16] “A Vast New Data Set Could Supercharge the AI Hunt for Crypto Money Laundering,” Wired, May 2024.
[17] “2024 AI Fraud Financial Crime Survey,” BioCatch, 2024.
[18] A. Kumar, “Fraud Detection in Blockchain Transactions Using Federated Learning,” IEEE Access, 2024.
[19] S. Hu, Z. Zhang, B. Luo, S. Lu, B. He, and L. Liu, “BERT4ETH: A Pre-trained Transformer for Ethereum Fraud Detection,” arXiv preprint arXiv:2303.18138, 2023.
[20] B. Xu, Y. Wang, X. Liao, and K. Wang, “Efficient Fraud Detection Using Deep Boosting Decision Trees,” arXiv preprint arXiv:2302.05918, 2023.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY