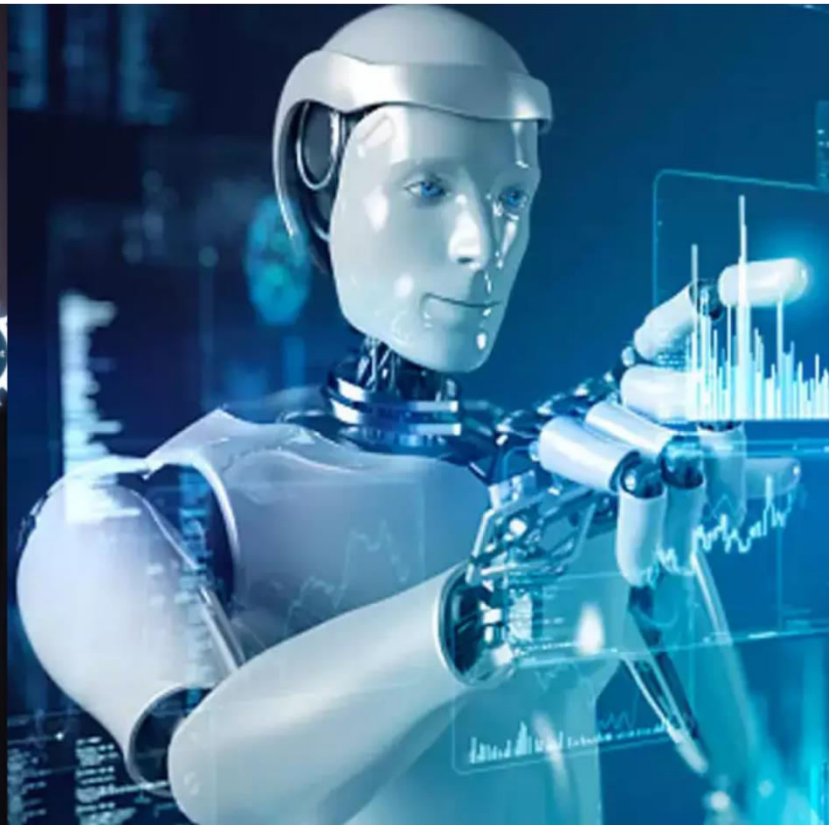
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411046|

A Multi-perspective Fraud Detection Method for Multi-Participant Banking Transactions using Blockchain Technology

Sayali Lipare[1], Prof. S. C. Puranik[2]

ME Student, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[1]

Professor, Department of Computer Engineering, Vishwabharti Academy's College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: In the current digital era, online banking transactions have become a vital part of financial systems, but with the rapid increase in transaction volume, fraudulent activities and unauthorized access have also become a major concern. This project aims to design and develop a secure and transparent platform that minimizes fraud in multi-party banking systems. The system utilizes Blockchain technology to record, verify, and store transaction data in an immutable and decentralized ledger, ensuring that every transaction is traceable and tamper-proof. Each banking activity, whether initiated by a user or a financial institution, is validated by multiple participants to prevent data manipulation and false transaction entries. The proposed model integrates a custom blockchain framework with multi-level authentication mechanisms, including a unique password generation system, visual dual keypad interface, and two-step verification for enhanced security. This ensures that only authorized users can initiate and validate transactions, thereby reducing the risks of identity theft, phishing, and unauthorized fund transfers. Moreover, the blockchain network supports distributed verification, meaning all participating banks and users act as validators, ensuring transaction integrity from multiple perspectives. The fraud detection system analyzes transaction patterns, checks anomalies, and alerts administrators about any suspicious activities in real-time. This web-based system, developed using Java technology, not only provides a secure platform for executing banking transactions but also promotes accountability, transparency, and trust among multiple banking participants. By leveraging blockchain and smart verification layers, the proposed model effectively reduces data breaches, ensures end-to-end encryption, and enhances the resilience of digital banking infrastructures. The combination of blockchain security and intelligent verification mechanisms offers a sustainable solution for the future of secure and fraud-free banking systems.

KEYWORDS: Custom Blockchain Technology, Fraud Detection, Multi-Participant Banking, Distributed Ledger, Consensus Mechanism, Visual Dual Keypad, Two-Step Authentication, Cryptographic Hashing, Java Web Application, Secure Transaction System, etc.

I. INTRODUCTION

Healthcare systems generate large amounts of patient data every day, including medical history, diagnostics reports, treatment details, and prescription records. Traditional centralized databases face challenges such as unauthorized access, data manipulation, and lack of interoperability among hospitals, diagnostic labs, and other healthcare stakeholders. To overcome these challenges, blockchain technology offers a decentralized and secure platform that can store patient data in a tamper-proof and traceable manner.

This project focuses on developing a web-based application using Java technology that integrates blockchain for secure patient data-sharing. The system is designed to connect patients, hospitals, diagnostic centers, and other healthcare entities in a unified framework. Patients can control access to their medical records, hospitals and diagnostic centers can securely share and retrieve data, and blockchain ensures that all transactions are immutable, transparent, and auditable.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411046|

The proposed system also incorporates a Medical Diagnostics Healthcare Supply Chain module, which analyzes the flow of medical services and products from suppliers to hospitals and patients. By integrating blockchain, the system not only enhances data security and privacy but also improves efficiency, traceability, and reliability in the healthcare supply chain. This approach ensures that patient data remains secure while supporting seamless collaboration among healthcare stakeholders, ultimately contributing to better medical outcomes and operational efficiency.

PROBLEM STATEMENT

Current fraud detection systems in banking lack transparency, real-time verification, and strong security against advanced cyberattacks. In multi-participant transactions involving multiple banks or users, tracking and detecting fraudulent activities becomes more difficult. Traditional password-based authentication is also vulnerable to phishing and brute-force attacks. Therefore, there is a need for a secure, transparent, and reliable fraud detection method using custom blockchain technology that ensures data integrity, authenticates users effectively, and prevents fraud in real-time.

II. LITERATURE SURVEY

- **Taher et al. (2024)** presented an advanced fraud detection model for blockchain transactions by combining Ensemble Learning and Explainable Artificial Intelligence (XAI) techniques to improve detection accuracy and interpretability. Their study focused on addressing the major challenge of transparency in blockchain fraud detection models, as most AI-based systems function as black boxes with limited interpretability. The authors proposed a hybrid ensemble framework integrating Random Forest, XGBoost, and Gradient Boosting classifiers to detect fraudulent blockchain activities efficiently. Furthermore, they employed SHAP (SHapley Additive exPlanations) values to interpret model predictions, enabling analysts to understand key contributing features to fraudulent behavior. The model was validated using real-world Ethereum transaction datasets, where it achieved superior detection precision and reduced false positives compared to traditional methods. This research demonstrated that coupling ensemble methods with explainable AI could significantly enhance both performance and trustworthiness in blockchain-based fraud detection systems.

- **Hasan Pranto et al. (2022)** developed a privacy-preserving fraud detection framework that integrates blockchain with machine learning to enhance trust, security, and adaptability in decentralized environments. Their proposed system leverages blockchain's immutability to store encrypted transaction data, which is then analyzed by adaptive ML models for fraud detection while maintaining user privacy. The novelty of this work lies in its incentive-based learning mechanism, where participants contributing accurate fraud reports or model improvements are rewarded using blockchain tokens, promoting collaborative model enhancement. The study also introduced differential privacy techniques to ensure sensitive transaction details remain confidential. Experimental evaluations on simulated datasets demonstrated that this hybrid approach achieved high scalability, better model adaptability, and improved protection against adversarial manipulation. The framework provides a foundation for creating distributed, transparent, and incentive-driven fraud detection systems within financial ecosystems.

- **Zhang et al. (2025)** proposed a Dynamic Feature Fusion (DFF) model that integrates global graph structures and local semantic features for efficient blockchain fraud detection. Recognizing that blockchain transaction data inherently forms complex graph relationships, the authors employed Graph Neural Networks (GNNs) to capture global transaction dependencies while utilizing deep semantic encoders to extract contextual attributes from local transaction records. The fusion of these two perspectives allowed the model to better identify hidden fraud patterns across multi-hop relationships that traditional models often overlook. The study introduced a dynamic attention mechanism to adaptively weigh global and local features based on their relevance, improving model robustness across different blockchain platforms. Experimental results on large-scale Ethereum datasets showed that DFF achieved higher accuracy and recall compared to baseline GCN and CNN models. This approach highlights the significance of combining relational and contextual features for comprehensive blockchain fraud analysis.

- **Reddy et al. (2024)** presented a machine learning-based framework for detecting fraudulent online transactions by analyzing behavioral and transactional features. Their approach utilized supervised algorithms such as Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine (SVM) to identify fraudulent activity patterns from online banking datasets. The system focused on preprocessing and feature engineering to handle imbalanced

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411046|

datasets and improve classification performance. Through comparative analysis, the authors found that the Random Forest model achieved the highest accuracy and reliability due to its ensemble nature and ability to handle non-linear relationships among features. The proposed model also emphasized real-time fraud detection capability and scalability for integration into existing e-banking systems. The research highlighted how classical machine learning techniques can still provide effective and interpretable fraud detection solutions when optimized for transaction data characteristics.

- **Maurya and Kumar (2022)** designed a credit card fraud detection system using multiple machine learning algorithms to enhance fraud identification accuracy in high-volume transactional environments. The authors compared models such as Logistic Regression, K-Nearest Neighbors (KNN), Decision Tree, and Neural Networks to determine their efficiency in detecting anomalies within imbalanced datasets. The study emphasized the importance of data preprocessing, feature selection, and resampling techniques such as SMOTE (Synthetic Minority Oversampling Technique) to handle the imbalance between legitimate and fraudulent transaction samples. Experimental results indicated that ensemble models combining decision trees and neural networks achieved superior precision and recall rates. Additionally, the paper discussed the importance of continuous model retraining to adapt to evolving fraud patterns. Their work contributed valuable insights into designing scalable, accurate, and adaptive fraud detection mechanisms suitable for real-world banking systems.

III. SYSTEM OVERVIEW

The proposed blockchain-based fraud detection system operates as a multi-layered architecture comprising the user interface, application logic, blockchain network, and database layer. The User Interface Layer provides a web-based platform where users can log in securely using the visual dual keypad and two-step authentication system. Once authenticated, users can initiate transactions that are automatically encrypted and sent to the blockchain network. The Application Layer, developed in Java, manages user requests, validates transaction data, and interacts with blockchain APIs for block creation and verification. This layer also includes the fraud detection logic, which continuously analyzes data patterns to identify irregularities.

The Blockchain Layer acts as the backbone of the system, where every verified transaction is stored in a cryptographically linked block. The consensus mechanism ensures that each transaction is validated by multiple participants before being permanently added to the chain. This guarantees data integrity, traceability, and non-repudiation. The Banking and Security Layer oversees the digital signature validation, password generation process, and real-time authentication feedback. Additionally, the Data Layer maintains encrypted copies of transaction history and fraud analysis logs, allowing secure retrieval for audit purposes.

In summary, the System Overview highlights how the integration of blockchain technology, multi-level authentication, and intelligent fraud detection forms a unified and secure financial ecosystem. The modular design ensures scalability, enabling the system to support multiple banks, users, and transaction types. The use of distributed consensus, encryption, and real-time verification minimizes vulnerabilities and builds trust among all stakeholders. By combining security, transparency, and automation, the proposed model lays the foundation for a reliable, fraud-free multi-participant banking environment.

IV. PROPOSED SYSTEM

The proposed system introduces a multi-perspective fraud detection mechanism using a custom blockchain framework for multi-participant banking transactions. It focuses on creating a secure, transparent, and tamper-proof ledger where all transactions are recorded in blocks linked cryptographically to maintain integrity. Each transaction initiated by a user undergoes validation by multiple network participants (banks, nodes, or authorized entities), ensuring that fraudulent or unauthorized actions are identified before final approval. The blockchain structure allows for distributed verification, making it impossible for any single party to alter or manipulate transaction data without consensus from others. This ensures accountability and auditability across all participants in the banking system.

The system architecture consists of several key modules — User Module, Bank Module, and Blockchain Security Module. The user module handles login, registration, and transaction initiation using enhanced authentication features such as visual dual keypad and two-step verification. The bank module manages transaction validation, digital signatures, and consensus generation. The blockchain module stores the validated transactions, performs hashing

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411046|

operations, and ensures the immutability of each block. Every transaction is digitally signed, timestamped, and stored permanently in the ledger, providing a clear and traceable audit trail. Fraud detection is achieved by continuously monitoring transaction patterns, identifying unusual behaviors, and raising alerts for suspicious activities.

Moreover, the system integrates with a Java-based web application for user interaction and real-time monitoring. It employs secure communication protocols and cryptographic hashing algorithms (such as SHA-256) to protect sensitive financial data. The incorporation of blockchain with AI-based fraud analysis ensures that every transaction is verified from multiple perspectives — user, bank, and network — before being executed. This layered approach strengthens the overall resilience of the banking network, providing a secure and scalable framework for future financial systems.

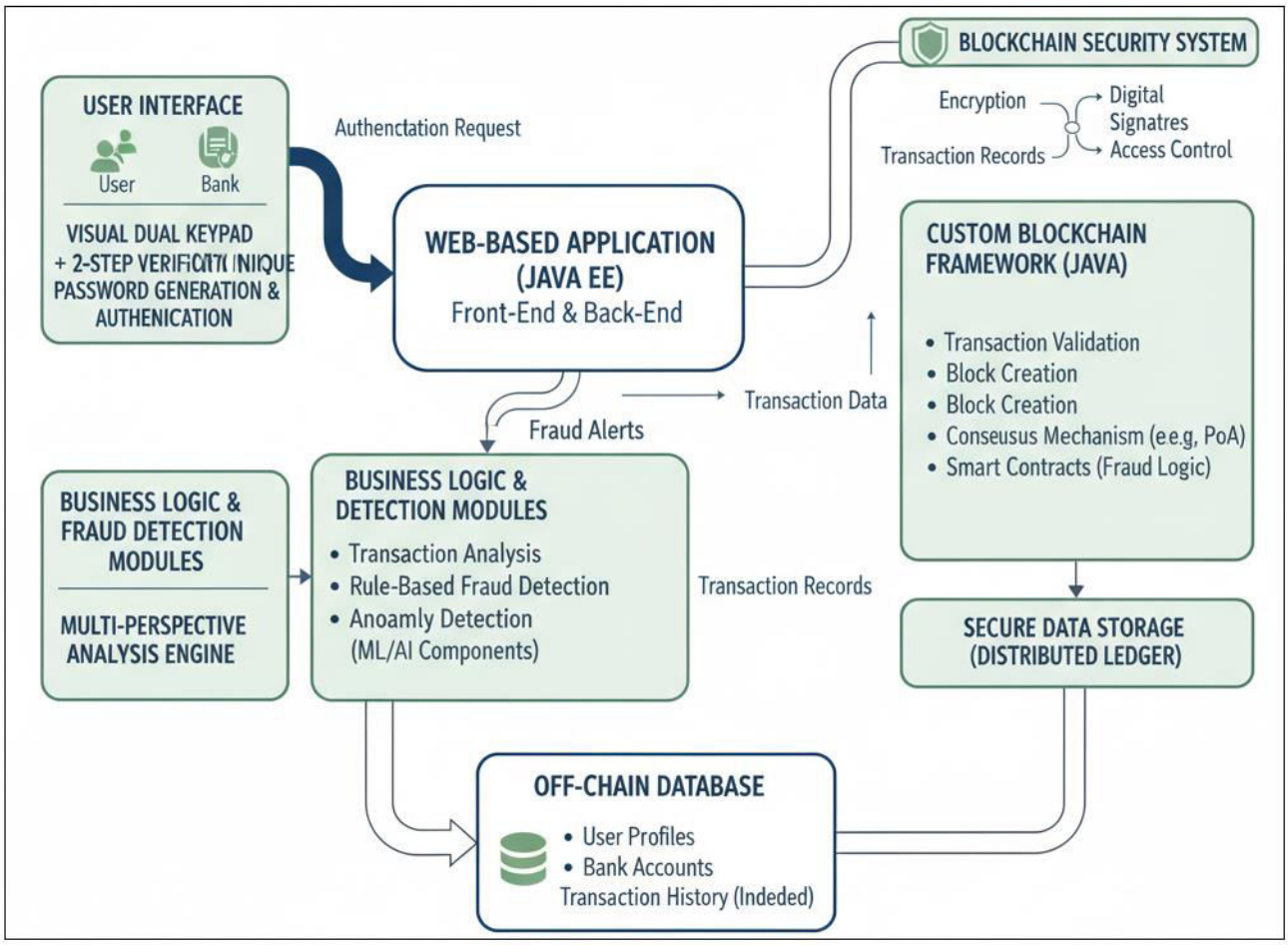


Fig.1: System Architecture Design

V. CONCLUSON

In this paper proposed blockchain-based system presents a robust framework for securing multi-participant banking transactions using a custom blockchain architecture integrated with advanced fraud detection mechanisms. By combining blockchain's inherent properties of immutability, transparency, and decentralization with machine learning-based anomaly detection, the system ensures that all transactions are securely validated and recorded, minimizing the risk of fraudulent activities. The integration of visual dual-keypad authentication and two-step verification adds an additional layer of security, providing both strong user authentication and protection against unauthorized access.

The system architecture and proposed algorithms demonstrate the feasibility of implementing a secure, scalable, and automated banking transaction platform that can handle multiple participants efficiently. By leveraging a web-based

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411046|

interface and Java-based backend, the system provides a user-friendly experience while ensuring high reliability and performance. The modular design, including user, bank, blockchain, and authentication modules, allows easy maintenance, future scalability, and integration with additional security or analytical features. Moreover, the detailed technical specifications, including hardware, software, and network requirements, ensure that the system can be deployed effectively in real-world banking environments.

ACKNOWLEGEMENT

I would like to sincerely thank the researchers and publishers for making their valuable resources available. I am also grateful to my guide for their constant support and guidance, and to the reviewers for their insightful suggestions. Finally, I thank the college authorities for providing the necessary infrastructure and support throughout the course of this project.

REFERENCES

[1] Taher, S. Sh., Ameen, S. Y., & Ahmed, J. A. (2024). "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach." Engineering, Technology & Applied Science Research, 14(1), 12822–12830. DOI: 10.48084/etasr.6641.

[2] Hasan Pranto, T., Akhter, K. T., Rahman, T., Haque, A. K. M. N. I., & Rahman, R. M. (2022). "Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach." arXiv preprint. DOI: 10.48550/arXiv.2210.12609.

[3] Zhang, S., Song, L., & Wang, Y. (2025). "Dynamic Feature Fusion: Combining Global Graph Structures and Local Semantics for Blockchain Fraud Detection." arXiv preprint. DOI: 10.48550/arXiv.2501.02032.

[4] M. R. Reddy, H. Qasim Owaied, M. M. Abdulhasan, P. Karthik, M. Rajkumar and P. U. Kumar, "Fraud Detection of Online transaction Using Machine Learning," 2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), Manipal, India, 2024, pp. 1-7, doi: 10.1109/ARIIA63345.2024.11051851.

[5] Maurya and A. Kumar, "Credit card fraud detection system using machine learning technique," 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom), Malang, Indonesia, 2022, pp. 500-504, doi: 10.1109/CyberneticsCom55287.2022.9865466.

[6] K. Kaur, K. Bhagyalakshmi, S. S. Bharathi, S. Chepyala, K. S. Kumar and R. Singh, "Fraud Detection Using Machine Learning in Blockchain Stock Marketing Transactions," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-7, doi: 10.1109/ICSES63760.2024.10910816.

[7] T. Adam and F. Babič, "Anomaly Detection on Distributed Ledger Using Unsupervised Machine Learning," 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Berlin, Germany, 2023, pp. 1-4, doi: 10.1109/COINS57856.2023.10189278.

[8] M. Bhowmik, T. Sai Siri Chandana and B. Rudra, "Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 539-541, doi: 10.1109/ICCMC51019.2021.9418470.

[9] S. N. Chordia and S. Shinde, "Using Unsupervised Learning to detect Fraud in Cryptocurrency," 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, 2024, pp. 1-6, doi: 10.1109/ICBDS61829.2024.10837066.

[10] K. Singh, N. Singh and D. Singh Kushwaha, "An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 2018, pp. 165-169, doi: 10.1109/GUCON.2018.8674919.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details