Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Enhancing Financial Fraud Detection Using a Hybrid Blockchain–AI Approach

Narayan Jee*[1], Sumit Kumar[2], Sarthika Dutt[3], Anjali Arora[3]

[1]Haridwar University Roorkee, Uttarakhand, India
[2]Shivalik College of Engineering Dehradun, Uttarakhand, India
[3]Dev Bhoomi Uttarakhand University, Uttarakhand, India
[4]Haridwar University Roorkee, Uttarakhand, India

*Corresponding Author.: narayan.btech@gmail.com

Abstract

Financial fraud is a serious problem in the digital economy, with billions being lost each year. Conventional fraud detection schemes are usually insufficient in real-time processing, false positives, and adaptive fraud pattern changes. This paper introduces a Hybrid system combining Block chain and Artificial Intelligence (AI) to improve fraud detection in financial transactions. Block chain provides data immutability and integrity, whereas AI models (machine learning, deep learning) monitor patterns of transactions for detecting anomalies. We compare existing methods, introduce a new architecture that is a hybrid of smart contracts and AI-driven fraud detection, and discuss some of the challenges and research directions Experimental results prove greater accuracy and safety compared to existing practices

Keywords: Block chain, Artificial Intelligence, Fraud Detection, Financial Transactions, Smart Contracts, Machine Learning.

Introduction

The rapid growth of digital financial services has significantly transformed the global financial ecosystem. Online banking, mobile payments, digital wallets, and cryptocurrency transactions have made financial operations faster and more convenient. However, this digital transformation has also increased the risk of financial fraud, including credit card fraud, identity theft, phishing attacks, and money laundering. Financial fraud causes billions of dollars in losses every year and poses a serious threat to financial institutions, businesses, and customers worldwide.

This research proposes a hybrid framework that integrates AI-based fraud detection models with Block chain technology to create a secure and efficient fraud detection system for financial transactions. The proposed architecture utilizes machine learning algorithms to analyze transaction patterns and detect anomalies, while Block chain ensures secure storage and verification of transaction data. Smart contracts are used to automate fraud prevention actions such as transaction blocking and alert generation.

A. Context: The rapid advancement of digital financial systems has transformed the way financial transactions are performed across the world. Online banking, mobile payment systems, e-commerce platforms, and digital wallets have made financial services faster, more convenient, and more accessible. However, this increasing reliance on digital platforms has also led to a significant rise in financial fraud activities. Cybercriminals exploit vulnerabilities in financial systems to perform fraudulent activities such as credit card fraud, identity theft, phishing attacks, money laundering, and unauthorized transactions.

Financial institutions process millions of transactions every day, making it extremely challenging to manually monitor and detect suspicious activities. Traditional fraud detection systems mainly rely on rule-based mechanisms, where predefined rules and thresholds are used to identify potentially fraudulent transactions. Although these systems were effective in earlier financial environments, they struggle to cope with the complexity and scale of modern financial systems. Fraudsters continuously adapt their techniques to bypass security mechanisms, making static rule-based detection systems less effective.

In recent years, the emergence of advanced technologies such as Artificial Intelligence (AI) and Block chain has opened new possibilities for improving fraud detection systems. AI enables intelligent analysis of large volumes of transaction data, while Block chain provides a secure and tamper-resistant platform for storing financial records.

Integrating these technologies has the potential to significantly enhance fraud detection accuracy, transparency, and security in financial systems.

B. Rationale: The primary motivation behind this research is the growing need for more advanced and reliable fraud detection mechanisms in digital financial systems. Traditional fraud detection approaches suffer from several limitations, including high false positive rates, limited scalability, and the inability to detect new or evolving fraud patterns. These limitations create challenges for financial institutions in maintaining secure and trustworthy transaction environments.

Artificial Intelligence provides powerful tools for analyzing complex transaction patterns and identifying anomalies that may indicate fraudulent activity. Machine learning algorithms such as Random Forest, Isolation Forest, and Long Short-Term Memory (LSTM) networks can learn from historical transaction data and continuously improve their detection capabilities. These models can identify both known fraud patterns and previously unseen anomalies, making them highly effective for modern fraud detection.

Block chain technology complements AI by providing a decentralized and immutable ledger for storing financial transactions. Once a transaction is recorded on the Block chain, it cannot be altered or deleted, ensuring data integrity and transparency. Smart contracts can automatically execute predefined rules and trigger alerts or actions when suspicious activities are detected.

By combining Artificial Intelligence and Block chain technology, it is possible to create a hybrid fraud detection system that leverages the strengths of both technologies. AI can analyze transaction behavior and detect anomalies, while Block chain ensures secure and transparent storage of transaction data. This integration can significantly improve the efficiency, reliability, and security of fraud detection systems in financial transactions.

were effective in earlier financial environments, they struggle to cope with the complexity and scale of modern financial systems. Fraudsters continuously adapt their techniques to bypass security mechanisms, making static rule-based detection systems less effective.

In recent years, the emergence of advanced technologies such as Artificial Intelligence (AI) and Block chain has opened new possibilities for improving fraud detection systems. AI enables intelligent analysis of large volumes of transaction data, while Block chain provides a secure and tamper-resistant platform for storing financial records.

Integrating these technologies has the potential to significantly enhance fraud detection accuracy, transparency, and security in financial systems.

C. **Contributions:** This research proposes a hybrid framework that integrates Artificial Intelligence and Block chain technology to enhance fraud detection in financial transactions. The key contributions of this study are summarized as follows:

- The study examines traditional fraud detection techniques and highlights their limitations in handling modern digital financial systems.
- The research proposes a hybrid system that combines AI-based anomaly detection with Block chain-based secure transaction recording.
- A layered architecture is introduced that includes Block chain for secure data storage, AI models for fraud detection, and smart contracts for automated decision-making.
- The research evaluates the performance of different AI algorithms such as Random Forest, Isolation Forest, and LSTM networks in detecting fraudulent transactions.
- The proposed system demonstrates improved fraud detection accuracy and reduced false positive rates compared to traditional rule-based systems.
- The proposed system demonstrates improved fraud detection accuracy and reduced false positive rates compared to traditional rule-based systems.

Literature Review

A. **Traditional Fraud Detection Approaches:** Financial services institutions have used rule-based systems, statistical models, and manual inspection to identify fraudulent activities. These approaches often rely on heuristic approaches such as fixed-thresholds or static if- then rules to spot such malicious behaviour. Among these, easy-to-use patterns are utilized, but they are not always effective against changing fraud strategies and produce a number of false alarms. Besides, they are not flexible and fail to support real-time transaction workloads, which make them not very effective in current digital environments.

Although rule-based systems are simple to implement and easy to understand, they suffer from several limitations. One major drawback is their inability to adapt to new fraud patterns. Fraudsters constantly change their techniques, making static rule-based systems ineffective in detecting newly emerging fraud strategies. Additionally, these systems often produce a large number of false positives, where legitimate transactions are incorrectly flagged as fraudulent. This increases the workload for manual verification and reduces the efficiency of fraud detection processes.

B. **AI-Based Fraud Detection:** With the advancement of computational power and availability of large data sets, Artificial Intelligence (AI) techniques have become increasingly popular for fraud detection. AI-based systems can automatically learn patterns from historical transaction data and identify suspicious activities without relying solely on predefined rules.

Machine Learning (ML) algorithms have been widely applied for fraud detection tasks. Supervised learning techniques such as Decision Trees, Support Vector Machines (SVM),

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Random Forest, and Logistic Regression are commonly used when labeled data sets are available.

These models are trained using historical data containing both fraudulent and legitimate transactions. Once trained, the models can classify new transactions as either fraudulent or legitimate.

Among these techniques, Random Forest has gained significant attention due to its high accuracy and ability to handle large data sets. It works by constructing multiple decision trees and combining their predictions to improve classification performance. Similarly, Support Vector Machines are effective in separating fraudulent and non- fraudulent transactions using optimal hyper-planes.

Unsupervised learning techniques are also widely used in fraud detection, especially when labeled data is limited. Algorithms such as Isolation Forest, K-Means Clustering, and Auto encoders are capable of identifying anomalies in transaction data. These methods detect transactions that significantly deviate from normal patterns, which may indicate fraudulent behavior.

Deep learning models have also shown promising results in fraud detection tasks. Recurrent neural networks (RNN) and Long Short-Term Memory (LSTM) networks are particularly useful for analyzing sequential transaction data. These models can capture temporal patterns and relationships between transactions, enabling them to detect complex fraud patterns that traditional machine learning models may miss.

Despite their effectiveness, AI-based systems also face challenges such as data privacy concerns, lack of transparency in decision-making, and the requirement of large labeled data sets for training.

C. **Block chain-Based Fraud Prevention:** Block chain technology has recently emerged as a powerful tool for improving transparency and security in financial systems. Block chain is a distributed ledger technology that records transactions across multiple nodes in a decentralized network. Once a transaction is recorded in a Block chain block, it becomes extremely difficult to modify or delete, ensuring data integrity and trust.

Several studies have explored the use of Block chain technology for fraud prevention in financial transactions. Block chain systems such as Hyper ledger Fabric and Ethereum allow financial institutions to securely record transaction data in an immutable ledger. This prevents unauthorized modifications and ensures that all transactions are traceable and verifiable.

Smart contracts are another important feature of Block chain technology. These are self-executing programs stored on the Block chain that automatically enforce predefined rules when certain conditions are met. In fraud detection systems, smart contracts can automatically block suspicious transactions, trigger alerts, or initiate further verification processes.

Organizations such as IBM have already explored Block chain-based solutions for secure financial transactions and fraud prevention. By maintaining a decentralized record of financial activities, Block chain helps reduce the risk of data tampering and improves trust among participants in the financial network.

However, Block chain technology also faces certain challenges. Issues such as scalability, transaction latency, and high computational requirements can limit its adoption in large-scale financial systems.

D. **Hybrid AI–Block chain Approaches:** Recent research has explored the integration of Artificial Intelligence and Block chain technology to create more effective fraud detection

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

systems. Hybrid AI–Block chain frameworks combine the predictive capabilities of AI models with the security and transparency provided by Block chain.

In these systems, AI algorithms analyze transaction data and detect anomalies or suspicious patterns. The results of this analysis are then recorded on a Block chain network, ensuring that the fraud detection process is transparent and tamper-resistant. Smart contracts can automatically execute actions such as blocking transactions or notifying financial institutions when potential fraud is detected.

One example of such an approach is the use of AI-driven fraud detection in cryptocurrency transactions, where machine learning models analyze Block chain transaction data to identify suspicious behavior. Companies such as Elliptic have developed Block chain analytics platforms that use AI techniques to detect fraudulent cryptocurrency activities.

Despite the potential benefits of hybrid systems, several research gaps still exist. Challenges include ensuring scalability for high transaction volumes, maintaining privacy while using transparent Block chain networks, and improving the explainability of AI models used in fraud detection.

E. **Research Gap:** Although significant research has been conducted in fraud detection using Artificial Intelligence and Block chain technologies individually, limited work has focused on the effective integration of both technologies in a unified framework. Many existing systems either rely solely on AI models for detecting fraud or use Block chain only for secure transaction storage.

There is a need for a comprehensive fraud detection framework that combines the strengths of both technologies to provide real-time detection, improved accuracy, secure data storage, and automated fraud prevention mechanisms.

The proposed system in this research aims to address these challenges by integrating AI-based anomaly detection models with Block chain-based transaction verification and smart contract automation.

Proposed Methodology and System Architecture

The proposed architecture integrates Artificial Intelligence (AI) and Block chain technology to develop a secure and efficient fraud detection system for financial transactions. The system is designed to analyze large volumes of transaction data, detect suspicious activities using machine learning algorithms, and ensure secure storage of transaction records through Block chain technology. The architecture follows a layered approach consisting of multiple interconnected components that work together to detect and prevent fraudulent activities in real time.

The proposed architecture consists of four major layers: Data Collection Layer, Data Processing Layer, AI-Based Fraud Detection Layer, and Block chain Verification Layer. Each layer performs specific tasks to ensure accurate fraud detection and secure transaction management.

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

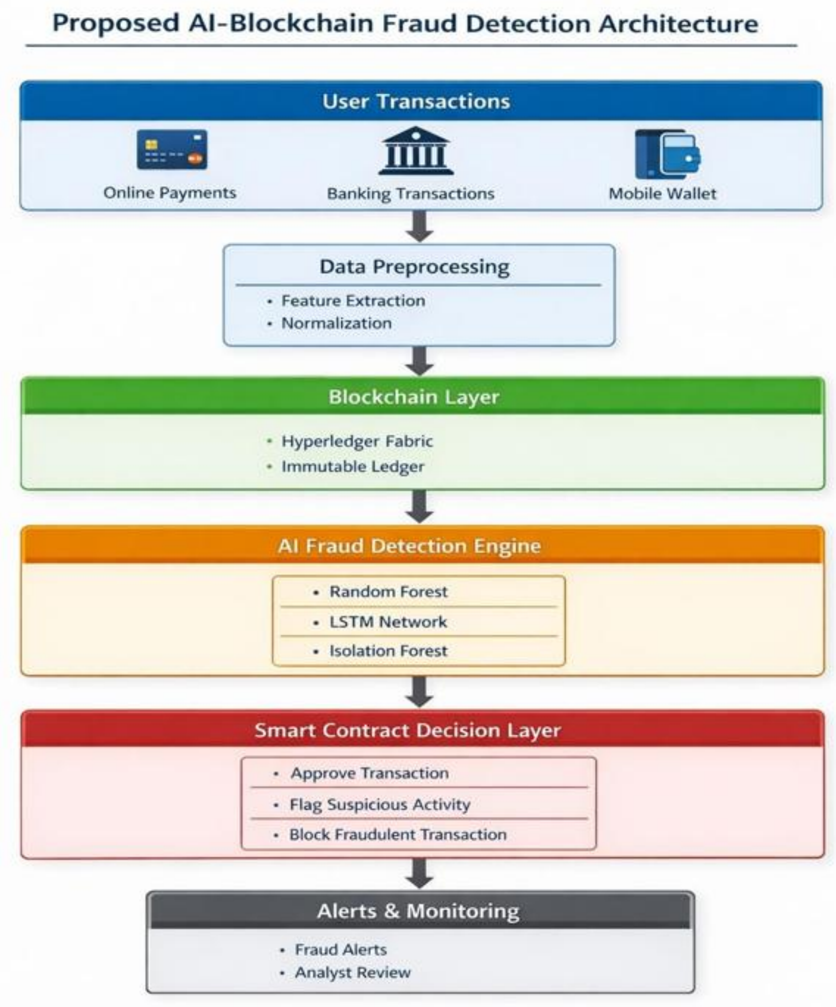

Fig. 1.Hybrid AI–Block chain Architecture for Financial Fraud Detection

A. **Description of IEEE-CIS Fraud Detection data set:** The IEEE-CIS Fraud Detection data set is widely used as a benchmark data set for developing and evaluating financial fraud detection models in machine learning research. The data set is divided into two main parts: transaction data and identity data. The transaction data set contains detailed information about each financial transaction, including attributes such as transaction amount, transaction time, product category, and card details. In total, the data set contains over 590,000 transaction records, each associated with a binary target variable called "is Fraud." This variable indicates whether a transaction is fraudulent or legitimate. A value of 1 represents a fraudulent transaction, while 0 represents a legitimate transaction. The data set also includes a large number of anonymized features (V1–V339) that are generated through feature engineering techniques to capture hidden patterns in transaction behavior.

B. **Data Collection Layer:** The data collection layer is responsible for gathering transaction data from various financial platforms such as online banking systems, payment gateways, credit card networks, and digital wallet applications. The collected data contains multiple attributes that describe the transaction behavior.

Typical transaction attributes include:

- Transaction ID
- Transaction amount
- Timestamp of transaction
- Location of transaction
- User identification details
- Merchant category
- Transaction frequency

This data serves as the input for the fraud detection system. Since financial transaction data is often large and complex, efficient data collection mechanisms are required to ensure that the system can process transactions in real time.

C. **Data Processing and Feature Engineering Layer:** Before applying machine learning models, the collected transaction data must be processed and transformed into a suitable format for analysis. This layer performs data preprocessing and feature engineering tasks to improve model performance.

The major processes in this layer include:

- Data Cleaning: Removing incomplete or inconsistent records from the data set.
- Data Normalization: Scaling transaction values to maintain uniformity in the data set.
- Feature Extraction: Identifying important transaction characteristics such as transaction amount patterns, user spending behavior, transaction location changes, and frequency of transactions.
- data set Splitting: Dividing the data set into training and testing sets for machine learning model development.

D. **AI-Based Fraud Detection Layer:** The AI-based fraud detection layer is the core component of the proposed architecture. This layer uses machine learning and deep learning algorithms to analyze transaction patterns and identify suspicious behavior. Several AI models are used in the system to detect fraudulent transactions:

- Random Forest Algorithm: Random Forest is a supervised machine learning algorithm that builds multiple decision trees to classify transactions as legitimate or fraudulent. It provides high accuracy and performs well with large data sets.
- Isolation Forest Algorithm: Isolation Forest is an unsupervised learning algorithm used for anomaly detection. It identifies unusual transaction patterns that differ significantly from normal behavior.
- Long Short-Term Memory (LSTM) Network: LSTM is a deep learning model that analyzes sequential transaction data. It captures temporal relationships between transactions and helps detect complex fraud patterns that occur over time.

Random Forest provides high classification accuracy, Isolation Forest detects anomalies, and LSTM captures sequential transaction patterns. Combining these models improves the overall fraud detection capability.

The trained models analyze incoming transactions and assign a fraud probability score to each transaction.

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Transactions that exceed a predefined risk threshold are flagged as suspicious and forwarded to the Block chain verification layer.

E. Block chain Verification Layer

The Block chain layer ensures secure and tamper-proof storage of financial transaction records. In the proposed system, a private Block chain network such as Hyper-ledger Fabric is used to maintain confidentiality while ensuring distributed verification.

Block chain technology provides the following benefits:

- Immutability: Once a transaction is recorded in the Block chain, it cannot be modified or deleted.
- Transparency: All participants in the network can verify transaction records.
- Security: Cryptographic techniques protect transaction data from unauthorized access.

Smart contracts are deployed within the Block chain network to automate fraud detection responses. When the AI detection layer identifies a suspicious transaction, the smart contract automatically executes predefined actions such as

- Blocking the transaction.
- Generating alerts for financial institutions.
- Requesting additional authentication from users.

This automated mechanism significantly reduces the response time for fraud prevention.

F. Decision and Alert Layer

The final layer of the system is responsible for making decisions based on the outputs generated by the AI models and Block chain verification process.

The system performs the following actions:

- Approve Transaction: If the transaction is classified as legitimate.
- Flag Transaction: If the transaction is suspicious but requires further verification.
- Block Transaction: If the transaction is identified as fraudulent.
- Generate Alert: Notify banks or financial authorities for manual investigation.

By integrating AI-driven fraud detection with Block chain-

based security mechanisms, the proposed architecture provides a robust, transparent, and efficient system for detecting fraudulent financial transactions.

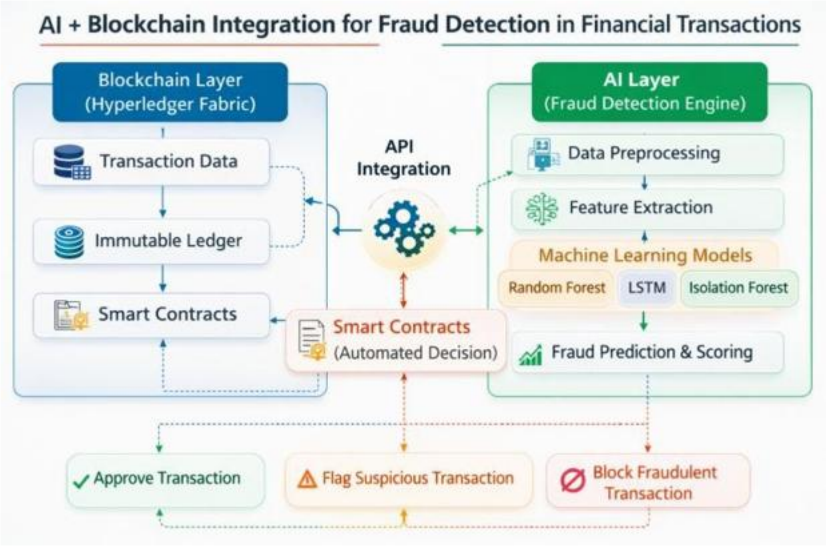
AI + Blockchain Integration for Fraud Detection in Financial Transactions
Blockchain Layer (Hyperledger Fabric)
Transaction Data
Immutable Ledger
Smart Contracts
API Integration
AI Layer (Fraud Detection Engine)
Data Preprocessing
Feature Extraction
Machine Learning Models
Random Forest
LSTM
Isolation Forest
Smart Contracts (Automated Decision)
Fraud Prediction & Scoring
✓ Approve Transaction
⚠ Flag Suspicious Transaction
Block Fraudulent Transaction

Fig. 2 AI and block chain Integration for fraud detection.

Performance Evaluation

A. Mathematical Model: Fraud detection in financial transactions can be formulated as a binary classification problem, where each transaction is classified as either legitimate or fraudulent.

Let:

T={t1,t2,t3,...,tn} represent the set of financial transactions. Each transaction contains multiple features: ti=(x1,x2,x3,...,xm)
where:

x1 = Transaction amount

x2 = Transaction time

x3 = User location

xm = Other behavioral attributes

The fraud detection model predicts a probability score: P(Fraud|ti)

where:

P(Fraud|ti) represents the probability that transaction ti is fraudulent.

A classification decision is made using a threshold value θ :

$$f(ti) = \in)^{1,} \left\{ \begin{array}{ll} & (ru|) > 0 \\ 0, & \qquad hr \end{array} \right.$$

where:

- 1 = Fraudulent transaction
- 0 = Legitimate transaction

B. Evaluation Metrics and Result: To evaluate the performance of the proposed AI–Block chain fraud detection system, several standard machine learning evaluation metrics are used. These metrics help measure the ability of the model to correctly identify fraudulent and legitimate transactions. Since fraud detection is a classification problem, performance is evaluated using metrics derived from the confusion matrix.

A confusion matrix represents the prediction results of a classification model and contains four important components:

- True Positive (TP): The number of fraudulent transactions that are correctly identified as fraud.
- True Negative (TN): The number of legitimate transactions that are correctly identified as non- fraudulent.
- False Positive (FP): The number of legitimate transactions that are incorrectly classified as fraudulent.
- False Negative (FN): The number of fraudulent transactions that are incorrectly classified as legitimate.

Based on these values, several performance evaluation metrics are calculated to assess the effectiveness of the fraud detection system.

- **Accuracy:** Accuracy measures the overall correctness of the classification model. It represents the ratio of correctly predicted transactions to the total number of transactions in the data set.

$$accurcy = \frac{P+N}{P+N+P+N}$$

Although accuracy provides a general measure of model performance, it may not always be reliable for fraud detection problems because fraudulent transactions usually represent a very small percentage of the total data set.

- **Precision:** Precision measures the proportion of correctly identified fraudulent transactions among all transactions that were predicted as fraudulent. It indicates how reliable the fraud predictions made by the model are.

$$Prco = \frac{P}{P+P}$$

A high precision value means that the system generates fewer false alarms, which is important for reducing unnecessary transaction investigations.

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

- **Recall (Sensitivity):** Recall measures the ability of the model to correctly detect fraudulent transactions. It represents the proportion of actual fraud cases that are successfully identified by the system.

$$c = \frac{P}{P + N}$$

  A high recall value indicates that the system can detect most fraudulent transactions, minimizing the risk of fraud going unnoticed.

- **F1-Score:** The F1-score is the harmonic mean of precision and recall. It provides a balanced evaluation of the model when both precision and recall are important.

$$1 - cor = \frac{2 \times (Prco \times c)}{P + N}$$

  The F1-score is particularly useful in fraud detection problems where the data set is highly imbalanced.

- **Fraud Detection Rate:** Fraud Detection Rate represents the percentage of fraudulent transactions correctly identified by the system. A higher fraud detection rate indicates better performance of the fraud detection model.

Table I. Summary of Adversarial Attacks And Defense Techniques

Model	***Accuracy***	***Precisi o n***	***Recall***	***F1-score***
Random Forest	0.94	0.91	0.93	0.92
LSTM	0.96	0.93	0.95	0.94
Isolation Forest	0.90	0.88	0.90	0.89
Hybrid AI+Block chain	0.97	0.95	0.96	0.95

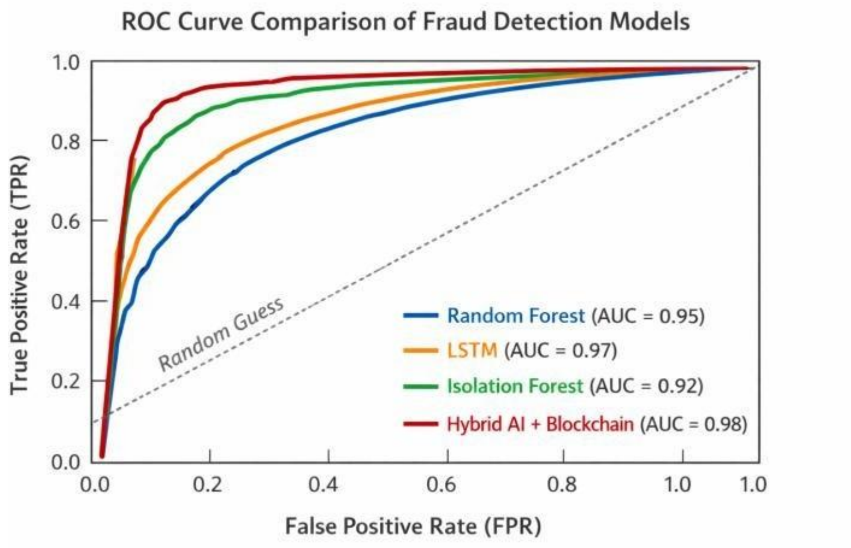

Fig. 3 Fraud detection Model Comparison.

Discussion

The experimental results demonstrate that the proposed hybrid fraud detection system combining Artificial Intelligence and Block chain technology provides improved performance in detecting fraudulent financial transactions. The evaluation metrics, including precision, recall, and F1- score, indicate that machine learning models are capable of identifying suspicious transaction patterns with a high level of accuracy.

Among the evaluated models, the Long Short-Term Memory (LSTM) network achieved the highest performance due to its ability to analyze sequential transaction data and capture temporal dependencies. Financial transactions often occur in sequences, and fraudulent activities may follow specific patterns over time. The LSTM model is particularly effective in learning these sequential behaviors, which helps in identifying complex fraud patterns that may not be easily detected by traditional machine learning models.

The Random Forest algorithm also demonstrated strong performance in classifying transactions as legitimate or fraudulent. As an ensemble learning method, Random Forest constructs multiple decision trees and aggregates their predictions to improve classification accuracy and reduce over-fitting. This makes it highly suitable for handling large financial transaction data sets with multiple features.

In contrast, the Isolation Forest model is designed specifically for anomaly detection and works by isolating unusual data points that differ from normal transaction behavior. Although its precision and recall values are slightly lower than those of supervised models, Isolation Forest plays an important role in detecting previously unseen or unknown fraud patterns. This capability is valuable in financial systems where new fraud strategies continuously emerge.

The integration of multiple models in the proposed architecture creates a hybrid fraud detection framework that improves overall system robustness. Each model contributes unique strengths: Random Forest provides strong classification capabilities, Isolation Forest identifies anomalies, and

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

LSTM captures sequential transaction behavior. The combination of these approaches allows the system to detect both known and emerging fraud patterns more effectively.

Another important component of the proposed system is the integration of block chain technology. It provides a decentralized and tamper-resistant ledger for recording financial transactions. By storing verified transactions on the block chain network, the system ensures data transparency, integrity, and security. This reduces the risk of data manipulation and enhances trust in the fraud detection process.

However, despite the promising results, some limitations remain. The performance of AI models is highly dependent on the quality and diversity of the data-set used for training. If the dateset does not adequately represent real-world fraud scenarios, the models may struggle to detect certain types of fraudulent behavior. Additionally, implementing block chain technology in real-time financial systems may introduce computational overhead and latency challenges.

Future improvements may include the use of larger and more diverse financial transaction data sets, optimization of deep learning architectures, and integration with real-time streaming fraud detection systems. Furthermore, advanced techniques such as federated learning and explainable AI could be incorporated to enhance model transparency and scalability in large-scale financial applications.

Overall, the results indicate that the proposed hybrid AI and Block chain-based fraud detection system provides an effective approach for improving the security and reliability of financial transactions.

Conclusion and Future Work

Financial fraud has become a major concern in modern digital financial systems due to the rapid growth of online transactions and digital payment platforms. Traditional fraud detection methods often struggle to identify complex and evolving fraud patterns, which makes the use of advanced technologies necessary. This research proposed a hybrid fraud detection framework that integrates Artificial Intelligence techniques with Block chain technology to enhance the security and reliability of financial transactions.

Although the proposed system demonstrates promising results, several improvements can be explored in future research. One possible direction is the use of larger and more diverse real-world financial transaction data sets to further improve the accuracy and generalization capability of the models. Incorporating additional deep learning architectures such as Graph Neural Networks or Transformer-based models may also enhance the detection of complex fraud patterns.

Future work can also focus on implementing real-time fraud detection systems that can analyze transactions instantly and prevent fraudulent activities before they are completed.

Optimizing the Block chain integration to reduce computational overhead and latency will be important for deploying the system in large-scale financial environments.

Additionally, explainable AI techniques can be integrated into the fraud detection models to provide better interpretability and transparency of model decisions. This will help financial institutions understand why a transaction has been flagged as fraudulent and improve trust in automated fraud detection systems.

By addressing these areas, future research can further enhance the efficiency, scalability, and practical applicability of AI and block-chain-based fraud detection systems in the financial sector.

References

[1] D. V. Lindberg and H. K. H. Lee, “Optimization under constraints by applying an asymmetric entropy measure,” J. Comput. Graph. Statist., vol. 24, no. 2, pp. 379–393, Jun. 2015,doi: 10.1080/10618600.2014.901225.

[2] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[3] F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation forest,” in Proc. IEEE Int. Conf. Data Mining, Pisa, Italy, 2008, pp. 413–422.

[4] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” Neural Computation, vol. 9, no. 8, pp. 1735–1780,1997.

[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Block chain technology: Beyond bitcoin,” Applied Innovation Review, vol. 2, pp. 6–19, 2016.

[7] A. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, “The application of data mining techniques in financial fraud detection: A classification framework and academic review,” Decision Support Systems, vol. 50, no. 3, pp. 559–569, 2011.

[8] D. B. Rawat and V. Doku, “Block chain technology for IoT applications and cybersecurity,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2004–2013, 2019.

[9] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, “Data mining for credit card fraud: A comparative study,” Decision Support Systems, vol. 50, no. 3, pp. 602– 613, 2011.

[10] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2016, pp. 785–794.

[11] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[12] J. West and M. Bhattacharya, “Intelligent financial fraud detection: A comprehensive review,” Computers & Security, vol. 57, pp. 47–66, 2016.

[13] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[14] A. Dorri, S. S. Kanhere, and R. Jurdak, “Block chain in internet of things: Challenges and solutions,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2004–2015, 2019.

[15] P. K. Chan and S. J. Stolfo, “Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection,” in Proc. ACM SIGKDD Int. Conf., 1998, pp. 164–168.

[16] S. Jurgovsky, M. Granitzer, S. Ziegler, S. Calabretto, and L. Portier, “Sequence classification for credit-card fraud detection,” Expert Systems with Applications, vol. 100, pp. 234–245, 2018.

[17] J. Chen, H. Li, and K. Li, “Credit card fraud detection using deep learning and machine learning models,” IEEE Access, vol. 9, pp. 93024–93034, 2021.

[18] M. M. Rahman and M. A. Islam, “A hybrid machine learning approach for financial fraud detection,” Journal of Information Security and Applications, vol. 58, pp. 102–110, 2021.

[19] Y. Yuan and F. Y. Wang, “Block chain and cryptocurrencies: Model, techniques, and applications,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, 2018.

Received: 2026-02-05
Accepted: 2026-03-20
Published Online: 2026-03-30
DOI: 10.70454/JRIST.020103

[20] K. Zhou, Y. Wang, and L. Zhang, "Deep learning-based fraud detection for financial transactions," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 12, pp. 5558–5568, 2021.