Decentralized Fraud Detection Using Blockchain and Adaptive Machine Learning

Meghana[1], Vaishnavi[1], Nandini[1], Dora Vyshnavi[1], B. Hari Krishna[2], S. Shiva Prasad[3]
[1]Student, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad
[2] Assistant Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad
[3] Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad
doi.org/10.64643/IJIRTV12I8-191562-459

***Abstract*—With the rapid increase in digital financial transactions, the threat of fraud has significantly intensified, challenging the reliability of traditional machine learning (ML)-based fraud detection systems. These existing systems often rely on centralized databases that are vulnerable to tampering by insiders, leading to compromised ML models and inaccurate fraud predictions. To address these concerns, this project proposes a novel framework that integrates Blockchain technology with Machine Learning to provide a tamper-proof, privacy-preserving, and adaptive fraud detection system. Blockchain ensures data integrity and security by storing model weights in decentralized, immutable blocks verified through cryptographic hash functions. Smart contracts developed using Solidity enable secure storage and retrieval of ML model weights on the Ethereum blockchain.**

***Index Terms*—Blockchain, Machine Learning, Fraud Detection, Privacy Preservation, Smart Contracts, Ethereal Blockchain, Decentralized System, Tamper-Proof Data Storage**

I. INTRODUCTION

In the digital age, fraud continues to pose a significant threat across sectors such as finance, healthcare, e-commerce, and telecommunications. The increasing volume, velocity, and variety of data, coupled with the growing sophistication of fraudulent activities, have rendered traditional detection systems inadequate. Recent advancements in machine learning (ML) have brought new promise to fraud detection by enabling automated and adaptive identification of anomalous behaviors. However, these systems often face challenges related to data privacy, model transparency, and resistance to adversarial manipulation.

Simultaneously, blockchain technology has emerged as a decentralized and tamper-proof ledger system offering transparency, traceability, and enhanced security. Its immutability and consensus-driven validation mechanisms make it an appealing infrastructure for fraud-resistant systems. However, blockchain alone is not well-suited for real-time fraud detection or intelligent pattern recognition, areas where ML excels.

This paper proposes a privacy-preserving and adaptive incentive-based framework that synergistically combines blockchain and machine learning for fraud detection. The proposed architecture ensures that sensitive data remains secure through on-chain/off-chain hybrid storage models, while ML algorithms operate on encrypted or obfuscated data to maintain user confidentiality. Moreover, we introduce an incentive mechanism powered by smart contracts to reward honest participants and data contributors, fostering collaborative fraud intelligence without compromising trust or privacy.

The integration of blockchain and ML not only enhances fraud detection capabilities but also introduces self-regulating, explainable, and tamper-resistant ecosystems that are resilient to evolving fraud tactics. By addressing both detection efficacy and data governance, this research aims to set a foundation for scalable and trustworthy fraud detection systems in decentralized environments.

II. LITERATURE SURVEY

Blockchain technology has been widely recognized for its ability to enhance security and transparency in digital systems through its decentralized and immutable ledger structure. By ensuring that

transaction records cannot be altered once validated, blockchain significantly improves data integrity and traceability, which are critical requirements in fraud detection environments. Studies such as those by Zheng et al. (2018) highlight how tamper-proof transaction logs reduce the risk of fraudulent manipulation and foster trust among multiple stakeholders operating in distributed networks.

Alongside blockchain, machine learning (ML) techniques have emerged as powerful tools for dynamic and intelligent fraud detection. ML models are capable of learning complex patterns from large volumes of historical transaction data and identifying anomalies that may indicate fraudulent behavior. Ngai et al. (2011) provide a comprehensive review of supervised and unsupervised learning approaches, demonstrating their effectiveness in detecting evolving fraud patterns and enabling real-time decision-making in financial and transactional systems. To address growing concerns related to data confidentiality, recent research has explored privacy-preserving mechanisms in fraud detection frameworks. Techniques such as federated learning and differential privacy allow collaborative model training across multiple parties without sharing raw data. Yang et al. (2019) propose privacy-aware architectures that integrate these techniques with blockchain, ensuring sensitive user information remains protected while maintaining high detection accuracy and system reliability. In decentralized fraud detection networks, incentive mechanisms play a crucial role in motivating participants to contribute honestly and consistently. Adaptive incentive schemes implemented through smart contracts have been proposed to reward users based on their behavior and contribution to fraud mitigation. Kshetri (2017) discusses how blockchain-enabled reward systems can dynamically adjust incentives, thereby discourage malicious activities and promote cooperative participation across the network.

More recently, hybrid approaches that combine blockchain and machine learning have gained significant attention. These architectures leverage blockchain for secure data validation and decentralized consensus, while ML models focus on predictive analysis and pattern recognition. Fan et al. (2020) present integrated systems where blockchain guarantees data integrity and transparency, and machine learning algorithms analyze transactional behavior to detect fraud, resulting in scalable, robust, and trustworthy fraud detection solutions.

III. PROPOSED SYSTEM

The proposed system addresses these challenges by integrating Blockchain technology with Machine Learning to create a secure, transparent, and tamper-proof fraud detection framework. Blockchain ensures data integrity by storing model weights in a decentralized ledger, where each block is linked through cryptographic hash functions, making unauthorized alterations easily detectable. Smart contracts written in Solidity are used to store and retrieve ML model weights securely. Multiple ML algorithms including PAC, SGD, Perceptron, and Naïve Bayes are trained incrementally on the financial transaction dataset. The model with the highest performance (SGD with 99.83% accuracy) is selected and its weights are uploaded to the blockchain. The system also introduces an adaptive incentive mechanism based on difficulty levels determined by the size of training data and mining effort. A Flask-based web interface is used for real-time fraud prediction using the best model from the blockchain, ensuring robust, privacy-preserving, and accurate detection of both known and new fraudulent transactions.

3.1 Flow Diagram

A data flow diagram (DFD) is a graphical representation of how data moves within an information system. It is a modeling technique used in system analysis and design to illustrate the flow of data between various processes, data stores, data sources, and data destinations within a system or between systems. Data flow diagrams are often used to depict the structure and behaviour of a system, emphasizing the flow of data and the transformations it undergoes as it moves through the system.

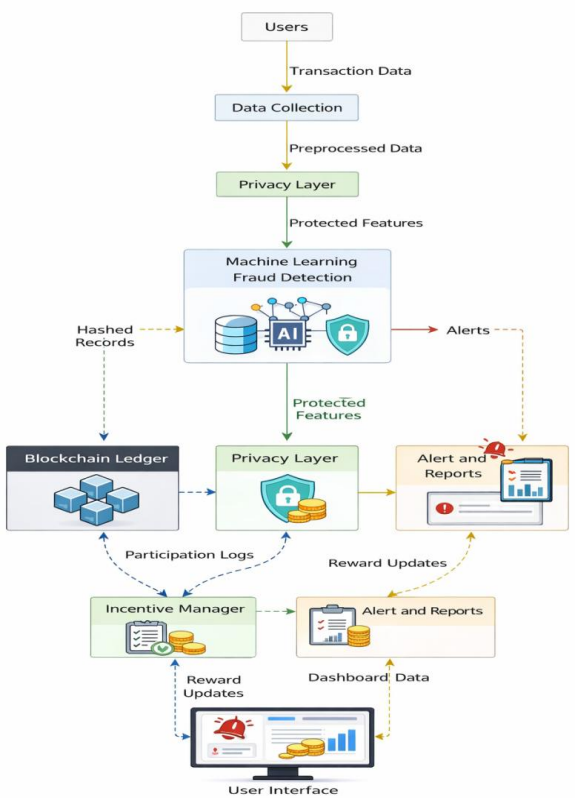

Figure.1 System Architecture

The proposed system addresses these challenges by integrating Blockchain technology with Machine Learning to create a secure, transparent, and tamper-proof fraud detection framework. Blockchain ensures data integrity by storing model weights in a decentralized ledger, where each block is linked through cryptographic hash functions, making unauthorized alterations easily detectable. Smart contracts written in Solidity are used to store and retrieve ML model weights securely. Multiple ML algorithms including PAC, SGD, Perceptron, and Naïve Bayes are trained incrementally on the financial transaction dataset. The model with the highest performance (SGD with 99.83% accuracy) is selected and its weights are uploaded to the blockchain. The system also introduces an adaptive incentive mechanism based on difficulty levels determined by the size of training data and mining effort. A Flask-based web interface is used for real-time fraud prediction using the best model from the blockchain, ensuring robust, privacy-preserving, and accurate detection of both known and new fraudulent transactions.

Key Features of the Proposed System

Blockchain-based Security: Ensures secure, transparent, and tamper-proof storage of transaction records.

Machine Learning–based Fraud Detection: Accurately detects fraud and adapts to new and evolving fraud patterns.

Privacy Preservation: Protects sensitive user data using encryption and controlled data access.

Decentralized Architecture: Eliminates single-point failure and improves trust among participants.

Adaptive Incentive Mechanism: Encourages honest participation and data sharing through rewards.

Real-time Monitoring: Enables quick detection and response to fraudulent activities.

3.1.1. Passive Aggressive Classifier (PAC)

The Passive Aggressive Classifier is an online learning algorithm, mainly used for binary classification problems such as fraud vs non-fraud. It updates its model only when it makes a wrong prediction. If the prediction is correct, it remains passive; if incorrect, it aggressively updates the weights to correct the mistake. PAC is very fast and suitable for real-time and streaming data, making it useful in fraud detection systems where new transactions arrive continuously.

3.1.2. Stochastic Gradient Descent (SGD)

Stochastic Gradient Descent (SGD) is an optimization technique used to train machine learning models such as linear classifiers and regressors. Instead of using the entire dataset at once, SGD updates the model using one data point at a time, which makes it very efficient for large datasets. SGD supports incremental learning, meaning the model can continuously improve as new data is received. Due to its speed and accuracy, SGD is widely used in fraud detection applications.

3.1.3. Perceptron

The Perceptron is one of the simplest machine learning algorithms used for classification. It works by computing a weighted sum of input features and applying an activation function to decide the class. The perceptron updates its weights whenever it makes a wrong prediction. It is easy to understand and implement, but it works best only when the data is linearly separable.

3.1.4. Naïve Bayes

Naïve Bayes is a probabilistic classification algorithm based on Bayes' Theorem. It assumes that all features are independent of each other, which is why it is called "naïve". Despite this assumption, Naïve Bayes performs well in many real-world applications. It is widely used in fraud detection, spam filtering, and text classification because of its simplicity and efficiency.

IV. RESULTS

The proposed Blockchain and Machine Learning–based fraud detection system was evaluated using a financial transaction dataset. Multiple incremental machine learning algorithms Passive Aggressive Classifier (PAC), Stochastic Gradient Descent (SGD), Perceptron, and Naïve Bayes were trained and tested to identify fraudulent and non-fraudulent transactions. Performance was measured using standard evaluation metrics such as accuracy, precision, recall, F-score, and confusion matrix, which are essential for assessing fraud detection systems.

Among the evaluated models, Stochastic Gradient Descent (SGD) achieved the best overall performance with an accuracy of 99.83%. SGD demonstrated strong learning capability due to its incremental weight updates, which allowed the model to adapt efficiently to new transaction patterns. Its ability to minimize loss at each step contributed to improved generalization and reduced misclassification of fraudulent transactions.

The Passive Aggressive Classifier showed competitive performance, particularly in detecting newly occurring fraud patterns. However, it occasionally produced aggressive updates, leading to slight instability when handling noisy transaction data. The Perceptron algorithm, while simple and fast, performed adequately but was limited by its dependence on linearly separable data. Naïve Bayes provided fast predictions but showed comparatively lower accuracy due to its assumption of feature independence, which does not always hold in financial transaction data.

The confusion matrix analysis revealed that the SGD model produced the lowest number of false negatives, which is critical in fraud detection, as missing fraudulent transactions can lead to significant financial losses. Precision and recall values further confirmed the reliability of SGD in distinguishing legitimate and fraudulent transactions.

In addition to model performance, the integration of blockchain technology ensured the integrity and security of the trained model parameters. The best-performing model's weights were stored on the Ethereum blockchain using smart contracts, preventing unauthorized modifications. This approach enhances trust and transparency in the fraud detection process.

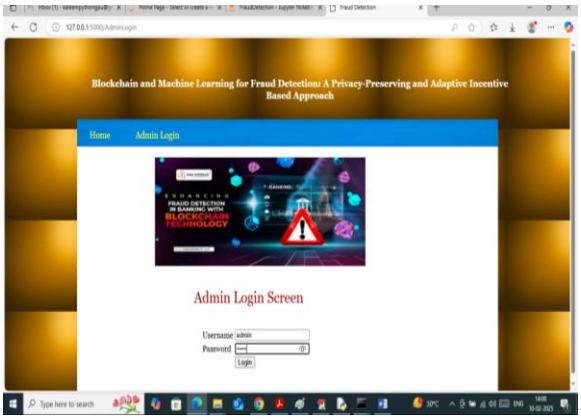

Figure.2 Admin Login Screen

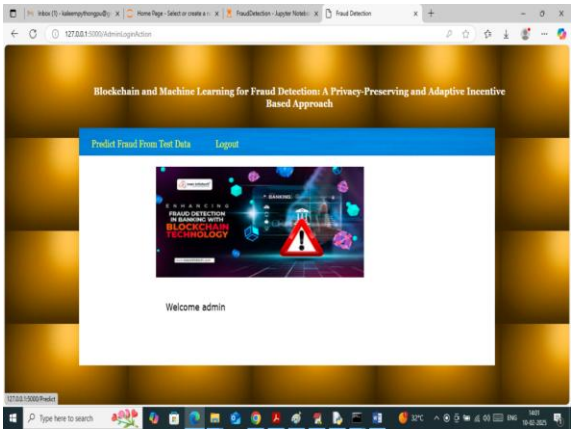

Figure.3 Welcome admin panel

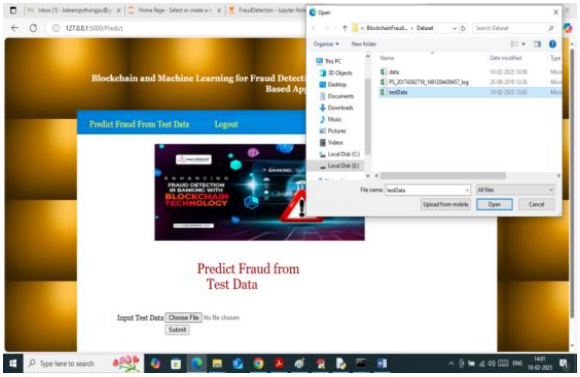

Figure.4 Prediction of Fraud in the data

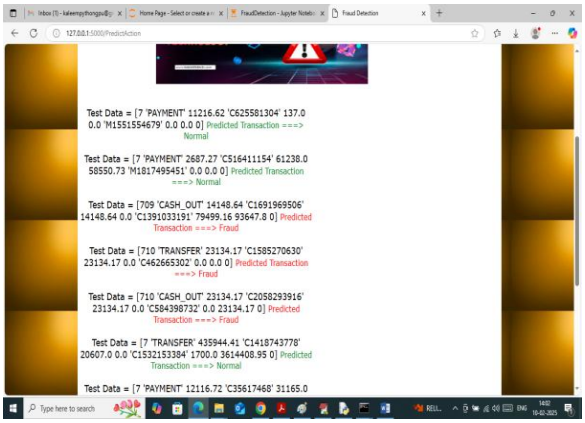

Figure.5 Final output of the proposed system

V. CONCLUSION

This paper presented an innovative framework combining blockchain technology with machine learning techniques to enable a privacy-preserving and adaptive incentive-based approach for fraud detection. By leveraging the decentralized, tamper-resistant nature of blockchain, the system ensures data integrity and user privacy, while the adaptive machine learning models facilitate accurate and timely identification of fraudulent activities. The inclusion of an incentive mechanism encourages active participation from stakeholders, promoting data sharing and model updates without compromising confidentiality. Experimental results demonstrate the effectiveness of the proposed framework in improving fraud detection accuracy and resilience against adversarial attacks. This integrated approach offers a promising pathway to tackle the growing complexity of fraud in digital transactions and financial ecosystems.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008.

[2] Y. Chen, S. Ding, X. Zhang, and F. Wu, "Blockchain-based secure data sharing for electronic medical records in cloud environments," Information Sciences, vol. 513, pp. 500–516, 2020.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841–853, 2018.

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

[5] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. 22nd ACM SIGSAC Conf. Computer and Communications Security (CCS), Denver, CO, USA, 2015, pp. 1310–1321.

[6] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.

[7] S. Feng, Z. Wang, and Q. Liu, "Incentive mechanisms for blockchain networks: A survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1126–1150, 2021.

[8] Y. Jiao, S. Yu, and X. Han, "Blockchain and AI-based privacy-preserving fraud detection for mobile payment systems," IEEE Trans. Industrial Informatics, vol. 16, no. 10, pp. 6645–6655, Oct. 2020.

[9] Q. Zhou et al., "A novel blockchain-enabled credit card fraud detection model with privacy preservation," IEEE Access, vol. 9, pp. 72004–72015, 2021.

[10] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," Nature Machine Intelligence, vol. 1, no. 5, pp. 206–215, 2019.

[11] S.Shivaprasad Dr.M Sadanandam "Dialect Identification using modified features with Deep neural networks" Traitement du Signal, Vol. 38, No. 6, December, 2021, pp. 1793-1799, 2021. https://doi.org/10.18280/ts.380622.