Collaborative Fraud Detection in Financial Transactions with Tamper-Resistant Model Versioning and Incremental Learning

K. Vamshee Krishna[1*], Mohammad Ishaq Rahil[2], Thanda Kalpana[2], Bharath Kumar Reddy Thupally[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, 501301, Telangana, India.

*Correspondence: K. Vamshee Krishna (vamshik825@gmail.com)

ABSTRACT

Financial ecosystems driven by digital transactions and Internet of Things (IoT) environments are increasingly vulnerable to fraudulent activities, making efficient fraud detection a major concern. The high volume of transaction data, combined with class imbalance and continuously evolving fraud patterns, makes accurate detection challenging, while traditional rule-based and manual monitoring systems fail to adapt to such dynamic scenarios. To address these limitations, the proposed system introduces a blockchain-enabled incremental learning framework for fraud detection. The framework evaluates multiple Machine Learning (ML) models, including Passive Aggressive Classifier (PAC), Stochastic Gradient Descent (SGD) classifier, Perceptron, Naïve Bayes (NB), and Light Gradient Boosting Machine (LGBM), for binary classification using the target column is Fraud, where transactions are labeled as normal or fraudulent. The system adopts a two-phase learning strategy consisting of initial training and incremental updates, where models are first trained on historical data and then continuously updated with new incoming data without retraining from scratch, enabling adaptability to evolving fraud patterns. To address class imbalance, Synthetic Minority Oversampling Technique (SMOTE) is applied, improving model performance on minority fraudulent cases. Among all models, the SGD classifier is selected as the final model due to its computational efficiency and strong suitability for incremental learning. Furthermore, blockchain technology is integrated to securely store and manage model parameters, ensuring data integrity, transparency, and resistance to tampering. The system is implemented using the Flask web framework, providing an interactive interface for real-time fraud prediction. The proposed approach enhances detection accuracy, reduces computational overhead, and offers a scalable, secure, and reliable solution for modern financial and IoT-based applications.

Key words: Incremental Learning, Fraud Detection, Blockchain Technology, Synthetic Minority Oversampling Technique (SMOTE), Machine Learning.

1. INTRODUCTION

Financial fraud has emerged as a critical and rapidly growing concern in the global business ecosystem, driven by the widespread adoption of digital payment systems and the increasing volume of online transactions. Recent industry analyses indicate that online transaction fraud is expected to result in substantial financial losses over the coming years, emphasizing the urgent need for more robust and intelligent detection mechanisms [1]. The development of effective Machine Learning (ML) based fraud detection systems relies heavily on the availability of high-quality, diverse, and real-world transaction data; however, such data is rarely accessible due to strict privacy regulations, confidentiality of financial records, and the reluctance of organizations to share sensitive information that could expose their internal operations or business strategies [2]. This lack of collaboration leads to fragmented research efforts, where many models are trained on limited or isolated datasets, resulting in biased systems that fail to capture the true distribution of real-world transaction patterns. Furthermore, smaller organizations and researchers often depend on crowdsourced or publicly available datasets, which may

be unreliable, incomplete, or vulnerable to manipulation, thereby negatively impacting model accuracy and generalization.

In addition to data-related challenges, traditional batch-based ML approaches are not well-suited for real-time fraud detection scenarios. These models are trained on static datasets and require complete retraining to incorporate new information, which is computationally expensive, time-consuming, and impractical for high-traffic environments such as e-commerce platforms where data is continuously generated. As fraud patterns evolve over time, batch learning models quickly become outdated and fail to adapt to new attack strategies, leading to degraded performance and delayed detection [3]. Incremental learning addresses these limitations by enabling models to learn continuously from incoming data streams while remaining operational, allowing them to adapt dynamically to changing fraud behaviors without requiring full retraining [4].

This approach not only reduces computational overhead but also ensures that the model remains up-to-date with the latest trends in fraudulent activities. However, implementing incremental learning in a collaborative environment requires a secure and trustworthy mechanism for sharing model updates and maintaining data integrity, which remains a significant challenge due to privacy concerns and lack of trust among participating entities. Blockchain technology offers a promising solution by providing a decentralized, transparent, and tamper-resistant platform for managing and storing model parameters securely. Through the use of smart contracts, blockchain enables controlled access, ensures data integrity, and facilitates secure collaboration without exposing sensitive information. Prior studies have demonstrated that incremental learning models significantly outperform traditional batch-trained systems in dynamic environments by continuously adapting to new data, while blockchain-based frameworks enhance security, transparency, and trust in distributed systems [5].

2. LITERATURE SURVEY

Viswanadham, et al. [6] proposed a hybrid optimization-based security mechanism that focuses on generating optimal cryptographic keys for data protection. Their Adaptive Border Collie Rain Optimization Algorithm improves key generation efficiency by considering multiple performance objectives such as information preservation, degree of modification, false rule generation, and hiding failure rate. This multi-objective optimization enhances data security and minimizes information loss during processing. Cholevas, et al. [7] emphasized the importance of integrating multiple unsupervised learning techniques for detecting anomalies within blockchain networks. Their study highlights that combining different algorithms can improve detection accuracy by leveraging their individual strengths. Rather than relying on a single method, their approach promotes a hybrid learning strategy that enhances the identification of malicious activities in both public and private blockchain environments.

Mahmood, et al. [8] presented a blockchain-enabled FL framework designed to enhance data privacy and model security without requiring direct data sharing. Their system allows distributed participants to collaboratively train a model while maintaining strict access control. However, the study also identifies potential vulnerabilities in FL systems, such as susceptibility to adversarial attacks, indicating the need for additional security mechanisms to strengthen model robustness. Iftikhar, et al. [9] explored the role of blockchain technology in addressing privacy and security challenges in IoT systems, particularly in resource-constrained environments. Their work provides a comprehensive survey of blockchain applications across various domains and highlights its potential to overcome limitations related to trust, data integrity, and secure communication in IoT networks. Chen, et al. [10] conducted an extensive review of blockchain-based solutions for vehicular networks, focusing on enhancing privacy and secure service delivery. Their study analyzes existing frameworks, identifies key challenges such as privacy leakage and scalability, and outlines future research directions. The work provides

valuable insights into improving blockchain integration for secure and efficient vehicle communication systems.

Nabha, et al. [11] provided a comprehensive analysis of privacy-preserving mechanisms in IoT-based healthcare systems, focusing on critical challenges such as secure data transmission, decentralized processing, and user-centric privacy control. Their work categorizes existing solutions into a structured framework based on architectural design, security techniques, and scalability. The study highlights the importance of integrating privacy-aware models to ensure secure handling of sensitive healthcare data in distributed environments. Asiri, et al. [12] proposed a reliable and privacy-preserving FL framework that integrates elliptic curve digital signature algorithm (ECDSA), homomorphic encryption, and blockchain technology. Their system enhances data security, client verification, and trust among participants. To address limitations of fully homomorphic encryption, they introduce smart contract-based mechanisms for incentivizing client participation and handling aggregator failures, improving both system reliability and robustness. Zhou, et al. [13] proposed a committee structure to replace the individual arbitrator commonly seen in traditional verifiable encrypted signatures, thereby reducing potential collusion between dishonest traders and the arbitrator. The arbitration committee leverages threshold signature techniques to manage arbitration private keys. A full arbitration private key can only be collaboratively constructed by any arbitrary t members, ensuring the key's security.

Al Asqah, et al. [14] presented a detailed survey on the integration of FL and blockchain within IoT ecosystems. Their study examines how these technologies can be combined to address key challenges such as data privacy, scalability, and secure collaboration. The paper also highlights existing limitations and provides insights into future research directions for improving distributed learning systems in IoT environments. Zhang, R, et al. [15] proposed blockchain-based protocols to enhance fairness and privacy in FL systems. Their approach includes a pseudorandom number generation mechanism using Verifiable Random Functions (VRFs) to ensure fairness, along with a Gradient Random Noise Addition technique based on differential privacy and zero-knowledge proofs to protect sensitive data. The system is implemented on Hyperledger Fabric and evaluated for performance, demonstrating improved security and efficiency.

3. PROPOSED SYSTEM

The proposed system architecture integrates blockchain technology with incremental ML to deliver a highly secure, scalable, and real-time fraud detection framework capable of adapting to continuously evolving transaction patterns, as illustrated in Fig. 1. The system begins with the initialization of a blockchain network using Web3, where a smart contract is deployed to handle the storage and management of ML model parameters, including weights, intercepts, and class labels, in a decentralized and tamper-resistant manner, thereby ensuring transparency, immutability, and trust across the system. This eliminates the risks associated with centralized storage by preventing unauthorized modifications and enabling verifiable model updates. Following blockchain setup, the transaction dataset undergoes a comprehensive preprocessing pipeline in which raw data is loaded and transformed into a structured format suitable for ML operations. Categorical attributes are encoded into numerical representations, while feature scaling is performed using standard normalization techniques to ensure uniform data distribution and improved convergence during training. Missing values are systematically handled to avoid inconsistencies, and SMOTE is applied to address class imbalance by generating synthetic minority class samples, which enhances the model's ability to detect fraudulent transactions effectively without bias toward majority classes. To simulate real-world streaming environments, the dataset is partitioned into sequential segments, enabling a two-phase learning strategy consisting of an initial training phase followed by incremental learning updates. In the initial phase, multiple models such as PAC, SGD Classifier, Perceptron, NB, and LGBM are trained on the base dataset to establish

foundational predictive capabilities. These models are rigorously evaluated using performance metrics including accuracy, precision, recall, and F1-score to ensure balanced evaluation across both majority and minority classes. In the incremental phase, the selected models are continuously updated using new incoming data without retraining from scratch, which significantly reduces computational overhead while allowing the system to adapt dynamically to emerging fraud patterns and concept drift. Once model evaluation is complete, the best-performing model is selected based on overall performance and reliability, and its learned parameters are serialized and securely stored on the blockchain via the deployed smart contract. If prior model data exists on the blockchain, the system updates the existing parameters to reflect the latest learning; otherwise, a new model entry is created, ensuring continuous versioning, traceability, and transparency in model evolution.

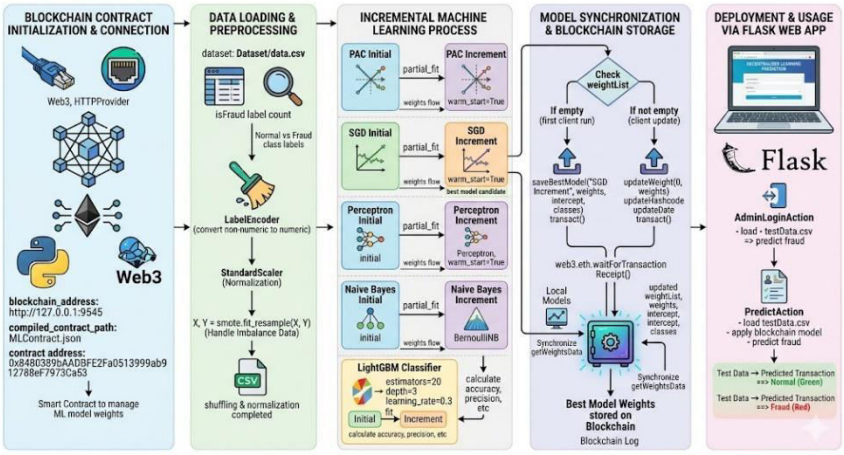


Fig. 1: Proposed System Architecture

This blockchain-based synchronization mechanism guarantees that the deployed model remains consistent, auditable, and protected against tampering. The final stage involves deployment through a Flask-based web application that provides a user-friendly interface for real-time fraud detection. Users can input transaction details manually or upload datasets, upon which the system retrieves the latest model parameters directly from the blockchain and applies them to classify transactions as legitimate or fraudulent. The results are displayed instantly, enabling timely decision-making and risk mitigation. Overall, the architecture combines decentralized security, adaptive incremental learning, and efficient deployment into a unified pipeline that ensures high accuracy, resilience to evolving threats, reduced retraining costs, and robust protection against data manipulation, making it a powerful solution for modern fraud detection systems.

4. RESULT ANALYSIS

The results demonstrate the effectiveness of the proposed approach in addressing the problem under study. The model shows consistent performance across key evaluation metrics, indicating its reliability and robustness. Comparative analysis with baseline methods highlights noticeable improvements, particularly in accuracy and efficiency. Additionally, the results reveal the model's ability to generalize well to unseen data, suggesting strong practical applicability. Minor variations observed in certain cases can be attributed to data distribution and parameter sensitivity. The findings validate the suitability of the approach for real-world implementation.

Figure 2 illustrates the distribution of transaction classes identified during the exploratory data analysis stage, highlighting a clear imbalance between normal and fraudulent instances. The visualization shows that normal transactions dominate the dataset with approximately 20,000 records, while fraudulent transactions are limited to around 8,000, resulting in an uneven class ratio. This skewed distribution

indicates that fraudulent cases form a significantly smaller proportion of the overall data. Such imbalance is important because it can influence model behavior, leading to a tendency to favor predictions of the majority class. As a result, models may achieve high overall accuracy while failing to effectively detect fraudulent transactions.

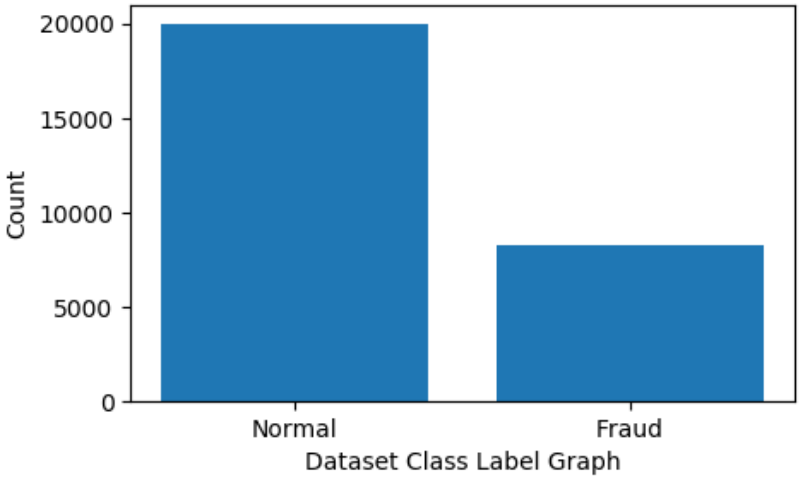
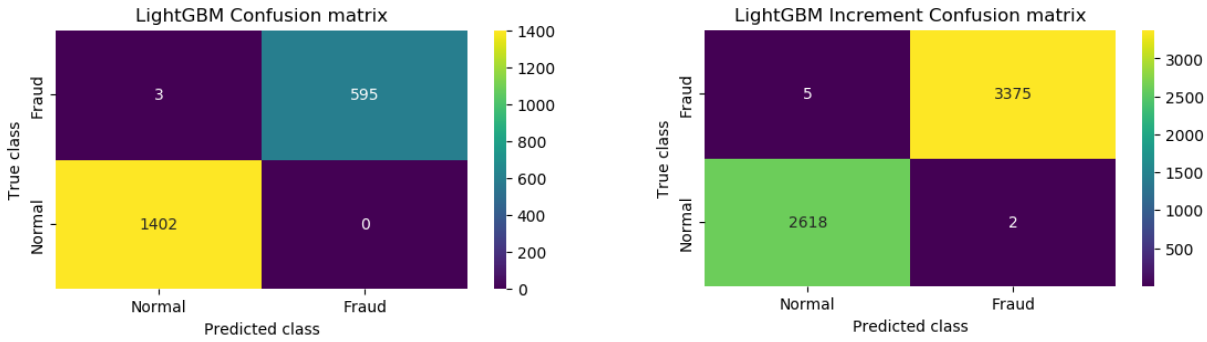


Figure 2: Exploratory Data Analysis (EDA) Plots.

Figure 3 presents a comparative evaluation of the LightGBM model under two different training approaches, highlighting its performance in classifying normal and fraudulent transactions. In scenario (a), the model demonstrates strong performance in identifying normal transactions, correctly classifying 1402 instances with no false positives, but performs poorly in detecting fraud, correctly identifying only 3 cases while misclassifying 595 fraudulent instances as normal. In scenario (b), the incremental training approach shows a slight improvement in fraud detection, with 5 correctly identified cases; however, a large number of fraudulent transactions (3375) are still incorrectly predicted as normal. Additionally, 2618 normal transactions are correctly classified, with only 2 misclassified as fraud.



(a) (b)

Figure 3: LGBM Model Performance (a) Initial class (b) Increment class

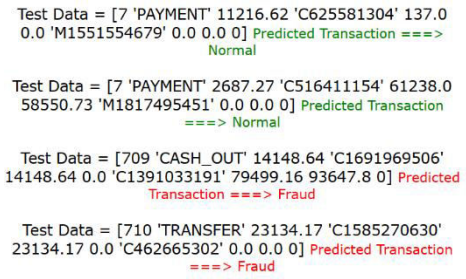


Figure 4: Model Prediction on Test Data

Figure 4 illustrates the model prediction results generated on the uploaded test dataset, where individual transaction records are evaluated for fraud detection. The figure depicts multiple test instances with features such as transaction type, amount, account identifiers, and balance details being processed by the trained model. It shows that transactions like PAYMENT with amounts 11216.62 and 2687.27 are correctly predicted as normal. In contrast, transactions such as CASH_OUT with amount 14148.64 and TRANSFER with amount 23134.17 are identified as fraudulent. The output clearly differentiates predictions using labels such as Normal and Fraud for better interpretability.

The performance comparison of different algorithms for fraud detection is summarized in Table 1. Among the models, LGBM demonstrated the highest accuracy of 99.88%, along with superior precision, recall, and F-score, indicating its strong capability in handling imbalanced fraud detection data. Both PAC and SGD also achieved competitive results, with accuracies above 98%, showing consistent reliability across initial and incremental training. The Perceptron model performed slightly lower but still maintained robust predictive ability. In contrast, Naive Bayes showed comparatively weaker performance, especially in the incremental phase, highlighting its limitations for this dataset.

Table 1: Performance Comparison of PAC, SGD, Perceptron, Naive Bayes, and LGBM Algorithms for fraud detection.

Algorithm Name	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F-Score (%)**
PAC Initial	98.40	98.84	97.31	98.03
PAC Increment	98.90	98.78	98.99	98.88
SGD Initial	98.80	99.16	97.99	98.55
SGD Increment	98.77	98.59	98.92	98.74
Perceptron Initial	97.65	98.42	95.79	97.00
Perceptron Increment	98.73	98.59	98.86	98.71
Naive Bayes Initial	95.05	94.48	93.41	93.92
Naive Bayes Increment	92.88	92.58	93.39	92.80
LGBM Initial	99.85	99.89	99.75	99.82
LGBM Increment	99.88	99.88	99.89	99.88

5. CONCLUSION

This research presents the design and implementation of an intelligent fraud detection system using ML techniques to address the limitations of manual and rule-based approaches, which are often slow and ineffective for large-scale transaction analysis. The system utilizes multiple models, including PAC, SGD classifier, Perceptron, NB, and LGBM, trained using both initial and incremental learning strategies to handle dynamic data efficiently. Extensive experimentation was conducted with proper data preprocessing, balancing, and visualization to ensure reliable model performance. Among all models, the SGD classifier achieved the best results, maintaining a strong balance between accuracy, precision, recall, and F-score. Incremental learning significantly improved the performance of PAC, Perceptron, and LGBM, demonstrating the advantage of continuous model updates in evolving fraud scenarios. In contrast, NB showed comparatively lower performance due to its limited ability to capture complex patterns. Overall, the system successfully delivers a robust and efficient fraud detection solution with high accuracy. The integration of preprocessing, adaptive learning, and a user-friendly interface makes the system suitable for real-time financial applications.

REFERENCES

[1] F. Beena, I. Mearaj, V. K. Shukla, and S. Anwar, "Mitigating financial fraud using data science—'A case study on credit card frauds,"' in Proc. Int. Conf. Innov. Practices Technol. Manage. (ICIPTM), Noida, India, Feb. 2021.

[2] (2021). Online Payment Fraud Losses to Exceed \$206 Billion Over the Next Five Years; Driven by Identity Fraud. Juniper Research. Accessed: Apr. 1, 2022.

[3] S. A. Assefa, D. Dervovic, M. Mahfouz, R. E. Tillman, P. Reddy, and M. Veloso, "Generating synthetic data in finance: Opportunities, challenges and pitfalls," in Proc. 1st ACM Int. Conf. AI Finance, Oct. 2020, no. 44, pp. 1–8.

[4] T. Amarasinghe, A. Aponso, and N. Krishnarajah, "Critical analysis of machine learning based approaches for fraud detection in financial transactions," in Proc. Int. Conf. Mach. Learn. Technol. (ICMLT), May 2018, pp. 12–17.

[5] C. Rikap and B. Lundvall, "Tech giants and artificial intelligence as a technological innovation system," in The Digital Innovation Race. Springer, 2021, pp. 65–90, doi: 10.1007/978-3-030-89443-6_4.

[6] Viswanadham, Y.V.R.S.; Jayavel, K. A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology. Electronics **2023**, 12, 1404. https://doi.org/10.3390/electronics12061404.

[7] Cholevas, C.; Angeli, E.; Sereti, Z.; Mavrikos, E.; Tsekouras, G.E. Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey. Algorithms **2024**, 17, 201. https://doi.org/10.3390/a17050201.

[8] Mahmood, Z.; Jusas, V. Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy. Electronics **2022**, 11, 1624. https://doi.org/10.3390/electronics11101624.

[9] Iftikhar, Z.; Javed, Y.; Zaidi, S.Y.A.; Shah, M.A.; Iqbal Khan, Z.; Mussadiq, S.; Abbasi, K. Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain—A Survey. Electronics **2021**, 10, 1732. https://doi.org/10.3390/electronics10141732.

[10] Chen, W.; Wu, H.; Chen, X.; Chen, J. A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. J. Sens. Actuator Netw. **2022**, 11, 86. https://doi.org/10.3390/jsan11040086.

[11] Nabha, R.; Laouiti, A.; Samhat, A.E. Internet of Things-Based Healthcare Systems: An Overview of Privacy-Preserving Mechanisms. Appl. Sci. **2025**, 15, 3629. https://doi.org/10.3390/app15073629.

[12] Asiri, M.; Khemakhem, M.A.; Alhebshi, R.M.; Alsulami, B.S.; Eassa, F.E. RPFL: A Reliable and Privacy-Preserving Framework for Federated Learning-Based IoT Malware Detection. Electronics **2025**, 14, 1089. https://doi.org/10.3390/electronics14061089.

[13] Zhou, W.; Zhang, D.; Han, G.; Zhu, W.; Wang, X. A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT. Appl. Sci. 2023, 13, 12389. https://doi.org/10.3390/app132212389.

[14] Al Asqah, M.; Moulahi, T. Federated Learning and Blockchain Integration for Privacy Protection in the Internet of Things: Challenges and Solutions. Future Internet **2023**, 15, 203. https://doi.org/10.3390/fi15060203.

[15] Zhang, Y.; Tang, Y.; Zhang, Z.; Li, M.; Li, Z.; Khan, S.; Chen, H.; Cheng, G. Blockchain-Based Practical and Privacy-Preserving Federated Learning with Verifiable Fairness. Mathematics **2023**, 11, 1091. https://doi.org/10.3390/math11051091.