

# Fraud Detection Using Blockchain and Machine Learning

Rasala Sushmitha<sup>1</sup>, Shaik Hasina<sup>2</sup>, S. Uday Kumar<sup>3</sup> and Mondeddu Sairam<sup>4</sup>

<sup>[1-4]</sup>IV Year Student, Dept. of IT, Malla Reddy Engineering College Secunderabad, Telangana, India.

Corresponding Author: [hodaiml439@gmail.com](mailto:hodaiml439@gmail.com)

## Abstract

Financial fraud cases are on the rise even with the current technological advancements. Due to the lack of inter-organization synergy and because of privacy concerns, authentic financial transaction data is rarely available. On the other hand, data-driven technologies like machine learning need authentic data to perform precisely in real-world systems. This study proposes a blockchain and smart contract-based approach to achieve robust Machine Learning (ML) algorithm for e-commerce fraud detection by facilitating inter-organizational collaboration. The proposed method uses blockchain to secure the privacy of the data. Smart contract deployed inside the network fully automates the system. An ML model is incrementally upgraded from collaborative data provided by the organizations connected to the blockchain. To incentivize the organizations, we have introduced an incentive mechanism that is adaptive to the difficulty level in updating a model. The organizations receive incentives based on the difficulty faced in updating the ML model. A mining criterion has been proposed to mine the block efficiently. And finally, the blockchain network is tested under different difficulty levels and under different volumes of data to test its efficiency. The model achieved 98.93% testing accuracy and 98.22% Fbeta score (recall-biased f measure) over eight incremental updates. Our experiment shows that both data volume and difficulty level of blockchain impacts the mining time. For difficulty level less than five, mining time and difficulty level has a positive correlation. For difficulty level two and three, less than a second is required to mine a block in our system. Difficulty level five poses much more difficulties to mine the blocks.

**Keywords:** *Blockchain, collaborative machine learning, incremental learning, privacy, smart contract.*

## I. INTRODUCTION

Fraud has become one of the most persistent and costly challenges in today's digitally connected world. As industries such as finance, healthcare, e-commerce, and telecommunications increasingly rely on online platforms and automated transactions, the opportunities for malicious actors have expanded significantly. The sheer scale and speed of digital interactions generate massive volumes of data, making manual monitoring impractical and traditional rule-based fraud detection systems insufficient. Consequently, organizations face growing financial losses, operational disruptions, and declining user trust due to increasingly sophisticated fraud schemes.

Machine learning (ML) has emerged as a powerful tool for modern fraud detection because of its ability to analyze large datasets and uncover hidden patterns indicative of anomalous behavior. Advanced ML techniques—including supervised learning, unsupervised anomaly detection, and deep learning—enable systems to learn from historical data and adapt to evolving fraud strategies. These models can significantly improve detection accuracy and reduce false positives compared to static methods. However, ML-based systems often depend on centralized data collection and processing, which raises serious concerns regarding data privacy, security, and regulatory compliance.

This makes it particularly attractive for applications requiring auditability and integrity. Despite these advantages, blockchain platforms are not

inherently designed for real-time predictive analytics or complex pattern recognition, limiting their standalone effectiveness in proactive fraud detection. The complementary strengths and weaknesses of machine learning and blockchain suggest the need for an integrated approach. Therefore, this work proposes a framework that synergistically integrates blockchain and machine learning for robust fraud detection. The proposed approach aims to enhance detection accuracy, ensure data confidentiality through hybrid on-chain/off-chain architectures, and promote trustworthy participation using smart contract-driven incentives. Furthermore, it emphasizes explainability and robustness to ensure long-term reliability.

## II. LITERATURE REVIEW

Online payment fraud is a rapidly growing threat, and recent analysis from Juniper Research highlights just how serious it has become. A major factor driving this surge is identity fraud, where criminals use stolen or synthetic personal information to carry out unauthorized transactions [1]. As digital services become more integrated into everyday life, attackers have more opportunities to exploit vulnerabilities in payment systems, mobile apps, and online platforms. The report emphasizes the need for stronger fraud-prevention technologies, such as advanced authentication and AI-driven detection tools, to help organizations reduce risk and protect users in the evolving digital landscape.

The work by M. T. Ribeiro, S. Singh, and C. Guestrin introduced the concept of interpretable machine learning through their well-known LIME (Local Interpretable Model-agnostic Explanations) framework. Their research addresses a critical limitation of many modern ML systems—the lack of transparency in model decision-making. The authors argue that for high-stakes domains such as fraud detection, healthcare, and finance, users must be able to understand why a model produced a particular prediction. The case study highlights the growing role of data-driven approaches in strengthening financial security and reducing economic losses in digital payment ecosystems [2].

The study by L. Ouyang, Y. Yuan, Y. Cao, and F.-Y. Wang (2021) proposes an innovative blockchain-based collaborative early warning framework designed to enhance information sharing and trust during the COVID-19 pandemic. By decentralizing the warning system, the framework promotes collaborative decision-making without compromising data integrity [3]. The work by C. Yang (2022) introduces an incremental outlier feature clustering algorithm tailored for blockchain networks operating in big data environments. The proposed algorithm focuses on extracting discriminative features from high-dimensional data and grouping similar behavioral patterns while isolating outliers that may indicate fraudulent or malicious activity [4]. The work by S. Aggarwal and N. Kumar (2021) provides a comprehensive overview of Blockchain 2.0 with a particular focus on smart contracts and their transformative potential in decentralized systems. The paper highlights how this paradigm shift allows blockchain platforms to support complex business logic and decentralized applications [5].

### III. METHODOLOGY

The system architecture is comprised of three layers, the application layer, the off-chain machine learning layer and the blockchain layer. The application layer is the user interface where participants (contributor, user) can register, use the machine learning model and contribute with their organization’s transaction data to improve the ML model. A decentralized application connects the actor to our blockchain network in the application layer. The selected ML model (Passive aggressive classifier) is deployed in the blockchain at the inception of the network (the genesis block of a blockchain)

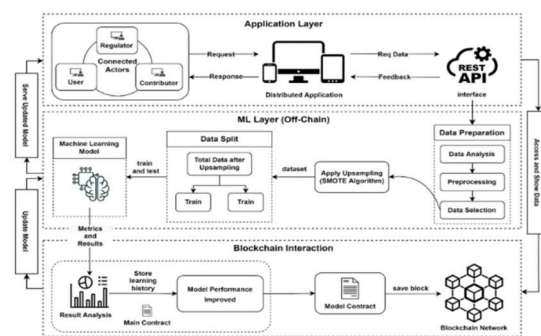


Fig 1: System Architecture

The methodology follows a modular and layered architecture, ensuring scalability, resilience, and adaptability under communication-constrained and hostile conditions. Each module contributes to transforming raw battlefield data into actionable and interpretable logistics decisions.

#### A. Network Participation and Query Access

When a contributor or user node joins the network, the participant is allowed to access the deployed machine learning (ML) model to perform inference queries regardless of its role within the ecosystem. This open query access ensures usability and broad adoption of the fraud detection service. However, only registered contributor nodes are authorized to submit datasets for incremental learning and model improvement. This design maintains controlled model evolution while preserving open inference capabilities for all connected stakeholders.

#### B. Data Submission and API Interface

Once a contributor uploads a new dataset instance, the request is routed through the distributed application interface (API). The API acts as a secure gateway between the application layer and the ML processing layer. Upon receiving the dataset, the interface forwards the data to the ML layer for preprocessing and incremental training. This modular separation ensures scalability, maintainability, and secure handling of organizational data contributions.

#### C. Machine Learning Layer and Data Preparation

The ML layer encapsulates all machine learning operations, beginning with data validation and ending with partial model training. Incoming datasets first pass through a data preparation filter that checks for structural and semantic consistency, including dataset shape verification, required feature presence, null-value detection, and schema compatibility. Since contributed datasets are expected to exhibit class imbalance similar to the original training data, the Synthetic Minority Oversampling Technique (SMOTE) is applied to balance the class distribution. The balanced dataset is then partitioned into training and testing subsets. The training portion is used to partially update a copy of the current

best model, while the test set evaluates post-training performance.

#### D. Smart Contract–Based Model Evaluation

The ML layer sends performance metrics to the main smart contract for validation. The contract compares the new metrics with the current best using the predefined mining criteria (Algorithm 1). If the model shows improvement—especially reduced false negatives while maintaining acceptable precision, recall, and  $F\beta$ —the decision is forwarded to the model contract for execution.

#### E. Optimization and Adaptive Decision-Making

If the smart contract detects performance improvement, a new block is created containing model metrics, model hash, previous hash, nonce, block index. The block is broadcast and appended to the blockchain after consensus. The improved model replaces the previous version, while its cryptographic hash is stored on-chain for integrity and traceability; the model itself remains off-chain for efficiency.

#### F. Incentive Distribution Mechanism

Upon successful model improvement, the smart contract calculates the contributor’s reward using the predefined incentive function and automatically transfers it to the contributor’s blockchain address. This approach promotes high-quality data sharing and discourages low-value contributions.

#### G. Blockchain Logging and Live Monitoring

All model updates and performance metrics are immutably recorded on the blockchain. The updated model becomes immediately available for inference, and the application dashboard provides real-time visibility into blockchain status, model updates, transactions, and contribution statistics, ensuring transparency and auditability.

### IV. RESULTS AND DISCUSSIONS

The results evaluate the performance of the proposed blockchain-enabled fraud detection framework from machine learning, smart contract, and blockchain perspectives. The experiments validate system functionality, incremental model improvement, and mining efficiency under varying conditions. Model updates were triggered only when the new model reduced the false-negative rate while keeping precision, recall, and  $F\beta$  within acceptable limits. Out of 40 dataset contributions, only 8 met the improvement criteria and produced blockchain updates. Each successful update created a new block with model metrics and automatically distributed incentives via smart contracts.

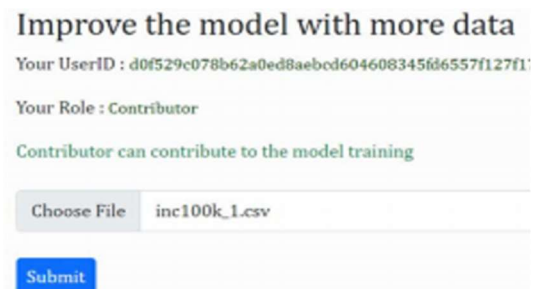


Fig 2: Data training

The comparison also highlights the trade-off between false positives and false negatives, which is critical in fraud detection systems. Since undetected fraud leads to direct financial loss, higher recall and F1-score are prioritized while maintaining acceptable precision. Based on this analysis, the most suitable model was selected for deployment in the blockchain-integrated framework, ensuring strong detection capability and stable performance during incremental learning.

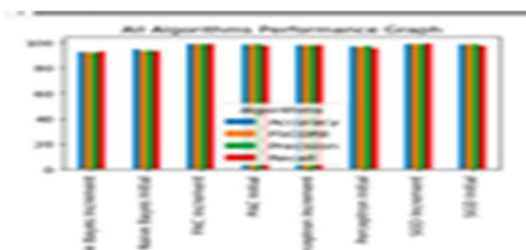


Figure 3: Performance Analysis

Figure 3 presents a comparative evaluation of multiple machine learning algorithms for fraud detection using key metrics such as accuracy, precision, recall, and F1-score. These metrics together provide a holistic view of model performance: accuracy reflects overall correctness, precision indicates the reliability of fraud alerts, recall measures the ability to detect actual fraudulent transactions, and the F1-score balances precision and recall. The visualization enables clear identification of how each algorithm performs across different evaluation dimensions.

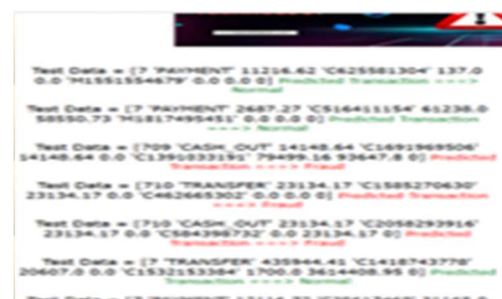


Figure 4: Fraud Prediction Output

The experimental results confirm that the proposed framework successfully integrates blockchain security, smart contract automation, and incremental machine learning. The system effectively filters low-quality

contributions, rewards meaningful improvements, reduces fraud detection errors, and maintains transparent, tamper-resistant model evolution.

Thus, the proposed privacy-preserving and adaptive incentive-based framework demonstrates practical feasibility, scalability, and robustness for decentralized collaborative fraud detection environments.

## V. CONCLUSION

This study proposes an approach where e-commerce organizations can work collaboratively to build robust machine learning algorithms incrementally while safekeeping business strategies and mitigating privacy concerns. To bring robustness to current solutions, authentic data from the real marketplace is required. This study takes advantage of state-of-the-art blockchain technology to build a platform for training fraud detection ML algorithms incrementally and collaboratively while protecting the privacy of contributing organizations. Smart contract has been used in this study to automate the process throughout the system with absolute sturdiness. The result shows that for difficulty levels 2 and 3, and with a varying amount of data, the mining time is below a second. For difficulty level 3, a maximum of 3 seconds can be taken to mine a block. And for difficulty 5, a much harder problem needs to be solved, and hence, the maximum mining time is approximately 70 seconds. Our approach is generic to be applied in sectors where data privacy and security are essential, but collaboration among organizations can bring about much better performance and accuracy. For future studies, we intend to build class-adaptive solutions under a stream of data.

## REFERENCES

- [1]. *Online Payment Fraud Losses to Exceed \$206 Billion Over the Next Five Years; Driven by Identity Fraud*. Juniper Research. Accessed: Apr. 1, 2022. [Online]. Available: <https://www.juniperresearch.com/press/online-payment-fraud-losses-exceed-206-bn>
- [2]. M. T. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you? Explaining the 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.
- [3]. L. Ouyang, Y. Yuan, Y. Cao, and F.-Y. Wang, "A novel framework of collaborative early warning for COVID-19 based on blockchain and smart contracts," *Inf. Sci.*, vol. 570, pp. 124–143, Sep. 2021.
- [4]. C. Yang, "Incremental outlier feature clustering algorithm in blockchain networks based on big data analysis," *IETE J. Res.*, pp. 1–9, Apr. 2022.
- [5]. S. Aggarwal and N. Kumar, "Blockchain 2.0: Smart contracts," *Adv. Comput.*, vol. 121, pp. 301–322, Sep. 2021.
- [6]. L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu, "Blockchain enabled fraud discovery through abnormal smart contract detection on Ethereum," *Future Gener. Comput. Syst.*, vol. 128, pp. 158–166, Mar. 2022.