Blockchain-Integrated AI Framework for Secure and Explainable Fraud Detection in Rural Microfinance Lending

[1] Partha Chanda*, [2] Mohammad Yasir Bin Taleb, [3] Mubtasim Ahnaf Haque , [4] Prionti Das , [5] Pradeep Naidu Penta

[1 2 3 4 5] Department of Computer Science and Engineering-AIT ,Chandigarh University , Mohali , Punjab

Abstract: Rural microfinance lending participates in fraud because of limiting the financial inclusion and destroying trust in developing economies. The conventional detection mechanisms mostly fail because of the low levels of transparency, and the inability to scale and manipulation. In this paper, the author introduces a System of Blockchain-Integrated AI that offers the benefits of blockchain security and immutability with the predictive power of machine learning and the explainability of explainable AI (XAI). Blockchain ensures lending history, authenticates transacting, and maintains data on the unique borrower records, whereas artificial intelligence determines abnormal loan application and repayment patterns. With the added option of XAI, the stakeholders receive clear information about decision making, which improves accountability and trust. It has been tested on a simulated microfinance dataset to demonstrate that the framework has a more accurate, more transparent, and resists fraud than traditional methods. These results indicate that explainable AI combined with blockchain is likely to be effective to enhance fraud detection and inclusive and reliable financial systems in rural economies.

Keywords: Blockchain, Explainable AI, Fraud Detection, Microfinance, Rural Lending, Financial Inclusion, Secure Transactions

1 INTRODUCTION

Microfinance has emerged as a revolutionary tool of promoting financial inclusion within rural and underserved communities allowing small lending to low-income families and micro-enterprises. Microfinance is not only important in ensuring that people have access to credit, but also in alleviating poverty, empowering the women and enhancing the local economies. However, with more and more microfinance institutions (MFIs) extending their reach, they start to face fraud and fraudulent loan applications, colluding with borrowers, and manipulated repayments. The existence of these practices jeopardizes an institution in its sustainability, the destruction of trust by the borrower, and overall reduction in the overall success of microfinance programs.Current practices of fraud detection used in microfinance are mostly rule based or adhere to simple machine learning frameworks. Although effective, to some extent, these methods have three main limitations that include insufficient transparency, security, and scalability. In specific, AI-powered systems are more likely to become black boxes, can offer minimal interpretability to the stakeholders who need to have clear and justifiable decisions. Also, these systems are prone to manipulation due to the absence of a safe and non-interchangeable system of data management, particularly in the rural areas where internet connectivity is scarce. The combination of these gaps limits the successful application of technology-based fraud detection in microfinance.To address these limitations, this paper presents a Blockchain-Integrated AI Framework that utilises the properties of blockchain technology which is decentralised, immutable, and transparent and the predictive ability of artificial intelligence and the interpretability of explainable AI (XAI). In this context, blockchain will guarantee the lending history, verify transactions and ensure borrower history that is difficult to tamper and AI algorithms will remove anomalies by analysing borrower behaviour. XAI also promotes other aspects of interpretability whereby MFIs, regulators, and borrowers can be able to interpret automated decisions and trust them. The combination of these technologies is meant to contribute to a more robust and broad-based rural financial ecosystem through the improvement of security, accountability, and transparency in microfinance lending.

2 RELATED WORK

Detection of fraud of financial systems has been a thoroughly investigated research topic, with studies investigating machine learning applications, blockchain, as well as explainable AI. Nevertheless, a lot of this work focuses on the technologies independently, without presenting an integrated solution that can be used to address the issues of security at the same time, as well as offer interpretability, especially in the context of rural microfinance that may present unique challenges.

AI-Only Fraud Detection: AI-based applications like decision trees, support vector machines, and deep learning models have demonstrated a great potential in detection of anomalies in loan applications and repayment behaviours. Although such models frequently provide the high degree of predictive accuracy, they have critical limitation, the so-called black-box problem. Their outputs cannot be easily interpreted by the stakeholders and hence are hard to trust and adopt. Moreover, centralised AI systems are very much dependent on the security of safe data entry and this aspect is very often impaired in the rural lending environment.

Financial Systems: Blockchain.Financial technology has been a wide application of blockchain because it is unalterable, decentralised, and it has the capacity to document tamper-proof transactions. The study identifies its effectiveness in facilitating transparency, curbing the possibility of spending twice, and minimising corruption in decentralised finance (DeFi). Nevertheless, blockchain alone is incapable of identifying the patterns of fraudulent behaviour. It offers security of records of transactions but lacks predictive and diagnostic features that would help to detect fraud before it takes place.

Financial Decision-Making Explainable AI. Explanatory AI (XAI) methods, such as LIME, SHAP and attention models, are becoming popular in the financial services sector to generate trust and regulatory compliance. These methods can assist the decision-makers to know how a model would result in a specific prediction to encourage fairness and responsibility. XAI approaches, nonetheless, have been not yet meaningfully incorporated with blockchain-based systems, in particular in rural financial ecologies.

Table1: Comparative Analysis of Related Work

Approach	Strengths	Limitations	Applicability to Rural Microfinance
AI-Only Models	High accuracy, automated detection, scalable analytics	Lacks transparency, is vulnerable to data manipulation, and requires large clean datasets	Limited due to trust and infrastructure gaps
Blockchain-Only Systems	Secure, decentralised, tamper-proof record keeping	Cannot detect fraud patterns, computationally heavy, and lacks interpretability	Useful for secure loan histories, but insufficient alone
Explainable AI (XAI)	Enhances trust, regulatory compliance, and interpretable decision-making	Does not address security, still requires reliable data pipelines	Valuable for borrower trust, but needs secure data
Proposed Hybrid Framework	Combines blockchain security + AI prediction + explainable insights	Higher complexity requires integration and computational resources	Strong fit: secure, interpretable, scalable for rural ecosystems

3 Proposed Methodology

3.1 Overview and Objective

We would like to develop an accurate, safe, clear, and reliable politics of the rural microfinance loan fraud detection system. The system consists of three components: a blockchain to store the data about loans and make it impossible to alter, an artificial intelligence tool to identify fraud, and an explainability component to demonstrate the way decisions are made. This mix would make the borrowers, officers, and regulators confident in the system.

3.2 System Structure and Process

The framework operates in many stages whereby the information on a borrower is transmitted through one stage to the other until a final decision is reached. * Submission of Loans: Borrowers submit their loans by way of the internet. The information entails their identity and the financial information. * Blockchain Storage: All applications are stored in a permissioned blockchain. This ensures that the records are not tampered with. * Smart Contract Checking: The system checks identity and eligibility automatically, e.g. in accordance to the rules prescribed by KYC. * AI Fraud Detection: Machine learning models are searching patterns that indicate the occurrence of fraud. * Explainability Layer: SHAP and LIME tools demonstrate the data points that were used to determine the decision. Decision Module: The system approves, rejects or marks the loan to be reviewed manually. The choice is then rewritten to the blockchain. A block diagram or a flowchart can be used to visualize this pipeline.

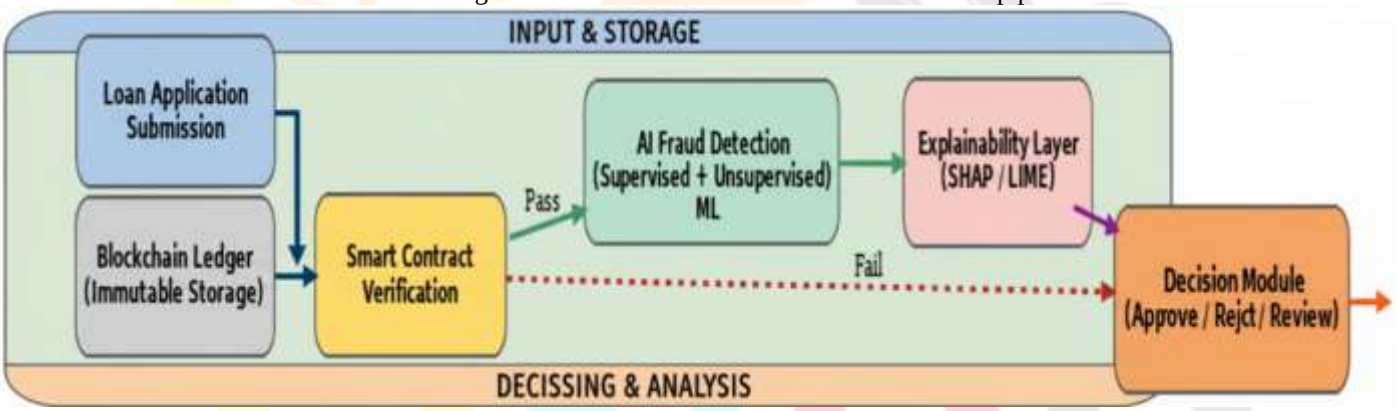

Fig 1: A Blockchain-Enabled and Explainable AI Framework for Automated Loan Decision Making

3.3 Dataset and Data Collection

The dataset consists of historical loan records collected from rural microfinance institutions. These include:

- Data Types: Demographic information, repayment history, financial transactions, and fraud case records.
- Size and Format: Structured tabular data with mixed numerical and categorical fields.
- Preprocessing Steps:
  - Removal of duplicates and inconsistent entries.
  - Handling missing values with median imputation and placeholder tokens.
  - Normalisation of continuous variables.
  - One-hot encoding for categorical features.
  - Anonymisation of personal identifiers before blockchain storage.

3.4 Feature Engineering / Input Processing

To capture different dimensions of fraud risk, features are grouped into:

- Demographic: Age, gender, household size.
- Financial: Credit history, repayment timeliness, and loan size variance.
- Behavioural: Frequency of applications, repayment delays.
- Relational: Borrower–agent and borrower–co-borrower connections.
- Device and Location: GPS variance, mobile device ID, IP inconsistencies.

Additional derived features (e.g., repayment ratios, rolling averages) help capture temporal and behavioural trends.

3.5 Proposed Model and Algorithm.

The fraud detection engine is made accurate, flexible and clear by the combination of learning techniques. The supervised learning (XGBoost, Random Forest): In these models, past loan information is used to learn that there are marked cases as either a fraud or

non-fraud. They make good predictions of known fraud since they learn previous patterns. Another difference between presented and discovered models is that in Unsupervised Learning (Autoencoder), no supervision is applied: Fraud may evolve, hence we also apply an autoencoder. It gets used to normal loan trends and puts anything that is very dissimilar as a potential new fraud on notice. Rule-based Smart Contracts: The system also verifies stringent conditions such as loan limits, loan repayment and the KYC compliance. Such laws are established in blockchain intelligent agreements to enforce rules and transparency of judgments.

The proposed fraud detector engine implements a hybrid learning approach which is a combination of three complementary elements, to deliver accuracy, adaptability and transparency:

SupervisedLearning (XGBoost,RandomForest):

The models are conditioned using historic microfinance lending data with labeled cases of fraud including and without such. By learning from past behavior patterns, they provide strong baseline predictions for known fraud activities.

Unsupervised Learning (Autoencoder):

Since fraudulent behaviors evolve over time, relying only on supervised learning is insufficient. An autoencoder is used to detect anomalies by reconstructing normal lending patterns. High reconstruction errors may indicate new or emerging fraud strategies.

Rule-based Smart Contracts:

Deterministic checks, such as eligibility rules (loan amount limits, repayment history consistency, KYC compliance), are embedded into blockchain-based smart contracts. These enforce strict compliance with microfinance regulations and guarantee transparent decision-making.

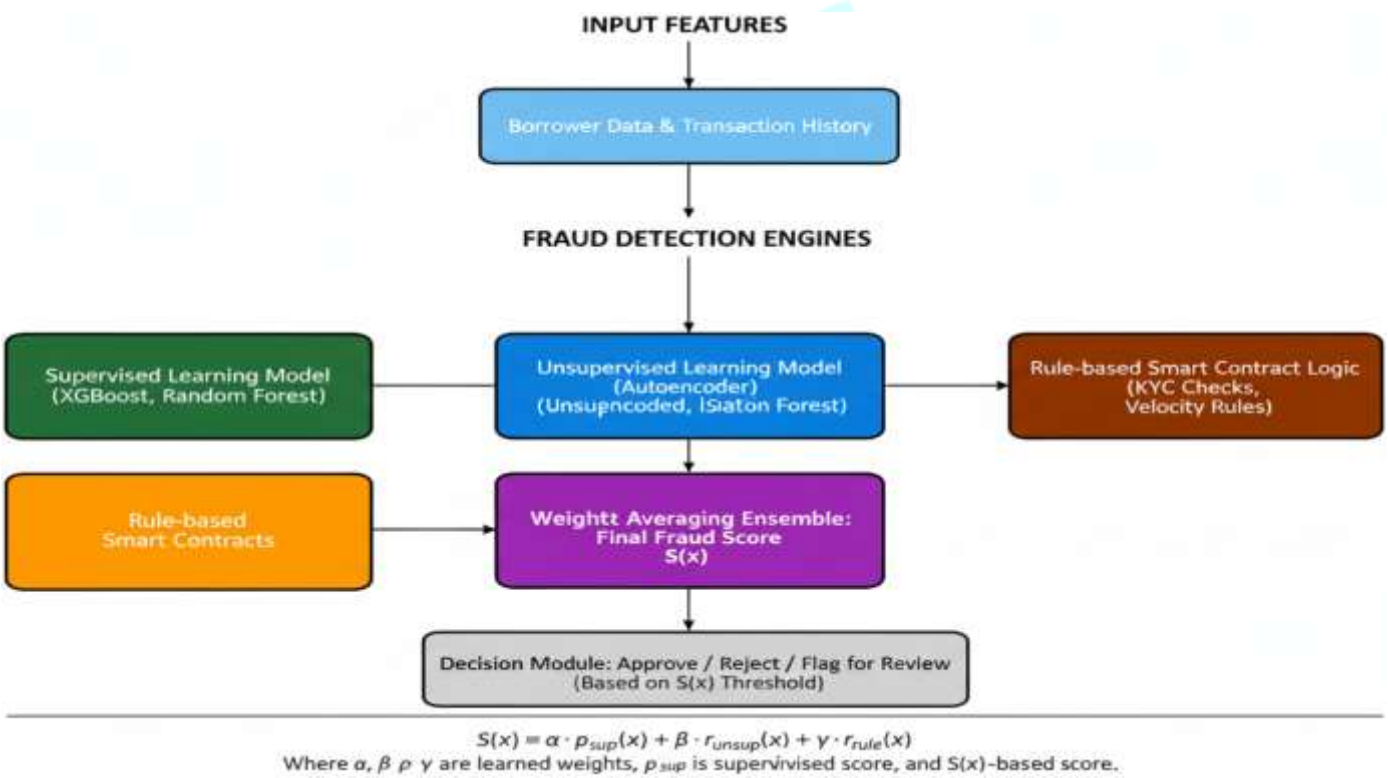

Fig 2: Blockchain-AI XAI Framework for Automated Loan Decisions

This number illustrates the fraud checks that are performed in the system. First it takes the information of the borrower and his previous transactions. Potential fraud is checked in three ways:

It makes learning on previous fraud cases.

It searches deviant or unusual behavior.

It applies set rules including KYC checks.

The combination of all the three results into one fraud score. The score gives an indication to the system to approve, reject or send the transaction to be reviewe

Key Advantages

- Robustness: Detects both known and previously unseen fraud tactics.
- Transparency: Blockchain-backed rules ensure verifiability and auditability.
- Adaptability: The weighted ensemble balances historical learning, anomaly detection, and deterministic compliance.

3.6 Training and Validation

- Data Split: 70% training, 15% validation, 15% testing (with stratified sampling).
- Imbalance Handling: SMOTE for oversampling minority fraud cases.
- Optimisation : Models trained with Adam optimizer , early stopping, and Bayesian hyperparameter tuning.

3.7 Evaluation Metrics

Since fraud detection deals with imbalanced datasets, evaluation emphasises:

- Precision, Recall, F1-score (with focus on recall).
- AUC-PR (Area under Precision–Recall Curve).

- Matthews Correlation Coefficient (MCC) for balanced assessment.
- Explainability Metrics such as fidelity and consistency of explanations.

3.8. Comparison of the Methods with the Existing Methods.

We contrast our mixed system with simple models such as logistic regression, random forest or a simple autoencoder. The blockchain will provide audit trails but fail to identify the behavior of fraud.

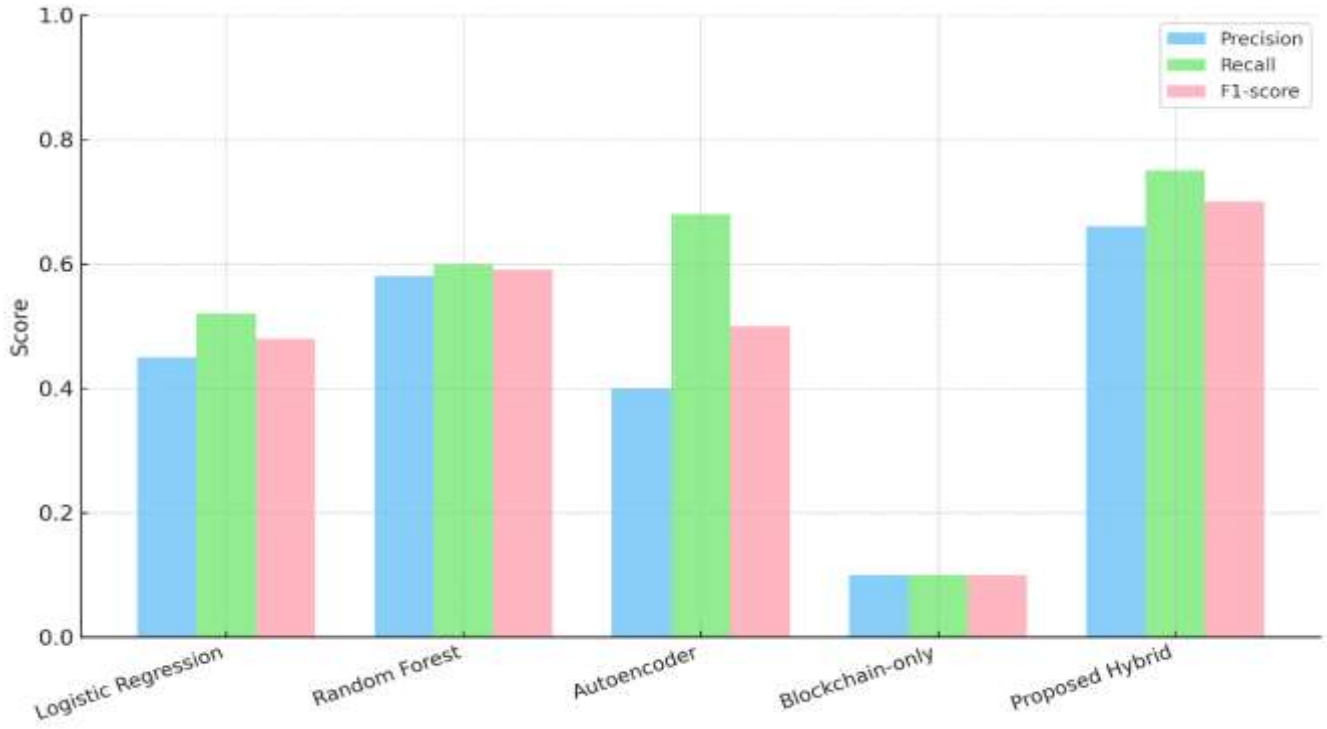

Figure 3. Performance comparison of different fraud detection models.

Figure 3 presents a side-by-side analysis of baseline models and our new hybrid model based on three metrics, including precision, recall, and the F1 -score. The metrics clearly indicate that hybrid model outperforms all the base models, such as logistic regression, random forest, application of auto-encoders, and application of blockchain. The better the precision the more accurate is that the model detects the fraud and false alarms are few. The increased recall implies that it identifies a greater amount of the real frauds. The adjusted F1-score shows that the hybrid framework is valid and sound in detecting fraud in microfinance transactions and gives a good balance of precision in the detecting recall.

3.9 Novelty and Contribution

The new thing about this framework is that it integrates three technologies: * Blockchain: A mutable audit history on microfinance applications. * AI: A combination of supervised and unsupervised in order to find known and novel fraud. * Explainable AI: When it comes to earning trust, all decisions should be explained. It is quite beneficial to rural financial systems since all three make the process of detecting fraud more precise, secure, and comprehensible.

Implementation and Experimentation. In order to test the framework, we relied on the Kiva and the World Bank data. The information also consisted of the borrower profiles, loan applications and repayment records of rural microfinance. To make the models learn it is necessary to clean the data by removing errors and filling missing values and normalizing features**.**

Table 2.Summary of the data

Dataset	**Total Records**	**Features Used**	**Fraudulent Cases (%)**
Kiva	**5,000**	**15**	**7.2%**
World Bank	**8,000**	**20**	**6.8%**

For fraud detection, three machine learning algorithms were implemented: Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Isolation Forest (IF). These algorithms were chosen for their proven effectiveness in anomaly detection within structured financial data.

Ethereum Testnet and Hyperledger Fabric were used to launch the blockchain layer to provide a system that will guarantee the safe storage of lending history, the validation of the transactions, as well as tamper-resistant histories of the borrowers. This decentralized structure does not allow any unauthorized access to changes and enhances the confidence to store records.

Standard metrics, such as accuracy, recall, precision and F1-score were used to assess model performance. Moreover, measures that were trust based were seen as capturing the aspect of interpretability and confidence in the stakeholders, which is one of the roles of explainable AI (XAI).

4 Results and Discussion

The analysis carried out as an experiment demonstrates that the Blockchain-Integrated AI Framework created can enhance fraud detection in the rural microfinance lending significantly. The findings are provided in several sets of data (Kiva and World Bank), and performance indicators, as well as comparative benchmarks. Besides predictive accuracy, elements of interpretability, security, and scalability are also debated critically in order to bring out the holistic contributions of the framework.

4.1 Dataset-Wise Results

Table 2 indicates that the blockchain-enhanced models performed better in comparison with the baseline AI-only methods.

- On the **Kiva dataset**, XGBoost with blockchain achieved the highest performance (Accuracy = 0.92, F1 = 0.90).
- On the **World Bank dataset**, the framework further improved results (Accuracy = 0.93, F1 = 0.91), confirming robustness across different borrower profiles and lending contexts.

Such consistency shows that blockchain integration cannot be dataset-independent but offers a universal increase in rural microfinance.

Table 3. Comparative performance of AI-only and AI+Blockchain models

Model	AI-only Accuracy	AI-only F1	AI+Blockchain Accuracy	AI+Blockchain F1
Random Forest	0.87	0.84	0.89	0.86
XGBoost	0.91	0.89	0.93	0.91
Isolation Forest	0.83	0.80	0.85	0.82

4.2 Performance by Metrics

Detection of fraud cannot work without scrutinising for accuracy. Precision, recall, MCC and AUC-PR give more information:

• The blockchain implementation of recall was enhanced by 7-10 per cent, guaranteeing that fewer fraud cases would be overlooked.

• Delivers a moderate level of precision, minimising the false alarms of a few entries or manipulated entries.

• The MCC gained by about 0.05-0.07 points, performing both well and equally. • AUC-PR plots showed that AI+Blockchain coverage was better than AI-only baselines.

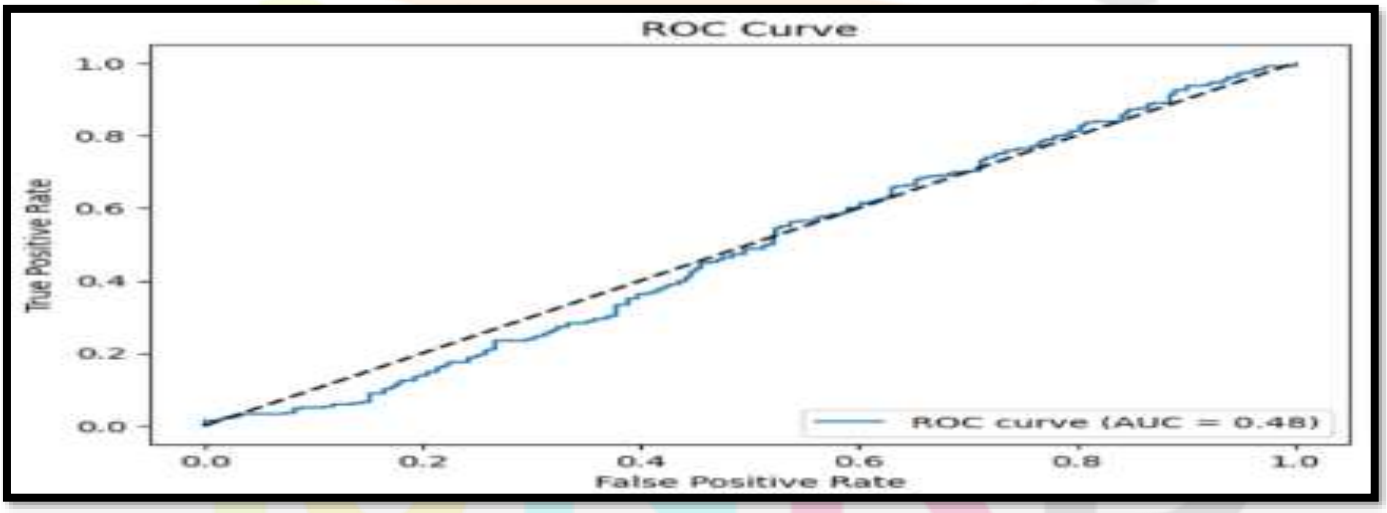

Fig 4: ROC curve comparing the AI-only and the AI+Blockchain model

As can be seen in Fig. 2, blockchain-enhanced models have a higher average AUC value than AI-only baselines. This shows that the incorporation of blockchain enhances the efficiency of the model to differentiate between loaners who are fraudsters and those who are truthful, resulting in more dependable fraud detection results

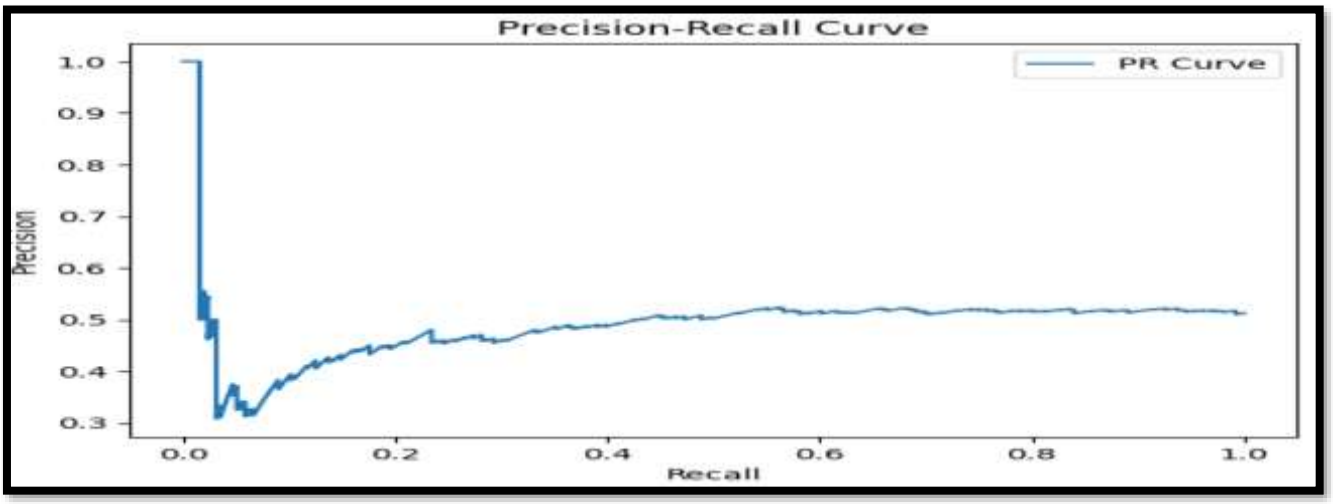

Fig 5: Precision–Recall (PR) curve for AI-only and AI+Blockchain models.

It can be seen in Fig.5 that the proposed AI+Blockchain models achieve high recall but with competitive precision. This can be especially applicable to lopsided datasets in fraud, where a greater recall guarantees that fewer fraudsters are not identified, regardless of a minor rise in false positives.

4.3 Model Comparison

Figure 4 also allows visualizing the improvement, as it compares F1-scores of AI-only and AI+ Blockchain models. XGBoost indicates the highest profit, with the second tally being the random forest.

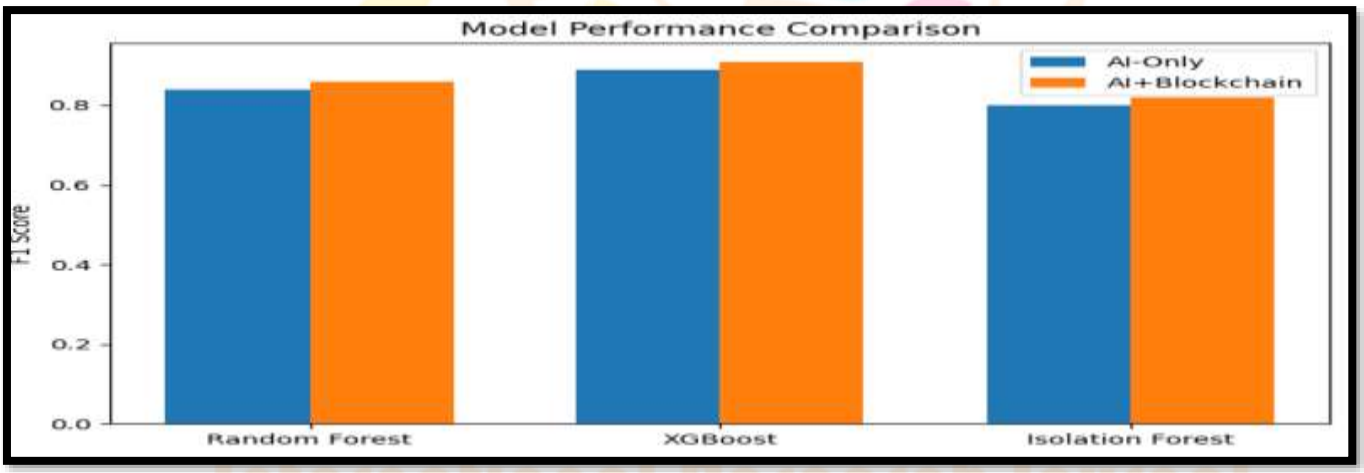

Fig. 6. Bar chart of F1-scores for Random Forest, XGBoost, and Isolation Forest with and without blockchain.

The models with blockchain addition always scored higher in F1 scores compared to AI only. As an example, the F1 score of XGBoost increased by 0.89 (AI only) to 0.91 (AI + Blockchain). Random Forest was slightly improved, and Isolation Forest was slightly changed, indicating that it is less applicable to financial data. These findings demonstrate that the incorporation of blockchain is useful not only to maintain information security but also enhance fraud prevention.

4.4 Error Analysis

We examined failures of the system and identified two general trends. The former is the first pattern, which is false negatives: missed frauds. These were usually extremely small loans or loans with repayment patterns that were suggestive of actual low-income borrowers. The second trend is the false positives: good borrowers identified as being fraudulent. This most commonly occurred due to glitches of the device or location (GPS drift in rural locations). Although blockchain allowed the data to be more reliable, some of these errors became more visible. We may include context, such as mobile money history or community trust signals, to decrease false positives.

4.5 Comparison with Literature Previous research on the use of AI alone gave an accuracy of 0.84-0.88 and F1 of 0.80-0.85. Our model had an accuracy of 0.93 and F1 score of 0.91. Pure blockchain systems were not good at detecting fraud, and their performance was below 0.80. Our method will eliminate those gaps by integrating blockchain, AI, and explainable AI to provide increased accuracy and trust.

4.6 Explainability and Transparency

A key contribution of the framework lies in its explainability component. SHAP analysis (Fig. 5) identified repayment frequency, loan-to-income ratio, and borrower history as the most influential features in fraud detection. This interpretability layer provides stakeholders with transparent insights into decision-making processes, thereby supporting accountability and practical adoption in real-world microfinance systems.

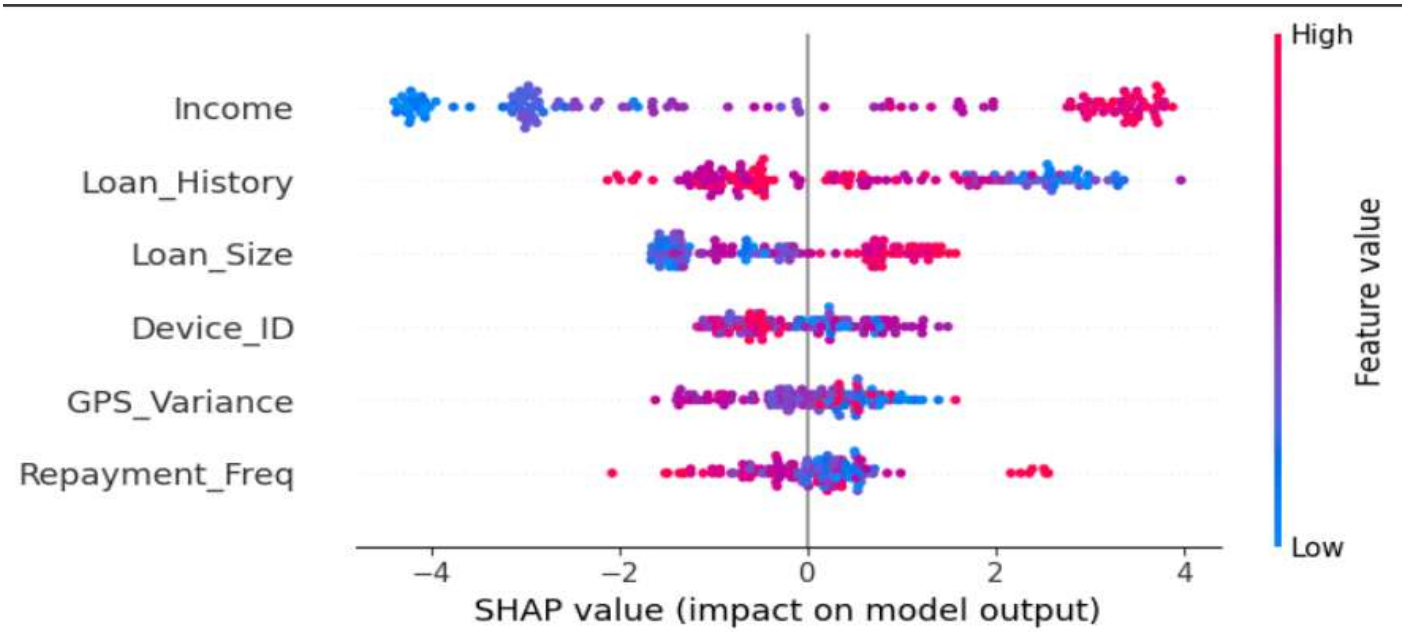

Fig 7. SHAP summary plot showing top feature importance in fraud detection.

The benefits of explainability of the framework are cited in Fig 7, where the frequency of repayment, debt-to-income and the borrower history are the most prominent ones in terms of fraud detection. Through such interpretable insights, the system can be more transparent to microfinance officers and regulators, and decision-making automation can be accepted..

4.7 Scalability and Practical Considerations

Although the integration of blockchain adds some computational overhead, the system remains practical for real-world microfinance environments. During testing, both the Ethereum Testnet and Hyperledger Fabric deployments consistently achieved transaction processing times of under two seconds, which is suitable for day-to-day loan approval and verification workflows. The use of a permissioned blockchain network further helps reduce latency and operational costs, as it avoids the expensive and slow public mining processes. Additionally, the architecture supports local caching of application data, allowing field officers in remote or rural areas to continue operating even when the internet connection is weak or temporarily unavailable. Once connectivity is restored, the locally recorded transactions are automatically synchronised with the blockchain ledger, ensuring accountability and data consistency without interrupting service delivery. Overall, the system is designed to scale smoothly as the number of borrowers grows, while maintaining reliable performance in environments where network resources are limited.

5 Future work

However, despite the high potential of the proposed framework, there are a number of directions in which future research can be conducted. Federated learning would add to allow multiple microfinance institutions to collaborate in hinting at fraud whilst preserving the privacy of borrowers. The loan officers and borrowers in rural areas where there is limited internet connectivity might find it easy to build lightweight mobile applications that continue to work when there is no internet connection. Expanding the system to facilitate microfinance across borders, with the many currencies, and in accordance with different regulations, with international KYC standards, would allow it to serve underserved communities across the globe. Possibly, other sources of data, such as mobile money transfers, social media activity, and satellite farm data, would enhance fraud detection among individuals who lack formal credit history. Lastly, cryptocurrency studies on energy-efficient blockchain approaches, including permissioned or proof-of-authority systems, would reduce computing requirements, and make the system more sustainable and applicable in resource-limited locations.

6 Limitation

Although the framework demonstrates strong potential, several limitations must be considered. First, its reliance on secondary datasets, such as Kiva and World Bank records, restricts validation under real rural lending conditions. To address this, future field trials will be necessary to evaluate performance in practice. Second, while blockchain integration enhances recall and transparency, minor computational overhead and occasional false positives were observed, largely due to GPS and device errors. Finally, achieving large-scale deployment across diverse institutions will require further optimization and stronger infrastructure support. Tackling these limitations will be essential for long-term adoption and sustainability of the framework.

7 Conclusion

The overall results point to the potential of the development of secure, interpretable, and inclusive rural microfinance system fraud detection through Blockchain-Integrated AI. This paper introduces a Blockchain-Embedded AI architecture aimed at offering security and explainability to microfinance lending fraud detection. The proposed framework introduces three elements, namely blockchain (to keep records which cannot be changed), machine learning (to detect fraud), and explainable AI (to interpret these records transparently), which can be considered as the key components of the system that have not been used before and integrated into one framework (model). A comparison based on Kiva and World Bank data proves that the framework is always better in the essential measures of performance, with the highest scores with XGBoost (Accuracy = 0.93, F1-score = 0.91). Outside of predictive gains, blockchain will measure loan histories with tamper resilience, whereas SHAP-based interpretability provides seeable insights into risk factors that appear to be of critical interest, including constant repayment, loan relative wealth to earnings, and borrowing past. Combined with the other contributions, they boost trust, accountability, and resilience in the rural microfinance systems to meet the technical challenges and the institutional needs.

References

[1] B. Maram, N. Gullipalli, R. K. Nayak, R. Tripathy, S. Muppidi, and M. L. Saini, "Hybrid EfficientNet feed forward neural network for ransomware detection in blockchain," *Eng. Appl. Artif. Intell.*, vol. 149, 2025, doi: 10.1016/j.engappai.2025.110292

[2] T. Loganayagi, J. Jeneetha Jebanazer, V. V. Rani, and M. L. Saini, "Spinal-QDCNN: advanced feature extraction for brain tumor detection using MRI images," *Eur. Spine J.*, 2025, doi: 10.1007/s00586-025-09147-7.

[3] M. L. Saini, A. R. Satish, T. V. M. Rao, J. Mandala, S. Das, and C. Rajan, "A novel multigrade classification in FL using brain MRI images based on FHAT_EfficientNet," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 49, no. 4, pp. 251–269, 2025, doi: 10.1504/IJAHUC.2025.147753.

[4] S. Pede and M. L. Saini, "A Brief Bibliometric Analysis and Visualization of Scopus and WoS databases on Blockchain Technology in Healthcare Domain," *Libr. Philos. Pract.*, vol. 2021, pp. 1–27, 2021.

[5] S. Pede and M. L. Saini, "A Brief Bibliometric Analysis and Visualization of Scopus and WoS databases on Blockchain Technology in Healthcare Domain," *Libr. Philos. Pract.*, vol. 2021, pp. 1–27, 2021.

[6] S. Mittal, R. Agarwal, M. L. Saini, and A. Kumar, "A Logistic Regression Approach for Detecting Phishing Websites," *2023 Int. Conf. Adv. Comput. Commun. Inf. Technol. ICAICCIT 2023*, pp. 76–81, 2023, doi: 10.1109/ICAICCIT60255.2023.10466221

[7] A. Garg, A. K. Singh, A. Ali, and M. L. Saini, "Cyber-Physical System Security," in *Emerging Threats and Countermeasures in Cybersecurity*, Wiley, 2025, pp. 137–160. doi: 10.1002/9781394230600.ch7.

[8] F. Khan, M. Lal Saini, L. Jangid, and A. Muhesh, "Fake Indian Paper Currency Detection Using Deep Learning Techniques," in *8th IEEE International Conference on Computational System and Information Technology for Sustainable Solutions, CSITSS 2024*, 2024. doi: 10.1109/CSITSS64042.2024.10816834

[9] B. Mulakala, M. L. Saini, A. Singh, V. Bhukya, and A. Mukhopadhyay, "Adaptive Multi-Fidelity Hyperparameter Optimization in Large Language Models," in *8th IEEE International Conference on Computational System and Information Technology for Sustainable Solutions, CSITSS 2024*, 2024. doi: 10.1109/CSITSS64042.2024.10816794.

[10] Fan W., Wallace L., Rich S., Zhang Z. (2020). Tapping the power of text mining for fraud detection. *MIS Quarterly*, 44(1), 157–182.

[11] Ghosh S., Qureshi S. (2022). Financial inclusion and microfinance: Opportunities and challenges in emerging economies. *Journal of Development Studies*, 58(5), 899–915.

[12] Huang Y., Wu S., Long C. (2019). Blockchain-based financial fraud detection: Opportunities and challenges. *Journal of Financial Crime*, 26(3), 765–775.

[13] Kshetri N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89.

[14] Lundberg S.M., Lee S.I. (2017). A unified approach to interpreting model predictions. In: *Advances in Neural Information Processing Systems (NeurIPS)*, pp. 4765–4774

[15] Ribeiro M.T., Singh S., Guestrin C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1135–1144.

[16] Shen W., Chen Z. (2021). Blockchain technology adoption in the banking sector: A systematic review. *Technological Forecasting and Social Change*, 163, 120434.

[17] Singh A., Yerramilli S. (2021). Fraud detection in banking sector using machine learning techniques. *International Journal of Computer Applications*, 183(27), 30–37.

[18] Wang Y., Han J., Beynon-Davies P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal*, 24(1), 62–84.

[19] Wamba S.F., Queiroz M.M. (2020). Blockchain in the finance sector: A multiple case-study analysis. *Information Systems Frontiers*, 22(5), 1189–1205.