Secure Financial Transactions through Machine Learning Based Anomaly Detection and End to End Data Encryption

Dhavjal Sanja

Indian college of commerce, Kolkata, India

Abstract: The rapid expansion of digital financial services has introduced unprecedented transaction speed and accessibility, but it has also significantly increased exposure to cyber threats, fraud schemes, and data breaches. Traditional security mechanisms based solely on encryption or rule-based fraud detection are insufficient against evolving adversarial techniques. This paper proposes an integrated framework combining machine learning–based anomaly detection with end-to-end data encryption to secure financial transactions. The framework ensures transactional confidentiality through strong cryptographic protocols while leveraging adaptive anomaly detection algorithms to identify fraudulent behaviors in real time. Experimental evaluation demonstrates that the proposed hybrid architecture enhances fraud detection accuracy, reduces false positives, and maintains minimal latency overhead. The results confirm that combining intelligent anomaly detection with robust encryption mechanisms provides a scalable and secure solution for modern FinTech ecosystems.

Keywords: Explainable AI, Fraud Prevention, FinTech Security, Data Governance

1. Introduction

Digital banking, online payments, peer-to-peer transfers, and embedded finance platforms have transformed global financial systems. However, this digital transformation has led to increasing risks including:

- Payment fraud
- Account takeover attacks
- Man-in-the-middle (MITM) attacks
- Data interception
- Synthetic identity fraud

While end-to-end encryption (E2EE) protects data confidentiality during transmission, it does not inherently detect malicious behavioral patterns. Conversely, machine learning–based fraud detection systems can identify suspicious activity but may expose sensitive financial data during processing.

This paper presents a dual-layered security architecture integrating:

1. End-to-end encryption for data protection
2. Machine learning–based anomaly detection for proactive fraud mitigation

The objective is to ensure transaction integrity, confidentiality, and intelligent threat detection within a unified framework.

2. Background and Related Work

2.1 Financial Transaction Security

Financial transaction systems rely on cryptographic mechanisms such as:

- Advanced Encryption Standard (AES)
- RSA-based public key cryptography
- Elliptic Curve Cryptography (ECC)
- Transport Layer Security (TLS)

Although these protocols secure communication channels, they do not detect behavioral fraud patterns.

2.2 Machine Learning in Fraud Detection

Anomaly detection models identify deviations from normal transactional behavior. Common approaches include:

- Isolation Forest
- One-Class Support Vector Machine (OC-SVM)
- Autoencoders

- Deep Neural Networks
- Gradient Boosting Machines

Machine learning enables detection of zero-day fraud strategies that static rule systems fail to capture.

2.3 Research Gap

Existing systems often treat encryption and fraud detection as independent modules. Few architectures integrate secure encrypted pipelines with intelligent anomaly detection while preserving computational efficiency.

3. Proposed Secure Transaction Framework

3.1 Architecture Overview

The proposed framework consists of four layers:

1. **Client-Side Encryption Layer**
2. **Secure Transmission Channel**
3. **Anomaly Detection Engine**
4. **Risk Scoring and Decision Module**

3.2 End-to-End Encryption Mechanism

Each transaction undergoes encryption at the source using:

- AES-256 symmetric encryption for transaction payload
- RSA/ECC for secure key exchange
- TLS 1.3 for transport-level protection

Encryption ensures that transaction details remain confidential during transmission and storage.

3.3 Machine Learning–Based Anomaly Detection

The anomaly detection module processes transaction metadata and behavioral features such as:

- Transaction frequency
- Geolocation variance
- Device fingerprint mismatch
- Transaction amount deviation
- Historical spending patterns

Models evaluated include:

- Isolation Forest (unsupervised anomaly detection)
- LSTM networks (sequential behavioral modeling)
- Autoencoders (reconstruction error analysis)

The system computes a **risk score** for each transaction. Transactions exceeding a predefined threshold trigger secondary authentication or blocking mechanisms.

4. Dataset and Experimental Design

4.1 Dataset Characteristics

A financial transaction dataset containing 2.5 million records was used. Features included:

- Transaction amount
- Timestamp
- Merchant ID
- Device ID
- IP address hash
- Fraud label

Fraud prevalence: 2.1%

4.2 Preprocessing

- Feature normalization

- Log transformation for skewed distributions
- Handling class imbalance using SMOTE
- Secure encryption applied after preprocessing

4.3 Evaluation Metrics

Performance evaluated using:

- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC
- Latency impact

5. Results

5.1 Detection Performance

Model	Precision	Recall	F1-Score	ROC-AUC
Isolation Forest	0.78	0.81	0.79	0.86
Autoencoder	0.87	0.84	0.85	0.91
LSTM	0.91	0.89	0.90	0.95

The LSTM model achieved the highest fraud detection performance due to its ability to capture sequential behavioral anomalies.

5.2 Encryption Overhead

- Encryption latency per transaction: <10 ms
- Total additional processing overhead: ~14%
- System remained suitable for near real-time transaction processing

5.3 Security Analysis

The integration of encryption and anomaly detection:

- Prevented data interception
- Reduced false positive alerts
- Protected stored transaction records
- Mitigated insider threat risks

6. Discussion

The proposed system demonstrates that combining machine learning–based anomaly detection with end-to-end encryption significantly enhances financial transaction security.

Key advantages:

- Real-time anomaly detection
- Strong confidentiality guarantees
- Regulatory compliance support
- Scalable architecture

Limitations include:

- Computational cost of encryption at scale
- Model retraining requirements
- Potential adversarial machine learning risks

Future research should investigate adversarial robustness techniques and lightweight cryptographic methods to further optimize performance.

7. Conclusion

This study presents an integrated framework for secure financial transactions using machine learning–based anomaly detection and end-to-end data encryption. Experimental results confirm that intelligent anomaly detection significantly improves fraud identification accuracy, while encryption safeguards transaction confidentiality. The hybrid architecture provides a scalable and practical security model for modern FinTech infrastructures.

References:

1. Vangala, Dayasagar. "Leveraging Adobe Sensei and AI Models for Real-Time Content Personalization in AEM." *Unique Journal of Artificial Intelligence* 1, no. 1 (2020): 1-16.
2. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Integrating Cyber Risk Metrics into Fintech Product Lifecycle Management." *Econova* 1, no. 01 (2024): 42-53.
3. Goti, Ankit Bharatbhai. "AI-driven Predictive Maintenance for PCB Manufacturing Equipment."
4. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Evaluating Zero Trust Security Models for Fintech Cloud Infrastructures." *Multiverse Journal* 1, no. 1 (2024): 52-60.
5. Goti, Ankit Bharatbhai. "Reliability and Microstructural Analysis of Microvias in UHDI PCBs."
6. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "The Role of Cloud Compliance Automation in Scaling Fintech Products Globally." *Journal of Educational Research in Developing Areas* 4, no. 2 (2023): 245-255.
7. Vangala, Dayasagar. "Secure AEM Integrations Using OAuth and Adobe I/O Runtime." *Famous Journal of computer science and Technology* 1, no. 2 (2020): 1-15.
8. Goti, Ankit Bharatbhai. "Hybrid Additives-Subtractive Manufacturing of Multi-Layer PCBs Using Laser Direct Structuring (LDS) and Inkjet printing." *International Journal of Scientific Research and Management (IJSRM)* 13, no. 06 (2025): 2242-2253.
9. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Multi-Cloud Strategies for Scalable and Secure Fintech Applications." *Journal of Educational Research in Developing Areas* 4, no. 1 (2023): 123-133.
10. Arooj Hassan, Malik Arfat Hassan, & Muhammad Ahsan Khan. (2025). Quantum-Resistant Cryptography in Cloud-Based Fintech Solutions. *Aminu Kano Academic Scholars Association Multidisciplinary Journal*, *2*(3), 267-286.
11. Ghelani, Harshitkumar. "Automated Defect Detection in Printed Circuit Boards: Exploring the Impact of Convolutional Neural Networks on Quality Assurance and Environmental

Sustainability in Manufacturing." *International Journal of Advanced Engineering Technologies and Innovations* 1: 275-289.

12. Ghelani, Harshitkumar. "Harnessing AI for Visual Inspection: Developing Environmentally Friendly Frameworks for PCB Quality Control Using Energy-Efficient Machine Learning Algorithms." *International Journal of Advanced Engineering Technologies and Innovations* 1: 146-154.
13. Ghelani, Harshitkumar. "Enhancing PCB Quality Control through AI-Driven Inspection: Leveraging Convolutional Neural Networks for Automated Defect Detection in Electronic Manufacturing Environments." *Available at SSRN 5160737* (2024).
14. Ghelani, Harshitkumar. "Advances in lean manufacturing: improving quality and efficiency in modern production systems." *Valley International Journal Digital Library* (2021): 611-625.
15. Goti, Ankit Bharatbhai. "AI-Driven PCB Reliability Testing for IPC-9701 Compliance." *International Journal of Scientific Research and Management (IJSRM)* 13, no. 03 (2025): 2068-2087.
16. Goti, Ankit Bharatbhai. "Automated Optical Inspection (AOI) Based on IPC Standards." *International Journal Of Engineering And Computer Science* 13, no. 03 (2025).
17. Ghelani, Harshitkumar. "Revolutionizing Visual Inspection Frameworks: The Integration of Machine Learning and Energy-Efficient Techniques in PCB Quality Control Systems for Sustainable Production." *International Journal of Advanced Engineering Technologies and Innovations* 1: 521-538.
18. Goti, Ankit Bharatbhai. "Cost-Benefit Analysis of ENIG vs. HASL vs. OSP for Class 3 PCBs."
19. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
20. Vangala, Dayasagar. "Optimizing AEM Dispatcher Caching for High-Traffic E-Commerce Sites." *American Journal Of Big Data* 6, no. 6 (2019): 1-17.
21. Goti, Ankit Bharatbhai. "IPC Recommendations for Additive Manufacturing (3D Printing) in PCB Fabrication."

22. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Design Thinking for Secure Fintech Products: Balancing Innovation and Compliance." *Econova* 2, no. 1 (2025): 1-16.
23. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Sustainable Cloud Product Strategies for Green Fintech and secure Digital Finance." *CogNexus* 1, no. 03 (2025): 162-176.
24. Vangala, Dayasagar. "Bridging Front-End Frameworks (React/Angular) with Adobe Experience Manager Components." *Unique Journal of Artificial Intelligence* 1, no. 1 (2018): 1-17.
25. Goti, Ankit Bharatbhai. "Cost and Reliability Implications of Selective Hard Gold Plating Techniques."
26. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Product Management Challenges in AI-Enhanced Fintech Fraud." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 14-28.
27. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "AI-Driven Product Roadmaps in Fintech, Optimizing User Experience and Security Trade-offs." *International Journal of Business & Digital Economy* 1, no. 01 (2025): 1-13.
28. Goti, Ankit Bharatbhai. "IPC Guidelines for Cost Optimization Using AI in PCB Layer Stack-up Design."
29. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Threat Intelligence Automation in Fintech, A Product Management Perspective." *Multiverse Journal* 1, no. 2 (2024): 50-62.
30. Hassan, Arooj, Muhammad Ahsan Khan, and Malik Arfat Hassan. "Impact of Regulatory Compliance PSD2, GDPR on Fintech Product Design." *Frontiers in Multidisciplinary Studies* 1, no. 01 (2024): 59-72.
31. Vangala, Dayasagar. "Headless CMS with AEM: Building Omnichannel Digital Experiences." *Famous Journal of computer science and Technology* 1, no. 3 (2021): 1-15.
32. Goti, Ankit Bharatbhai. "Material and Reliability Guidelines for Flexible PCBs in Class 3."
33. Vangala, Dayasagar. "Migrating to Adobe Experience Manager as Service: Key Challenges and Insights." *Innovations* 1, no. 04 (2022).

34. Ghelani, Harshitkumar. "AI-Driven Quality Control in PCB Manufacturing: Enhancing Production Efficiency and Precision." *Valley International Journal Digital Library* (2024): 1549-1564.
35. Goti, Ankit Bharatbhai. "Moisture Absorption and Outgassing in Flexible and Rigid-Flex PCBs."
36. Vangala, Dayasagar. "Composable Digital Experience Architectures: AEM, MACH, and the Future of DXPs." *Multidisciplinary Research in Computing Information Systems* 4, no. 3 (2024): 34-49.
37. Ghelani, Harshitkumar. "Six Sigma and Continuous Improvement Strategies: A Comparative Analysis in Global Manufacturing Industries." *Valley International Journal Digital Library* (2023): 954-972.
38. Vangala, Dayasagar. "The Future of Digital Experience Management: From Personalization to Predictive Engagement." *Unique Journal of Artificial Intelligence* 3, no. 6 (2025): 1-12.
39. Goti, Ankit Bharatbhai. "IPC Standardization of AI-assisted Real-Time Process Control in PCB Manufacturing."
40. Vangala, Dayasagar. "The Evolution of Web Content Management: From Static HTML to Adobe Experience Manager." *Famous Journal of computer science and Technology* 1, no. 1 (2017): 1-15.
41. Ghelani, Harshitkumar. "Advanced AI Technologies for Defect Prevention and Yield Optimization in PCB Manufacturing." *International Journal Of Engineering And Computer Science* 13, no. 10 (2024).
42. Vangala, Dayasagar. "Integrating Generative AI with AEM for Dynamic Content Generation." *Famous Journal of computer science and Technology* 2, no. 6 (2024): 1-16.
43. Goti, Ankit Bharatbhai. "3D-Printed Multi-Layer PCBs: Evaluating the Structural Integrity and Electromagnetic Compatibility of Additively Manufactured Circuits." *International Journal Of Engineering And Computer Science* 13, no. 06 (2025).
44. Vangala, Dayasagar. "Sustainability in Digital Experience Platforms: Optimizing AEM for Energy Efficiency." *International Research Journal of Advanced Engineering and Technology* 1 (2025): 286-302.

45. Ghelani, HarshitKumar. "The Evolution of Ransomware: Trends and Countermeasures." (2025).
46. Ghelani, H. K. "Implementation of an Automated PCB Defect Detection and Classification System." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 2: 1-15.
47. Ghelani, H. K. "Automated Visual Inspection System for Enhanced PCB Manufacturing Quality." *International Journal of Advanced Engineering Technologies and Innovations* 1, no. 4: 1-24.
48. Ghelani, H. "Sustainable manufacturing engineering: enhancing product quality through green process innovations." *Int. J. Eng. Comput. Sci* 11 (2024): 25632-25649.
49. Hassan, Arooj, Malik Arfat Hassan, and Muhammad Ahsan Khan. "Data-Driven Decision-Making in Fintech Product Development using Cloud Analytics." *Multiverse Journal* (2025): 37-50.