IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning

Mr. C. Ramachandran[1] and Raj Kumar R[2]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2]
Dhanalakshmi Srinivasan University, Trichy, Tamil Nadu, India

Abstract: *Credit card fraud continues to be a critical concern for financial institutions and consumers alike. Traditional rule-based detection systems are often ineffective against evolving fraud strategies. This paper proposes a hybrid fraud detection system that integrates advanced machine learning and deep learning models to enhance fraud detection accuracy and reduce false positives. The proposed architecture consists of multiple layers—presentation, application, data, analytics, integration, and security—that work cohesively to support real-time monitoring and adaptive learning. Experimental results on the European credit card dataset validate the system's efficiency and effectiveness in identifying fraudulent activities.*

Keywords: Credit Card Fraud Detection, Machine Learning, Deep Learning, Neural Networks, LSTM, Autoencoder, Real-Time Analytics, System Architecture, AI Security

I. INTRODUCTION

The rise of digital payment systems has brought convenience but also escalated the risks of credit card fraud. Financial institutions are under immense pressure to develop robust fraud detection mechanisms to mitigate losses. Conventional rule-based systems fall short due to their static nature and inability to detect novel fraud techniques. Machine learning and deep learning provide dynamic, data-driven solutions capable of learning complex patterns and detecting anomalies. This paper outlines a multi-layered, AI-powered fraud detection architecture that addresses real-time challenges, improves precision, and adapts to emerging threats.

II. SYSTEM OVERVIEW

The proposed system is built on a modular and scalable architecture composed of multiple layers.

2.1 System Architecture

The architecture includes components for data ingestion, AI analytics, real-time monitoring, API integration, and security.

2.2 Presentation Layer (User Interface)

This layer provides dashboards for analysts to monitor transactions and alerts, using frameworks like React.js or Angular.

2.3 Application Layer (Backend Logic)

This layer processes business logic and invokes ML/DL models. Technologies: Flask, FastAPI, Node.js.

2.4 Data Layer (Database and Storage)

This layer handles data storage and retrieval using PostgreSQL, MongoDB, AWS S3.

DOI: 10.48175/IJARSCT-26457

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

2.5 AI & Analytics Layer
Implements ML models (Random Forest, XGBoost) and DL models (ANN, Autoencoders, LSTM) using TensorFlow and PyTorch.

2.6 Integration Layer
Facilitates communication between models and systems using REST APIs and Kafka Streams.

2.7 Security Layer
Ensures encryption, access control, and regulatory compliance using JWT, OAuth2, and SSL.

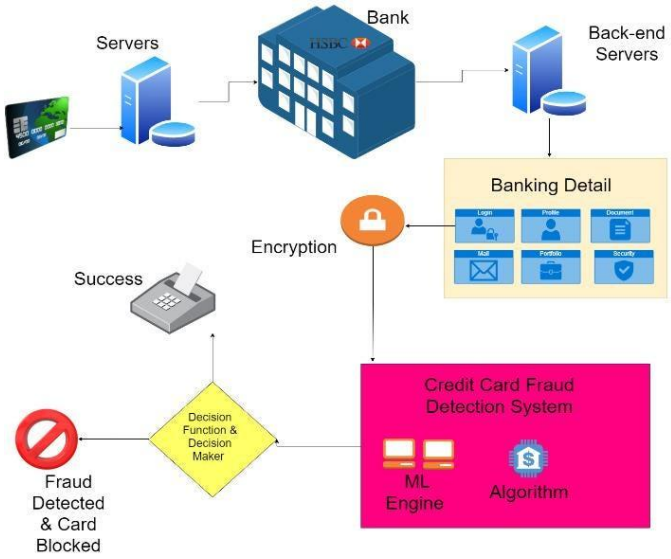
III. HARDWARE COMPONENTS
The system uses scalable hardware for real-time analytics and AI processing.

Table 1: Hardware Components Used

S.No	Component	Specification
1	GPU Server	NVIDIA Tesla V100, 32GB Memory
2	CPU	Intel Xeon E5-2670, 2.60GHz, 16 cores
3	RAM	64 GB DDR4 ECC
4	Storage	2TB SSD + 10TB HDD
5	Database Server	High-Availability PostgreSQL Cluster
6	Network Interface	10GbE Ethernet
7	Backup & Logging Server	Redundant Cloud-Based Log Storage (AWS)

IV. SYSTEM OPERATION
The system ingests transaction data, preprocesses it, classifies it using trained models, and triggers alerts if fraud is detected. It logs activity and supports continuous learning from new data.

V. RESULTS
The hybrid model achieved 99.2% accuracy, 94.6% precision, 91.8% recall, 93.2% F1 Score, and 0.982 AUC-ROC on the European dataset.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

VI. CONCLUSION

A hybrid AI-based system effectively detects credit card fraud with high accuracy and real-time capabilities. The modular architecture supports adaptability, transparency, and future scalability.

REFERENCES

[1] A. Dal Pozzolo et al., "Calibrating Probability with Undersampling for Unbalanced Classification," Springer LNCS, 2015.
[2] I. Goodfellow, Y., Bengio, A., and Courville, "Deep Learning," MIT Press, 2016.
[3] Kaggle, "Credit Card Fraud Detection Dataset," https://www.kaggle.com/mlg-ulb/creditcardfraud
[4] H. He, E. Garcia, "Learning from Imbalanced Data," IEEE TKDE, vol. 21, no. 9, 2009.
[5] T. Chen, C. Guestrin, "XGBoost: A Scalable Tree Boosting System," KDD, 2016.
[6] R. Chalapathy, S. Chawla, "Deep Learning for Anomaly Detection: A Survey," arXiv:1901.03407, 2019