

Deep Learning – Base Credit Card Fraud Detection with Real-Time Alert

Shruti Niphade¹, Nikita Dargude², Rutuja Gholap³, Shweta Gangurde^{4, 5}

¹²³⁴Student, Computer Engineering, Matoshri College of Engineering and Research Centre, Nashik, Maharashtra, India.

⁵Assistant Professor, Computer Engineering, Matoshri College of Engineering and Research Centre, Nashik, Maharashtra, India.

ABSTRACT

It is essential for credit card The rapid increase in online transactions, mobile banking, and digital payment systems has significantly improved financial services worldwide. However, this growth has also increased the number of fraudulent credit card transactions. Credit card fraud causes major financial losses to banks, businesses, and customers. Traditional fraud detection systems based on rule-based approaches and manual verification are no longer sufficient because fraudsters continuously develop new techniques to bypass security systems.

This research paper proposes a Deep Learning-Based Credit Card Fraud Detection System integrated with a Real-Time Alert Mechanism. The proposed system uses a Hybrid CNN-LSTM Deep Learning Model to analyze customer transaction patterns and identify fraudulent activities with high accuracy. Convolutional Neural Networks (CNN) are used for feature extraction, while Long Short-Term Memory (LSTM) networks analyze sequential transaction behavior.

1. INTRODUCTION

In recent years, digital payment systems have become an important part of modern society. Online banking, e-commerce platforms, mobile wallets, and internet transactions have increased the use of credit cards globally. Credit cards provide convenience, fast transactions, and secure payment facilities. However, the rapid growth of digital transactions has also increased fraudulent activities.

Credit card fraud is a type of financial crime where unauthorized users perform illegal transactions using stolen or fake credit card information. Fraudsters use techniques such as phishing, card cloning, identity theft, and online hacking to access customer information. According to global financial reports, millions of dollars are lost every year due to credit card fraud.

Traditional fraud detection systems use predefined rules and manual verification processes. These systems can identify only known fraud patterns and fail to detect new or complex attacks. In addition, traditional systems produce a high number of false alerts, causing inconvenience to genuine customers.

Artificial Intelligence (AI) and Deep Learning technologies provide advanced solutions for fraud detection. Deep learning algorithms can analyze large amounts of transaction data, identify hidden patterns, and detect unusual customer behavior automatically. Unlike traditional methods, deep learning models continuously improve their performance by learning from historical transaction data.

The proposed system combines CNN and LSTM deep learning models with a real-time monitoring framework. The system not only detects fraud accurately but also sends immediate alerts to customers and banking systems whenever suspicious activity occurs.

The major goals of the proposed system are:

1. Detect fraudulent transactions accurately.
2. Reduce false positive and false negative rates.
3. Monitor transactions in real time.
4. Generate instant alerts for suspicious activities.
5. Improve transaction security and customer trust.

The proposed research introduces a Deep Learning-Based Credit Card Fraud Detection System using a Hybrid CNN-LSTM Neural Network integrated with a Real-Time Alert Mechanism. The Convolutional Neural Network (CNN) is used for feature extraction, while the Long Short-Term Memory (LSTM) network analyzes sequential transaction behavior over time. The system continuously monitors transactions and predicts whether a transaction is genuine or fraudulent. Whenever suspicious activity is detected, the system immediately generates alerts through SMS, email, or mobile notifications. This real-time alert feature helps banks and customers take immediate action to prevent financial losses and unauthorized access.

The main aim of this research is to develop an intelligent, accurate, and real-time fraud detection system that improves transaction security, reduces false alarms, and enhances customer trust in digital payment platforms.

1.1 LITERATURE SURVEY

In 2025, researchers focused on improving fraud detection accuracy using Hybrid Deep Learning Models and Explainable Artificial Intelligence (XAI). Modern fraud detection systems combined Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to analyze transaction patterns and customer behavior more effectively. Researchers found that hybrid models provided higher accuracy and lower false positive rates compared to traditional machine learning algorithms. Real-time alert systems integrated with cloud computing and AI-based monitoring were also introduced to generate instant notifications for suspicious transactions.

In 2024, several researchers worked on anomaly detection techniques using Autoencoders and Deep Neural Networks (DNN). These systems automatically learned normal customer transaction behavior and identified unusual activities as fraudulent transactions. Hybrid ensemble learning methods combining Random Forest, CNN, and LSTM models were proposed to improve prediction accuracy and recall values. Researchers also focused on reducing false alarms because many genuine transactions were incorrectly classified as fraud.

In 2023, deep learning approaches such as Recurrent Neural Networks (RNN), LSTM, and CNN gained popularity in fraud detection systems. Researchers emphasized sequential transaction analysis because customer spending behavior changes over time. LSTM models showed better performance in identifying hidden fraud patterns from transaction sequences.

In 2022, researchers mainly focused on comparing traditional machine learning algorithms with deep learning techniques. Algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM) were analyzed along with Artificial Neural Networks (ANN).

In 2021, fraud detection systems based on Artificial Neural Networks (ANN) and data mining techniques were developed to improve transaction security. Researchers proposed intelligent classification systems capable of identifying suspicious transaction behavior automatically.

2. METHODOLOGY

The approach that this paper proposes, uses the latest machine learning algorithms to detect anomalous activities, called outliers. The basic rough architecture diagram can be represented with the following figure:

2.1 SYSTEM OVERVIEW:

The system begins when an incoming customer transaction is received through a banking or online payment system. The transaction is then sent to the Fraud Detection System, where the Fraud Detection Algorithm and Pattern Finding modules analyze the transaction details. The system compares the current transaction with previous customer transaction records stored in the Customer Transaction Database to identify suspicious behavior or unusual patterns.

After analysis, the system generates the Algorithm Output. If the transaction is identified as fraudulent, it is marked as a Fraudulent Transaction, and an immediate alarm is sent to the bank to stop or block the transaction. If the transaction is identified as genuine, it is marked as a Legal Transaction, and the system allows the transaction to complete successfully.

2.2 SYSTEM ARCHITECTURE:

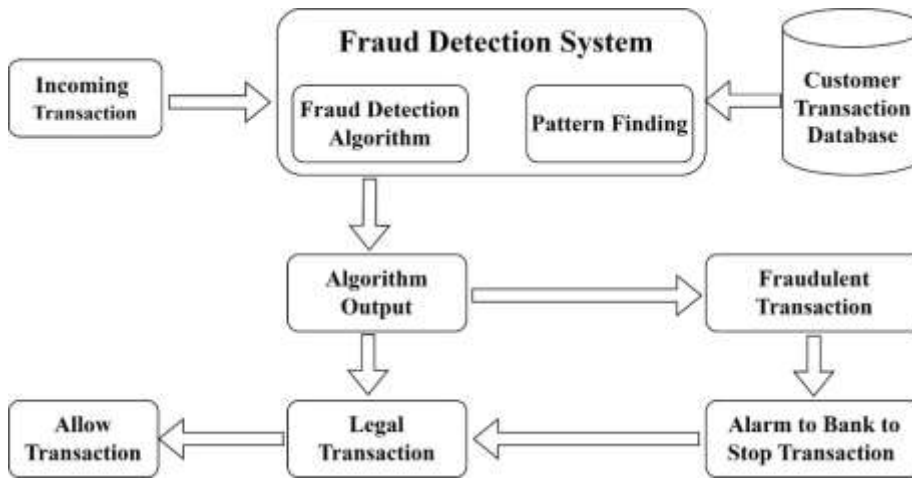


Fig 1.Architecture

3. Problem Statement

Credit card fraud has become a serious issue in the banking and financial sector. Existing fraud detection systems face multiple limitations such as:

- Inability to detect new fraud patterns.
- High false positive rate.
- Delayed fraud detection.
- Poor performance on large transaction datasets.
- Lack of real-time alert systems.
- Difficulty handling imbalanced datasets.

Fraudulent transactions are usually very small compared to genuine transactions, making fraud detection a highly imbalanced classification problem. Therefore, there is a need for an intelligent system capable of identifying fraudulent transactions efficiently in real time.

The proposed research aims to design a Deep Learning-Based Credit Card Fraud Detection System integrated with Real-Time Alerts to improve detection accuracy and transaction security.

4. Dataset Description

The proposed system uses the Kaggle Credit Card Fraud Detection Dataset. The dataset contains thousands of genuine and fraudulent transaction records.

Dataset Features

- Transaction ID
- Transaction Time
- Transaction Amount
- Customer Information
- Merchant Information
- Transaction Type
- Device Information
- Fraud Label

The dataset is highly imbalanced because fraudulent transactions are very small compared to genuine transactions.

5. Data Preprocessing

Data preprocessing is an important step in machine learning and deep learning systems.

Operations Performed

1. Handling missing values.
2. Removing duplicate records.
3. Data normalization.
4. Feature scaling.
5. Handling imbalanced datasets using SMOTE.
6. Splitting dataset into training and testing data.
7. Data encoding and transformation.

Preprocessing improves model performance and fraud detection accuracy.

6. System Architecture

1. Data Collection Module

Collects transaction information such as:

- Transaction ID
- Transaction amount
- Time and date

- Customer location
 - Merchant information
 - Payment method
-

2. Data Preprocessing Module

This module performs:

- Data cleaning
- Missing value handling
- Feature normalization
- Duplicate removal
- Data transformation

3. Feature Engineering Module

Important features are selected for training:

- Transaction frequency
 - Average spending pattern
 - Transaction location
 - Time interval between transactions
-

4. Deep Learning Training Module

ANN and LSTM models are trained using historical transaction datasets.

5. Fraud Detection Module

The trained model classifies transactions as:

- Genuine Transaction
 - Fraudulent Transaction
-

6. Real-Time Alert Module

If fraud is detected:

- SMS alert is sent
 - Email notification is generated
 - Bank administrator is notified
-

7. Modeling and Analysis

Training Phase

Dataset split:

- Training Data → 80%
- Testing Data → 20%

Optimizer used:

- Adam Optimizer
-

Accuracy Formula

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision Formula

$$Precision = \frac{TP}{TP + FP}$$

Recall Formula

$$Recall = \frac{TP}{TP + FN}$$

F1-Score Formula

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

8. CONCLUSION

The proposed Blockchain-Based Credit Card Fraud Detection and Secure Transaction System using Deep Learning provides an intelligent and secure solution for detecting fraudulent transactions. The Hybrid CNN-LSTM model improves fraud detection accuracy by analyzing customer transaction behavior effectively, while Blockchain technology enhances data security and transparency. Real-time alerts help banks and customers take immediate action against suspicious activities. Therefore, the proposed system can significantly improve digital payment security and reduce financial losses in modern banking systems.

The Deep Learning-Based Credit Card Fraud Detection System with Real-Time Alerts provides an efficient solution for detecting fraudulent financial transactions. Deep learning models such as DNN, LSTM, and Autoencoders improve fraud detection accuracy by learning hidden transaction behaviors. The integration of a real-time alert system enhances banking security and helps prevent financial losses. The proposed system is scalable, intelligent, and suitable for modern online banking environments.

9. REFERENCES

- [1] “Credit Card Fraud Detection Based on Transaction Behaviour -by John Richard D. Kho, Larry A. Veal” published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017
- [2] “H. Zhu, M. C. Zhou, Y. Xie, and A. Albeshri, “A Self-Adapting and Efficient Dandelion Algorithm and Its Application to Feature Selection for Credit Card Fraud Detection,” *IEEE/CAA Journal of Automatica Sinica*, vol. 11, no. 2, pp. 377–390, 2024.
- [3] “Ibrahim Almubark, “Advanced Credit Card Fraud Detection: An Ensemble Learning Using Random Under Sampling and Two-Stage Thresholding,” *IEEE Access*, vol. 12, pp. 192079–192089, 2024.
- [4] “Emmanuel Ileberi and Yanxia Sun, “A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection,” *IEEE Access*, vol. 12, pp. 175829–175838, 2024
- [5] “Credit Card Fraud Detection Yu Xie, Guanjun Liu, Chungang Yan, Changjun Jiang, Mengchu Zhou, and Maozhen Li, “Learning Transactional Behavioral Representations for Credit Card Fraud Detection,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 4, pp. 5735–5748, 2024.
- [6] “Credit Card Fraud Detection: Kanishka Ghosh Dastidar, Olivier Caelen, and Michael Granitzer, “Machine Learning Methods for Credit Card Fraud Detection: A Survey,” *IEEE Access*, 2024.
- [7] “Credit Card Fraud Detection-by Ishu Trivedi, Monika, Mrigya, Mridushi” published by International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016
- [8] Mengran Zhu, Ye Zhang, Yulu Gong, Changxin Xu, and Yafei Xiang, “Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach,” *arXiv Research Paper*, 2024.