Fraud Detection in Online Transactions

Nirajitha.M[1], Pavithra.M[2], Swetha.M[3], Swetha.S[4], Janani.C[5]

[12345] *Department of CSE, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore 18.*

22ueo035@avinuty.ac.in, 22ueo040@avinuty.ac.in, 22ueo056@avinuty.ac.in, 22ueo058@avinuty.ac.in, janani_cse@avinuty.ac.in

----
-

Abstract -The rapid growth of online transactions has significantly increased the risk of fraudulent activities, making fraud detection an important challenge for financial institutions. Traditional rule-based fraud detection systems often fail to adapt to evolving fraud patterns and large volumes of transaction data. To address this issue, this paper presents a machine learning-based approach for detecting fraudulent online transactions using deep learning models. The proposed system utilizes Convolutional Neural Networks (CNN) to extract meaningful patterns from transaction features and Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) to analyze sequential transaction behavior. The model is trained on a publicly available transaction dataset and evaluated using standard performance metrics such as accuracy, precision, recall, and F1-score. A user-driven web interface is also developed to allow fraud prediction based on input transaction details. Experimental results indicate that the proposed approach is effective in identifying fraudulent transactions and can support decision-making in online payment systems. This work focuses on practical implementation and performance evaluation.

Key Words: Online transaction, Fraud detection, Deep learning, CNN, LSTM, Transaction classification

1.INTRODUCTION

The rapid growth of online payment systems and digital transactions has increased the risk of fraudulent activities, resulting in financial losses and reduced customer trust. As transaction volumes continue to rise, accurate fraud detection has become an important challenge for banks and online payment service providers. Traditional fraud detection methods mainly rely on predefined rules and manual verification. While these methods are effective to some extent, they often fail to identify complex and evolving fraud patterns and may produce a high number of false alerts. Recent advances in machine learning and deep learning have shown significant potential in improving fraud detection by learning patterns directly from transaction data.

In this work, a deep learning-based approach for fraud detection in online transactions is presented using Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM). CNN is used to extract relevant features from transaction data, while LSTM captures sequential transaction behavior. The proposed system is developed as a project with a focus on practical implementation and performance evaluation using user-provided transaction inputs.

2. OBJECTIVES

- To analyze online transaction data and identify patterns associated with fraudulent activities.
- To apply Convolutional Neural Networks (CNN) for extracting meaningful features from transaction data.
- To utilize Recurrent Neural Networks (RNN) with Long Short-Term Memory (LSTM) to capture sequential transaction behavior.
- To evaluate the performance of the proposed model using standard classification metrics.

3. LITERATURE REVIEW

Recent studies highlight the growing importance of AI and machine learning in fraud detection across e-commerce and banking. Rao et al. (2025) review transaction risk prevention strategies in e-commerce, emphasizing scalability and usability. Kokkalakonda (2022) shows how AI-powered models enhance banking security by reducing false positives and negatives. Chang et al. (2022) discuss adaptive fraud detection methods in digital payments under Industry 4.0, while Madabhattula et al. (2021) present practical online transaction detection approaches. Beyond transactions, Bhardwaj et al. (2021) propose privacy-aware frameworks against phishing, and De Keyser et al. (2021) explore biometrics for fraud prevention, noting both opportunities and challenges. Shrestha et al. (2021) highlight deep learning's role in augmenting organizational decision-making, and Canhoto (2020) extends machine learning applications to global issues like money laundering and terrorism financing.

4.SYSTEM ARCHITECTURE AND COMPONENTS

The architecture begins with transaction data acquisition, followed by preprocessing steps such as cleaning, normalization, and encoding. CNN layers are used to capture local feature dependencies within structured transaction data, while LSTM captures temporal transaction behavior. The classification module flags fraud using probability thresholds. A web-based interface allows users to input transaction IDs and view fraud analysis results. Components include Python, Flask, TensorFlow, Pandas, NumPy, Scikit-learn, and visualization libraries, supported by hardware with GPU acceleration for efficient training.

5.METHODOLOGIES

5.1 Data Collection

The fraud detection process begins with collecting transaction datasets from sources such as Kaggle or financial institutions, which typically include transaction IDs, timestamps, merchant details, amounts, user demographics, and fraud labels. These datasets are often highly imbalanced, with fraudulent transactions making up a very small percentage, which poses challenges for model training.

5.2 Data Preprocessing

The raw data is cleaned to remove duplicates and handle missing values, normalized to scale numerical features like transaction amounts, and categorical variables (e.g., merchant type, location, device type) are encoded using techniques such as one-hot encoding or embeddings. Since fraud cases are rare, imbalance handling methods like SMOTE, undersampling are applied to ensure the model learns effectively from both fraudulent and legitimate transactions.

5.3 Feature Extraction

Convolutional Neural Networks (CNNs) are used to extract structured patterns from transaction data, such as correlations between merchants, users, and transaction times. By treating transaction records as structured matrices, CNNs can identify local dependencies and hidden fraud-related features that traditional models might miss.

5.4 Sequential Analysis

Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, are employed to capture sequential and temporal patterns in user behavior. For example, they can analyze transaction sequences over time to detect unusual spending habits or sudden deviations from normal activity, which are strong indicators of fraud.

5.5 Model Training

Both CNN and RNN models are trained on labeled datasets, where fraudulent and legitimate transactions are clearly marked. Training involves optimizing parameters to minimize classification errors, often using techniques like cross-validation and dropout to prevent overfitting. The combination of CNNs and RNNs allows the system to learn both spatial and temporal fraud indicators.

5.6 Prediction and Result Analysis

Once trained, the models predict whether a transaction is fraudulent or legitimate. The output includes fraud status, accuracy scores, and transaction details, enabling analysts to evaluate model performance. Metrics such as precision, recall, F1-score, and ROC-AUC are used to assess effectiveness, ensuring the system balances catching fraud with minimizing false alarms.

6. IMPLEMENTATION

The system implementation consists of a optimized usability web interface that allows users to enter a transaction ID and check its fraud status.

The major modules include:

1. Creation of Homepage
2. Development of User Input Interface
3. Implementing the interface for displaying results

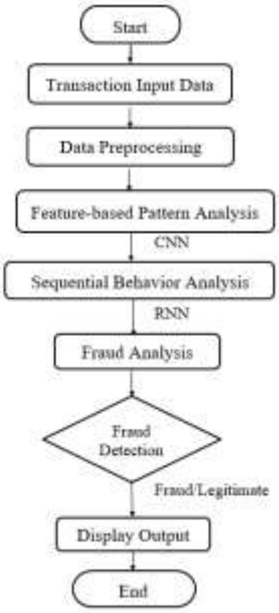
6.1 Creation of Homepage

The Homepage serves as the entry point, offering a structured interfacae with a clear heading titled "Transaction Fraud Detection." Users can input a transaction ID and click the "Check Transaction" button, which retrieves details and processes them using deep learning models CNN and RNN to classify fraudulent transactions. The results, including fraud status, transaction type, accuracy score, sender, receiver, and timestamp, are displayed below. The system integrates frontend, backend, and machine learning components seamlessly.

6.2 Development of User Input Interface

The main application interface is designed for simplicity and responsiveness, prompting users to enter a transaction ID into a clearly labeled input field. Beneath it, a interactive web interface "Check Transaction" button initiates backend processing, where transaction features are extracted and passed through trained CNN/RNN models. The system then returns fraud prediction results, displaying the fraud status along with accuracy scores and transaction details. This seamless interaction ensures a smooth user experience, making the tool accessible to both technical and non-technical users.

6.2.1 Block Diagram

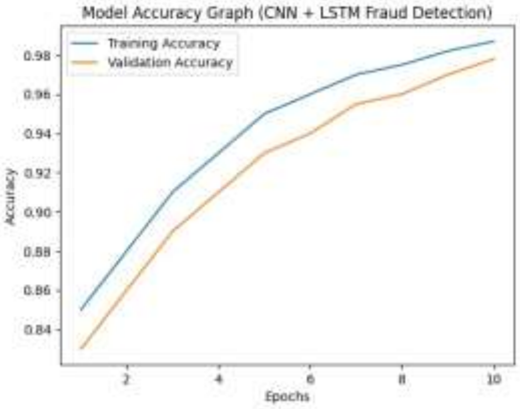


6.3 Implementing the interface for displaying results

After submitting a transaction ID, the results are shown in a clear, structured section displaying the transaction ID, fraud detection result, match accuracy, transaction type, and key details like sender, receiver, and timestamp. A collapsible option lets users expand detailed data without cluttering the screen, while visual cues such as colors and icons enhance transparency. This design ensures readability and user confidence, with deep learning models providing real-time fraud classification seamlessly integrated into the interface.

7. RESULT AND FEATURES

The CNN and LSTM fraud detection system works by progressively learning transaction patterns over multiple epochs, where training accuracy improves from about 85% to nearly 99% and validation accuracy rises from around 83% to 98%, confirming both effective learning and reliable generalization with minimal overfitting. After deployment , the system integrates deep learning models capability into a real-time interface: users enter a transaction ID, and the system instantly analyzes the transaction, presenting detection status, correctness, and transaction type, with collapsible details such as sender, receiver, and transaction time for deeper insights. Visual cues and icons enhance transparency, ensuring results are easy to interpret without overwhelming the user. This combination of high accuracy progression, scalable model design, and intuitive interface makes the system robust, efficient, and suitable for financial institutions and e-commerce platforms where fraud prevention is mission-critical.



8. CONCLUSION

The Online Payment Fraud Detection project successfully built a scalable and efficient system capable of identifying fraudulent transactions in real-time using machine learning. A structured workflow was followed data collection, preprocessing, model training, and evaluation resulting in a robust model that detects suspicious patterns in transaction data. CNN datand RNN were tested, and the best-performing one was chosen based on accuracy, precision, recall, and F1 score. Preprocessing techniques such as normalization, categorical encoding, and missing value imputation ensured data quality and optimized performance. The model was then integrated into a user-friendly interface, enabling seamless real-time fraud detection with transparency and accessibility. System testing and validation confirmed its reliability and scalability, preparing it for deployment in real-world financial and e-commerce platforms. Overall, the project demonstrates the potential of machine learning in combating online payment fraud, while emphasizing the need for continuous improvements as fraud techniques evolve.

9.APPLICATIONS

The system can be applied across banking, e-commerce, and payment gateways to detect suspicious transactions in real time. Its ability to handle large-scale fraud monitoring ensures that institutions can process high transaction volumes without compromising accuracy. By reducing false positives and negatives, it helps improve customer trust and confidence in digital payments. The system also plays a crucial role in minimizing financial losses, safeguarding both businesses and users. With its scalable architecture, it can be seamlessly integrated into existing financial platforms, making it suitable for deployment in diverse real-world environments. This adaptability ensures that the solution remains effective as transaction patterns and fraud techniques evolve.

10.ACKNOWLEDGEMENT

We, the students of CSE, want to express our heartfelt thanks to our guide, Assistant Professor C.Janani, for their essential help, support, and encouragement during this project. We also appreciate the Department of CSE at Avinashilingam Institute for giving us the resources and facilities we needed. Lastly, we would like to recognize our team members for their support and teamwork, which were crucial to finishing this work successfully.

REFERENCES

[1] Rao, S. X., Jiang, J., Han, Z., & Yin, H. (2025). *Fraud Detection in E-Commerce: A Systematic Review of Transaction Risk Prevention.* IntechOpen.

[2] Kokkalakonda, N. K. (2022). *AI-powered fraud detection in banking: Enhancing security with machine learning algorithms.* International Journal of Science and Research Archive.

[3] Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z., & Fortino, G. (2022). *Digital payment fraud detection methods in digital ages and Industry 4.0.* CSE.

[4] Madabhattula, L., Manikanta, M., & Kumar, P. (2021). *Online Transaction Fraud Detection.* International Journal of Creative Research Thoughts.

[5] Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). *Privacy-aware detection framework to mitigate new-age phishing attacks.* Computers & Electrical Engineering.

[6] De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. (2021). *Opportunities and challenges of using biometrics for business: Developing a research agenda.* Journal of Business Research.

[7] Shrestha, Y. R., Krishna, V., & von Krogh, G. (2021). *Augmenting organizational decision-making with deep learning algorithms: Principles, promises, and challenges.* Journal of Business Research.

[8] Canhoto, A. I. (2020). *Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective.* Journal of Business Research.