Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

Credit Card Fraud Detection using CNN

Piyush Mishra, Manthan Martiwar, Lucky Pandey,
Garv Pampattiwar, Lokesh Waydule,
Students, Department of Computer Science and Engineering Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, Maharashtra, India

Prof. Sachin Dhawas
Assistant Professor,
Department of Computer Science Engineering
Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, Maharashtra, India

Abstract-Credit card fraud has emerged as one of the most critical challenges in the digital financial ecosystem due to the rapid growth of online transactions and increasingly sophisticated fraudulent activities. Traditional machine learning techniques, though effective to some extent, often struggle to capture complex, high-dimensional patterns hidden in large transaction datasets. To address this limitation, this study explores the use of Convolutional Neural Networks (CNNs) for detecting credit card fraud with higher accuracy and generalization. CNNs, widely recognized for their ability to automatically learn spatial and hierarchical features, are applied to transaction data by transforming numerical features into structured representations suitable for convolutional operations. The model learns subtle variations between legitimate and fraudulent transactions through multiple convolution and pooling layers, reducing the need for manual feature engineering. The proposed CNN-based system demonstrates improved sensitivity to rare fraud cases, faster feature extraction, and robust classification performance. By leveraging deep learning's capability to handle imbalanced and noisy data, this approach contributes to building an intelligent, scalable, and real-time fraud detection framework. The findings highlight the potential of CNNs as a powerful tool for enhancing security in financial systems and mitigating economic losses caused by fraudulent transactions.

I. INTRODUCTION

In today's digital economy, the use of credit cards for online and offline transactions has increased rapidly, making financial services more convenient but also more vulnerable to fraud. Credit card fraud occurs when unauthorized individuals misuse card information to carry out illegal transactions, leading to significant financial losses for customers and companies. Traditional fraud detection systems rely on fixed rules or basic machine learning models, which often fail to detect new and evolving fraud patterns. As fraudulent activities become more complex, there is a growing need for intelligent systems that can automatically learn hidden patterns and adapt to changing behaviours.

Convolutional Neural Networks (CNNs), a popular deep learning technique, offer an effective solution due to their ability to extract meaningful features from structured data without manual intervention. By converting transaction data into suitable input formats, CNNs can identify subtle differences between legitimate and fraudulent transactions with higher accuracy. This approach improves detection speed, handles large datasets efficiently, and provides better performance against unseen fraud attempts. Therefore, applying CNNs in credit card fraud detection can significantly enhance security, reduce risks, and support safer digital financial operations.

II. LITERATURE SURVEY

Credit card fraud detection has been widely studied due to the rise of online transactions and the increasing complexity of fraudulent behaviours. Early research primarily focused on rule-based systems and traditional machine learning techniques, but these methods struggled to detect new and evolving fraud patterns. As a result, deep learning models, especially Convolutional Neural Networks (CNNs), have gained significant attention for their ability to learn hidden patterns without manual feature engineering.

One of the notable studies proposes a CNN-based fraud detection model specifically tailored for online transactions. It demonstrates that CNNs can effectively capture complex, non-linear relationships within transaction features by structuring data into matrices suitable for convolutional operations . Another study shows that CNN architectures outperform standard neural networks by automatically extracting hierarchical features and achieving higher accuracy in classifying fraudulent and legitimate transactions .

Recent reviews further highlight that deep learning techniques, including CNNs, have become state-of-the-art due to their robustness against imbalanced data and ability to scale for large datasets. These works emphasize the superiority of CNNs in detecting rare fraud cases and adapting to evolving patterns compared to traditional machine learning methods .

Overall, existing literature indicates that CNN-based models provide a powerful and reliable approach for modern fraud

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

detection systems, offering improved accuracy, automated feature learning

III. METHODOLOGIES

The methodology for credit card fraud detection using Convolutional Neural Networks (CNNs) involves a systematic sequence of steps designed to preprocess data, transform it into CNN-compatible formats, train the model, and evaluate its performance. The overall process ensures accurate classification of legitimate and fraudulent transactions.

1. Data Collection

The system begins with collecting a large dataset of credit card transactions. Each transaction contains attributes such as amount, time, location, merchant category, and anonymized numerical features. Since fraud datasets are highly imbalanced, data collection must preserve both majority (legitimate) and minority (fraudulent) classes.

2. Data Preprocessing

Preprocessing is essential to convert raw transactional data into a structured and clean format. Key steps include:

- **Handling Missing Values:** Removing or imputing missing entries.
- **Normalization/Scaling:** Applying Min-Max or Standard Scaling to maintain uniform value ranges.
- **Encoding Categorical Fields:** Transforming merchant types, transaction modes, etc., into numerical values.
- **Balancing the Dataset:** Using SMOTE, undersampling, oversampling, or class-weight adjustments to handle imbalance.

3. Data Transformation for CNN

CNN models require structured input. Transaction features are reshaped into **2D matrices** (e.g., 8×8 or 10×10 grids). This allows the CNN to identify spatial relationships between attributes, improving pattern recognition.

If using images, features are mapped onto grayscale pixel grids.
If using feature matrices, each value becomes a matrix cell.

4. CNN Model Design

The CNN architecture typically includes:

- **Convolutional Layers:** Extract important spatial features from transaction matrices.
- **ReLU Activation:** Introduces non-linearity and enhances pattern learning.
- **Pooling Layers:** Reduces dimensionality while preserving essential features.
- **Flatten Layer:** Converts extracted feature maps into a 1-dimensional vector.
- **Fully Connected Layers:** Perform final classification into “fraudulent” or “legitimate.”
- **Softmax/Sigmoid Output:** Produces probability scores for each class.

The architecture may vary based on dataset size and feature complexity.

5. Training the Model

The CNN is trained using:

- **Training Set:** Used to learn feature patterns.
- **Validation Set:** Helps tune hyperparameters like learning rate, batch size, and number of filters.
- **Loss Function:** Binary Cross-Entropy for two-class fraud detection.
- **Optimizer:** Adam or RMSprop to improve convergence.
- **Epochs:** Multiple iterations to ensure stable learning.

The model adjusts its weights to reduce misclassification errors.

6. Evaluation and Performance Metrics

Once trained, the model is evaluated using:

- **Accuracy**
- **Precision**
- **Recall (Sensitivity)** — critical for detecting fraud
- **F1-Score**
- **Confusion Matrix**
- **ROC–AUC Curve**

Since fraud cases are rare, recall and F1-score are more important than accuracy.

7. Real-Time Prediction

The final model is deployed to classify incoming transactions:

- Transactions are preprocessed in real time
- Converted to the required matrix format
- Passed through the trained CNN
- Output label determines if the transaction is normal or suspicious

If predicted as fraud, the system triggers an alert or blocks the transaction.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

8. Continuous Learning

Fraud patterns change rapidly. Therefore, the model is periodically retrained with new data to improve accuracy and adapt to emerging fraudulent behaviours.

IV. CHALLENGES IN CREDIT CARD FRAUD DETECTION USING CNN

Although Convolutional Neural Networks provide strong feature-learning capabilities, their application in credit card fraud detection faces several practical and technical challenges. These challenges arise from the nature of financial data, evolving fraud strategies, and the limitations of deep learning models.

1. Highly Imbalanced Datasets

Fraudulent transactions represent less than 1% of total transactions.
CNNs tend to learn patterns of the majority class (legitimate transactions) and may ignore rare fraud cases. This leads to high accuracy but poor recall, making the model unreliable for real-world use.

2. Difficulty in Data Representation

CNNs work best with image-like structured data. However, credit card transactions are numerical and categorical.
Converting them into 2D matrices can be challenging because:

- There is no natural spatial relationship between features.
- Different reshaping strategies may affect model performance.
- Feature ordering must be carefully designed to avoid misleading patterns.

3. Dynamic and Evolving Fraud Patterns

Fraudsters constantly change their techniques. CNN models trained on historical data may not detect new, unseen fraud behaviours unless frequently retrained. This reduces the long-term reliability of the system.

4. Data Privacy and Availability

Banks and financial institutions have strict rules regarding data sharing.
Access to large, real-world fraud datasets is limited, making it difficult to build robust CNN models. Synthetic datasets may not fully represent actual fraud patterns.

5. High Computational Requirements

CNN models require significant:

- Training time
- GPU resources
- Memory and processing power

Small organizations or real-time systems may find it difficult to deploy heavy CNN architectures.

6. Overfitting Issues

Because fraud cases are few and patterns are very specific, CNNs may overfit the minority class.
The model may perform very well on training data but fail to generalize to new transactions.

7. Noise and Irregularities in Transaction Data

Financial data may contain:

- Missing values
- Outliers
- Incorrect entries
- Unstructured textual information (location, merchant category)

CNN performance declines sharply when input data is noisy or poorly preprocessed.

8. Lack of Interpretability

CNNs are often criticized as “black box” models. It is difficult to explain why the model marked a transaction as fraud.
Banks and regulatory bodies require interpretability for compliance and customer trust.

9. Real-Time Processing Challenges

Fraud detection must work in milliseconds. Deep CNNs may cause latency due to:

- Complex architecture
- Large input matrices
- Heavy computations

Real-time payment systems cannot tolerate delays.

10. Integration with Existing Banking Systems

Banks use legacy systems. Integrating CNN-based solutions with these systems requires:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

- API modifications
- Security approvals
- Protocol compatibility
- Robust monitoring mechanisms

Implementation can be slow and costly.

V. APPLICATIONS

The application of Convolutional Neural Networks (CNNs) in credit card fraud detection has introduced advanced, intelligent, and real-time solutions to modern financial systems. CNN-based fraud detection models are applied across multiple domains to ensure secure, trustworthy, and efficient transaction processing.

1. Real-Time Transaction Monitoring

CNNs can classify transactions within milliseconds, making them ideal for live transaction environments. Banks and financial institutions use CNN-based systems to instantly detect suspicious behaviour and prevent unauthorized payments before they are completed.

2. Online and E-commerce Payment Security

E-commerce platforms use CNN models to analyze transaction patterns such as payment method, device ID, location, and spending habits.
CNNs help identify abnormal activities like:

- sudden high-value purchases
- unusual device usage
- rapid transaction sequences

This enhances safety for online shoppers and merchants.

3. Fraud Prevention in Mobile Banking

Mobile banking apps integrate CNN-based fraud detection to monitor:

- mobile wallet transactions
- UPI payments
- card-not-present transactions
- digital wallet top-ups

This helps reduce the risk of unauthorized access and transactions made from compromised devices.

4. Risk Scoring and Customer Behaviour Analysis

CNN models analyze user behaviour over time and generate dynamic risk scores.
This helps banks identify accounts with unusual spending patterns and apply:

- additional verification
- temporary account hold
- OTP requirements
- automatic alerts

It reduces financial losses and improves customer security.

5. Chargeback and Dispute Reduction

CNN-based detection systems minimize fraudulent transactions, directly lowering:

- chargeback claims
- reimbursement costs
- merchant losses

This helps businesses avoid legal and financial complications.

6. ATM and POS Transaction Monitoring

CNNs analyze patterns in ATM withdrawals and point-of-sale (POS) transactions.
They help detect:

- cloned card activities
- unusual withdrawal locations
- multiple attempts from the same machine

This strengthens physical banking security.

7. Banking Compliance and Regulatory Support

Financial institutions must follow strict fraud prevention guidelines.
CNN models support regulatory compliance by providing:

- automated fraud reports
- high-accuracy detection results
- reduced human intervention
- transparent risk management processes

8. Enhanced Security for Subscription Services

Platforms that use recurring billing (OTT platforms, digital services, SaaS products) employ CNN-based fraud detection to verify the legitimacy of transactions and prevent misuse of saved card details.

9. Integration in Financial Intelligence Systems

CNN models are used in advanced financial intelligence platforms for:

- big data analytics

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

- pattern visualization
- deep fraud investigation
- anomaly detection across millions of transactions

They support both operational and investigative teams in analyzing complex fraud networks.

VI. COMPARITIVE ANALYSIS OF DIFFERENT METHODS

Credit card fraud detection has evolved from simple rule-based approaches to advanced deep learning models. Each method has unique strengths and limitations. The following comparative analysis highlights how different techniques perform in terms of accuracy, scalability, adaptability, feature handling, and real-time performance.

1. Rule-Based Systems

- Simple and easy to implement.
- Fast in real-time detection.
- Cannot detect new or evolving fraud patterns.
- High false positives and low adaptability.

2. Traditional Machine Learning Models (SVM, Logistic Regression, Random Forest)

- Better than rule-based systems in pattern learning.
- Require heavy manual feature engineering.
- Struggle with highly imbalanced datasets.
- Limited ability to capture complex fraud behaviour.

3. Artificial Neural Networks (ANN)

- Automatically learn some non-linear patterns.
- Performance depends on good feature selection.
- Less effective in capturing advanced feature relationships.

4. Convolutional Neural Networks (CNN)

- Extract deep, meaningful features without manual engineering.
- Capture complex, hidden fraud patterns effectively.
- Higher accuracy, better recall, and robust performance.
- Suitable for large-scale and real-time fraud detection.

5. Hybrid Deep Learning Models (CNN + LSTM, CNN + Autoencoder)

- Combine spatial and temporal fraud pattern learning.
- Offer the highest detection accuracy and generalization.
- More computationally expensive and harder to train.

VII. CONCLUSION

Credit card fraud detection has become increasingly important as digital transactions continue to rise, bringing greater risks of financial loss and security threats. Traditional rule-based and machine learning methods, while useful in the past, are no longer sufficient to handle the complexity and constantly evolving nature of modern fraud activities. In contrast, Convolutional Neural Networks (CNNs) provide a powerful and intelligent approach by automatically extracting meaningful patterns from transaction data and identifying subtle irregularities that may indicate fraudulent behaviour. Their ability to learn complex non-linear relationships, handle large datasets, and reduce the need for manual feature engineering makes them highly efficient and adaptable for real-time fraud detection. Although challenges such as imbalanced data, computational requirements, and interpretability still exist, CNN-based models consistently demonstrate superior accuracy, faster response time, and improved generalization compared to earlier methods. Overall, the use of CNNs significantly enhances the reliability and effectiveness of fraud detection systems, offering a scalable and modern solution to protect financial institutions and customers from fraudulent activities.

REFERENCES

[1] 1. Books

1. Han, J., Kamber, M., & Pei, J. (2011). *Data Mining: Concepts and Techniques*. Morgan Kaufmann.
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
3. Aggarwal, C. C. (2015). *Data Mining: The Textbook*. Springer.

[2] 2. Research Papers and Articles

1. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). *Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy*. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.
2. Jurgovsky, J. et al. (2018). *Sequence Classification for Credit Card Fraud Detection Using Recurrent Neural Networks*. Expert Systems with Applications, 100, 234–245.

[3] Organizations and Websites

1. **IEEE Xplore Digital Library** – Research papers on fraud detection and neural networks: https://ieeexplore.ieee.org/
2. **SpringerLink** – Journals and book chapters on credit card fraud analytics: https://link.springer.com/

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

3. **Association for Computing Machinery (ACM)** – Articles on machine learning in finance: https://www.acm.org/
4. **Kaggle** – Public datasets for credit card fraud detection: https://www.kaggle.com/

[4] Tools and Models

1. **TensorFlow** – Deep learning framework for building CNN models.
2. **Keras** – High-level neural network API used for CNN experimentation.
3. **PyTorch** – Widely used framework for deep learning research and model development.
4. **Scikit-Learn** – Preprocessing, evaluation metrics, and classical ML comparisons.
5. **SMOTE (Synthetic Minority Oversampling Technique)** – Handling imbalanced fraud datasets.

[5] Journals

1. *Expert Systems with Applications*
2. *IEEE Transactions on Neural Networks and Learning Systems*
3. *Pattern Recognition Letters*
4. *Information Sciences*
5. *Journal of Financial Crime*