JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IDENTIFICATION OF CREDIT CARD FRAUDS USING MACHINE LEARNING AND DEEP LEARNING

Aravind.M[1, a)], CS Abhinay [2, b)] DS Prathamesh[3, c)] K. Naveen Kumar [4, d)] Sheetal Kundra [5, e)]

[1,2,3]Student, [4]Assistant Professor, [5]Professor & HOD,

[12345]Department of Artificial Intelligence and Data Science,

[12345]GURU NANAK INSTITUTE OF TECHNOLOGY, Ibrahimpatnam, Ranga Reddy ,501506, INDIA

Abstract:

The rapid proliferation of digital financial transactions has significantly escalated the risk of fraudulent activities, posing an increasingly serious challenge to financial security systems worldwide. Traditional fraud detection methods, typically reliant on rule-based systems and classical machine learning algorithms, often struggle to adapt to the constantly evolving tactics used by fraudsters. These legacy methods are especially inadequate in handling imbalanced datasets and learning from sequential transaction behaviour, leading to higher false positive rates and lower detection accuracy.

In this project, we present a robust and intelligent credit card fraud detection framework grounded in deep learning techniques, specifically utilizing Bidirectional Long Short-Term Memory (BiLSTM) networks. To establish a performance baseline and enable comparative analysis, we also employed traditional ensemble learning models, including Gradient Boosting, Random Forest, and Logistic Regression. While these models offer strong interpretability and generalization capabilities, their limitations in processing sequential data necessitated a more dynamic solution. The BiLSTM architecture, known for its capability to learn long-term dependencies in both forward and backward temporal directions, was implemented to effectively detect subtle anomalies in transaction sequences.

Preprocessing included data cleaning, feature scaling using StandardScaler, and reshaping to fit the sequential input format required by BiLSTM. The issue of class imbalance, a common characteristic in fraud detection datasets, was addressed through the use of under-sampling techniques to ensure better representation of minority class instances during training. Although SMOTE was initially considered, it was not included in the final model.

The model was built and trained using TensorFlow and Keras frameworks. Hyperparameter tuning was conducted through extensive experimentation to improve generalization and reduce overfitting. The final BiLSTM model achieved an outstanding accuracy of 99.96%, along with a macro average precision of 91.83%, recall of 99.98%, and F1-score of 95.54%. These results highlight the system's ability to outperform conventional fraud detection approaches.

Additionally, the trained model has been deployed through a user-accessible web platform featuring an integrated AI chatbot and AI Agent. This interface enables real-time fraud detection support, user interaction for credit-related inquiries, and ensures the system's scalability for real-world financial applications.

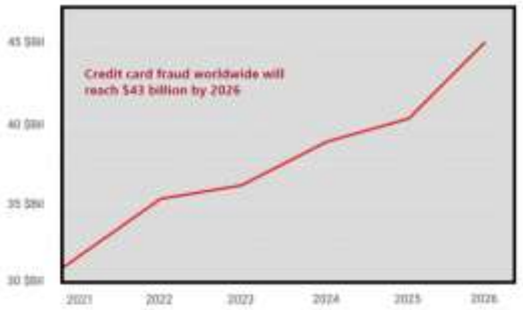
Keywords:

- Ensemble learning
- Gradient Boosting
- Random Forest
- Logistic Regression
- Bidirectional Long Short-Term Memory (BiLSTM)
- Sequential dependencies

- Under-sampling
- TensorFlow
- Keras
- AI Agent
- Web Deployment.

INTRODUCTION

With the rapid growth of the internet and digital banking, financial transactions have become more convenient but also increasingly vulnerable to fraud. Traditional fraud detection methods struggle to keep up with the massive volume of transactions, leading to inefficiencies. Machine learning and deep learning models offer a promising solution by detecting fraudulent transactions in real time. This project focuses on optimizing fraud detection using a sequential deep learning model, incorporating ensemble techniques and feature engineering. By enhancing accuracy and minimizing false positives, the proposed approach aims to strengthen financial security and improve fraud detection systems in modern banking environments.



EXISTING SYSTEM

Existing fraud detection systems typically rely on rule-based mechanisms and classical machine learning algorithms such as Decision Trees, Logistic Regression, and Support Vector Machines. While these models are relatively interpretable and easy to deploy, they often fall short in dealing with the complexities of real-world financial data.

One major limitation is their inability to effectively handle **imbalanced datasets**, where fraudulent transactions represent only a small fraction of total activity. This imbalance often results in biased predictions and poor recall for the minority class. Additionally, these systems suffer from high false positive rates, frequently misclassifying legitimate transactions as fraudulent, which can cause user dissatisfaction and operational inefficiencies.

Another critical drawback is the lack of adaptability to **emerging fraud tactics**. As fraudsters continuously evolve their strategies, static rule-based systems and traditional classifiers struggle to keep pace, reducing their overall effectiveness over time. Moreover, they lack the ability to capture **temporal dependencies** in transactional behaviour, which is crucial for identifying subtle patterns associated with fraudulent activity.

Key limitations include:

- Inability to adapt to evolving fraud techniques.
- Poor performance with highly imbalanced datasets.
- High false positive rates that hinder user trust.
- Lack of sequential learning capabilities to detect behaviour-based anomalies.

Another significant drawback is their static nature—these models often rely on predefined thresholds and manually crafted features, making it difficult for them to adapt to dynamic and evolving fraud tactics in real-time environments.

PROPOSED SYSTEM

To overcome the limitations of traditional fraud detection methods, the proposed system employs a deep learning-based architecture utilizing **Bidirectional Long Short-Term Memory (BiLSTM)** networks. This approach is specifically designed to capture temporal patterns and long-range dependencies in transaction sequences, enhancing the model’s ability to identify subtle and evolving fraudulent behaviour.

BiLSTM:

BiLSTM is an advanced type of Recurrent Neural Network (RNN) that processes sequence data in both forward and backward directions. This bidirectional learning captures past and future context for every transaction in a sequence, making it especially effective in identifying irregular transaction patterns. The LSTM units are equipped with memory cells and gates (input, forget, and output gates) that regulate the flow of information, thereby avoiding the vanishing gradient problem commonly found in traditional RNNs.

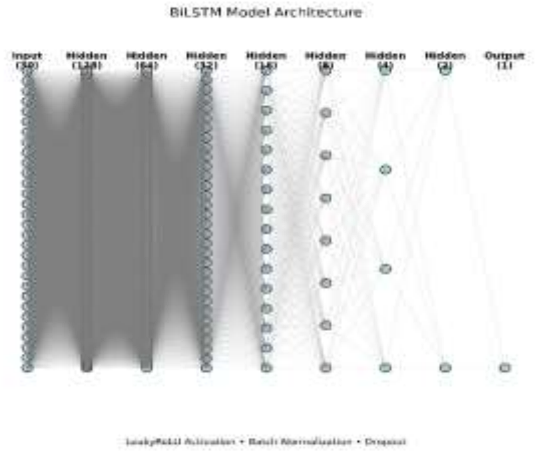
Max Pooling Layer:

Max pooling is used to reduce the dimensionality of feature maps and to retain the most important features. In our model, it follows the BiLSTM layers to summarize the most critical temporal features while reducing computational complexity.

Preprocessing Pipeline:

- **Data Cleaning**: Duplicate records and null values are removed to ensure data quality.
- **Feature Scaling**: StandardScaler is used to normalize the numerical features, which helps in faster and more stable model training.
- **Data Reshaping**: The transaction data is reshaped into 3D input format (samples, time steps, features) suitable for BiLSTM input.
- **Class Imbalance Handling**: Due to the rarity of fraudulent transactions, **under-sampling** is applied to balance the dataset. SMOTE was considered but not implemented.

MODEL ARCHITECTURE



The model is constructed using the Sequential API from TensorFlow and Keras, including:

- Stacked BiLSTM layers for learning bidirectional temporal dependencies
- Dropout layers to prevent overfitting
- Max Pooling layer for dimensionality reduction
- Dense output layer with sigmoid activation for binary classification

Training Parameters:

- **Loss Function**: Binary Cross-Entropy, suitable for two-class classification
- **Optimizer**: Adam, chosen for its efficiency and adaptive learning rate
- **Metrics**: Precision, Recall, F1-score, Accuracy, AUC

Performance and Deployment:

The trained model achieves 99.96% accuracy and is integrated into a web-based platform. This includes a chatbot and AI-powered credit assistant that enables real-time fraud detection, user engagement, and transaction monitoring.

The integration of BiLSTM with effective preprocessing and deployment techniques makes this system scalable, accurate, and practical for real-world financial applications.

Key Features of the Proposed System

- BiLSTM Network: Captures long-range temporal dependencies by processing transaction sequences in both forward and backward directions, enabling detection of subtle, sequence-based fraud patterns.
- Max Pooling Layer: Following BiLSTM, max pooling reduces feature dimensionality and retains the most salient temporal signals, improving computational efficiency without sacrificing detection capability.
- Data Preprocessing: Includes removal of duplicates and null values, normalization of numerical features using StandardScaler, and reshaping into a 3D tensor (samples, time steps, features) suitable for sequence modelling.
- Class Imbalance Handling: Uses under-sampling of the majority (legitimate) class to balance the dataset, ensuring that the model learns effectively from minority (fraud) examples. SMOTE was considered but not implemented.
- Dropout Regularization: Dropout layers are interleaved with BiLSTM to prevent overfitting by randomly deactivating neurons during training, which improves model generalization.
- Training & Optimization: Trained with binary cross-entropy loss and the Adam optimizer, with performance monitored via precision, recall, F1-score, accuracy, and AUC metrics. Hyperparameter tuning was performed to fine-tune layer sizes, dropout rates, and learning rate.
- Web-Based Deployment: The final model is deployed on a web platform featuring an AI-powered chatbot and virtual assistant, allowing real-time fraud alerts, transaction monitoring, and user support.
- Scalability & Real-Time Suitability: Architected for low-latency inference and horizontal scalability, enabling integration into production financial systems for continuous, real-time fraud detection.

Machine Learning and Deep Learning Processes Used

1. Data Preprocessing:
    - Removing duplicates and null values.
    - Normalizing features with StandardScaler.
    - Reshaping data into (samples, 1, features) for BiLSTM input.
    - Under-sampling to address class imbalance.
2. Deep Learning Model:

  - BiLSTM Layers: Two stacked BiLSTM layers to capture bidirectional temporal dependencies.
  - Max Pooling: Summarizes salient features from BiLSTM output.
  - Dropout Layers: Applied after each BiLSTM block for regularization.
  - Dense Output Layer: Sigmoid activation for binary fraud classification.

3. Training & Validation
   - Loss: Binary cross-entropy.
   - Optimizer: Adam with adaptive learning rate.
   - Callbacks: Early Stopping and Model Checkpoint to prevent overfitting and save best model.
   - Metrics: Accuracy, precision, recall, F1-score, AUC.
4. Deployment
   - Model exported and served via a RESTful API.
   - Integrated with a chatbot interface for user queries and real-time fraud notifications.

- Data Preprocessing: Data cleaning, standardization, and reshaping.
- Model Training: Using BiLSTM with Keras and TensorFlow.
- Evaluation: Metrics such as accuracy (99.96%), macro average precision (91.83%), recall (99.98%), and F1-score (95.54%) validate the system's effectiveness.
- Deployment: The trained model is deployed on a web-based interface accessible to users for fraud detection support.

Dataset Description

For training and evaluating our fraud detection model, we leveraged two publicly available credit card transaction datasets to ensure robustness and diversity in real-world scenarios.

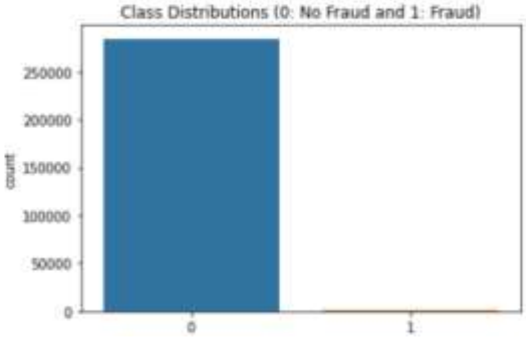
Dataset 1: European Credit Card Transactions

- Contains 284,807 transactions recorded over two days by European cardholders.
- Highly imbalanced: only 492 fraudulent transactions (0.172% of total).
- Features: 30 numerical features, including 28 anonymized principal components (V1–V28) obtained via PCA, plus two non-anonymized fields:
  - **Time**: seconds elapsed since the first recorded transaction.
  - **Amount**: monetary value of the transaction.
- Target label: **Class** (0 = legitimate, 1 = fraudulent).

Dataset 2: 2023 Credit Card Transactions

- Over 550,000 transactions conducted by European cardholders throughout 2023.
- Fully anonymized to protect cardholder identities.
- Key fields:
  - **id**: unique transaction identifier.
  - **V1–V28**: anonymized transaction attributes.
  - **Amount**: transaction amount.
  - **Class**: binary fraud label (0 or 1).
- Similarly imbalanced, with fraudulent cases constituting a small fraction of total transactions.

By combining these two datasets, our model is exposed to a broad spectrum of transaction behaviours and fraud patterns, improving its ability to generalize across different time periods and operational environments. Both datasets underwent identical preprocessing steps: data cleaning, feature scaling with StandardScaler, reshaping for BiLSTM input, and under-sampling to address class imbalance.



METHODOLOGY

This study employs a systematic approach to develop a deep learning-based credit card fraud detection system. The system integrates Bidirectional Long Short-Term Memory (BiLSTM) networks for temporal anomaly detection and leverages preprocessing, hyperparameter optimization, and evaluation strategies to achieve high accuracy.

1. **Dataset Selection and Preprocessing:**
   - **Datasets Used**:
     - Credit Card Fraud Detection Dataset (European Transactions) (284,807 transactions)
     - Credit Card Fraud Detection Dataset 2023 (550,000+ transactions)

These datasets are imbalanced, with fraudulent transactions being a very small percentage of the total.

  - **Data Cleaning:**

Removed duplicate transactions and missing values to ensure clean and high-quality data.

- **Feature Scaling:**
Applied StandardScaler for normalizing numerical features to ensure all features have similar scale, aiding model convergence.
- **Data Reshaping:**
Reshaped transaction data into a 3D format (samples, timesteps, features) to be compatible with the BiLSTM model.
- **Class Imbalance Handling:**
Utilized under-sampling to balance the classes. Although SMOTE was considered, it was not implemented in the final model.

2. Model Architecture:

- BiLSTM Network:
  - ▪ Captures both past and future dependencies in sequential transaction data, making it effective for detecting complex fraud patterns.
  - ▪ Equipped with memory cells and gates (input, forget, and output) to regulate information flow, mitigating the vanishing gradient problem.
- **Max Pooling Layer:**
After the BiLSTM layer, max pooling is applied to reduce dimensionality, retaining the most significant features and improving computational efficiency.
- **Dense Layer:**
A Dense output layer with a sigmoid activation function is used for binary classification (fraudulent or legitimate).

3. Training and Optimization:

- **Loss Function:**
Used Binary Cross-Entropy for binary classification.
- **Optimizer:**
Chose the Adam optimizer, known for its adaptive learning rate and efficiency in deep learning.
- **Hyperparameter Tuning:**
Conducted hyperparameter optimization using Grid Search Cross-Validation to find the best parameters for the model.
- **Dropout Layers:**
Included dropout layers to prevent overfitting, ensuring the model generalizes well across unseen data.

4. Model Evaluation:

- **Performance Metrics:**
Evaluated model performance using accuracy, precision, recall, F1-score, and AUC (Area Under the Curve).
- The final model achieved 99.96% accuracy and demonstrated the effectiveness of BiLSTM in fraud detection.

5. Deployment:

- **Web Platform:**
The trained model was integrated into a web-based platform featuring an AI-powered chatbot and virtual assistant for real-time fraud detection and user support.

Key Features of the Proposed System

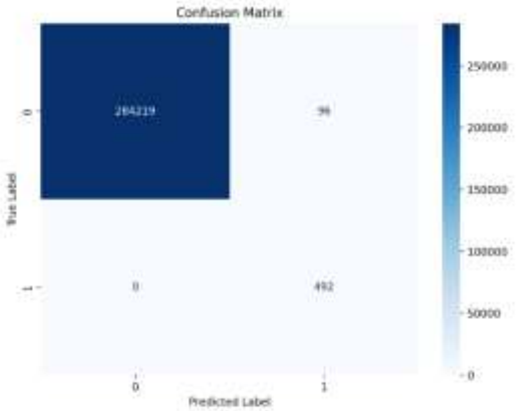
- BiLSTM Network: Effective at learning both past and future dependencies in sequential data.
- Data Preprocessing: Includes cleaning, scaling, reshaping, and balancing techniques.
- Imbalanced Data Handling: Utilizes under-sampling to balance the dataset, enhancing model robustness.
- Evaluation: Performance tracked through precision, recall, F1-score, accuracy, and AUC.
- Deployment: Integrated into a user-accessible platform with real-time support via AI assistant

RESULTS

The BiLSTM-based model demonstrated the following performance:

- Accuracy: 99.96%
- Macro Avg. Precision: 91.83%
- Macro Avg. Recall: 99.98%
- Macro Avg. F1-Score: 95.54%
- Weighted Avg. F1-Score: 99.97%

Confusion Matrix



CONCLUSION

This project establishes a comprehensive and intelligent approach to credit card fraud detection by integrating deep learning techniques, specifically BiLSTM networks, with robust preprocessing and deployment strategies. As fraudulent activities continue to rise in digital financial ecosystems, traditional methods have proven insufficient due to their static nature, inability to handle sequential patterns, and poor performance on imbalanced datasets.

By addressing these limitations, the proposed system significantly improves fraud detection accuracy through careful feature scaling, sequence modelling, and handling of class imbalance using under-sampling. Although traditional ensemble techniques like Gradient Boosting and Random Forest were considered for baseline comparisons, the BiLSTM model outperformed them in capturing temporal dependencies and reducing false positives.

The finalized model, trained using TensorFlow and Keras with binary cross-entropy loss and the Adam optimizer, achieved an accuracy of 99.96%, along with a macro average precision of 91.83% and F1-score of 95.54%. These results validate the effectiveness of deep learning in this domain.

Furthermore, the deployment of the trained model on a web-based platform—enhanced with a virtual AI assistant and chatbot—makes the system both scalable and user-centric. This integration allows real-time fraud detection support and offers a practical, interactive solution for modern banking infrastructure.

In summary, this study demonstrates the powerful synergy between deep learning and real-time deployment tools in developing reliable fraud detection systems. Future work may explore the addition of explainable AI and reinforcement learning to further elevate the model’s interpretability and adaptability.

REFERENCES

[1] A. Rb and S. K. Kr, ‘‘Credit card fraud detection using artificial neural network,’’ Global Transitions Proc., vol. 2, no. 1, pp. 35–41, Jun. 2021.

[2] M. C. Consulting. (2024). Credit Card Fraud Statistics (2024). Accessed: Jun. 28, 2024. [Online].

[3] H. D. Nayak, Deekshita, L. Anvitha, A. Shetty, D. J. Dsouza, and M. P. Abraham, ‘‘Fraud detection in online transactions using machine learning approaches—A review,’’ in Proc. Adv. Artif. Intell. Data Eng., 2019, pp. 589–599.

[4] A. Kannagi, J. Gori Mohammed, S. Sabari Giri Murugan, and M. Varsha, ‘‘Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbour algorithm for cloud security applications,’’ Mater. Today, Proc., vol. 81, pp. 745–749, Aug. 2023.

[5] T. Riasanow, R. J. Flötgen, D. S. Setzke, M. Böhm, and H. Krcmar, ‘‘The generic ecosystem and innovation patterns of the digital transformation in the financial industry,’’ in Proc. Pacific Asia Conf. Inf. Syst., 2018, pp. 1–20.

[6] B. Nikkel, ‘‘Fintech forensics: Criminal investigation and digital evidence in financial technologies,’’ Forensic Sci. Int. Digit. Invest., vol. 33, Jun. 2020, Art. no. 200908.

[7] B. Brandl and L. Hornuf, ‘‘Where did fintechs come from, and where do they go? The transformation of the financial industry in Germany after digitalization,’’ SSRN Electron. J., p. 8, 2020.

[8] S. Chanias, M. D. Myers, and T. Hess, ‘‘Digital transformation strategy making in pre-digital organizations: The case of a financial services provider,’’ J. Strategic Inf. Syst., vol. 28, no. 1, pp. 17–33, Mar. 2019.

[9] P. Pashkov and V. Pelykh, ‘‘Digital transformation of financial services on the basis of trust,’’ in Economic and Social Development: Book of Proceedings. Varaždin, Croatia: Varazdin Development and Entrepreneurship Agency, 2020, pp. 375–383.

[10] I. M. Sebastian, J. W. Ross, C. Beath, M. Mocker, K. G. Moloney, and N. O. Fonstad, ‘‘How big old companies navigate digital transformation,’’ in Strategic Information Management. Evanston, IL, USA: Routledge, 2020, pp. 133–150.

[11] L. Zheng, G. Liu, C. Yan, and C. Jiang, ‘‘Transaction fraud detection based on total order relation and behavior diversity,’’ IEEE Trans. Computat. Social Syst., vol. 5, no. 3, pp. 796–806, Sep. 2018.

[12] Z. Zhang, X. Zhou, X. Zhang, L. Wang, and P. Wang, ‘‘A model based on convolutional neural network for online transaction fraud detection,’’ Secur. Commun. Netw., vol. 2018, pp. 1–9, Aug. 2018.

[13] S. Cao, X. Yang, C. Chen, J. Zhou, X. Li, and Y. Qi, ‘‘TitAnt: Online real time transaction fraud detection in ant financial,’’ 2019, arXiv:1906.07407.

[14] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, ‘‘Random Forest for credit card fraud detection,’’ in Proc. IEEE 15th Int. Conf. Netw., Sens. Control (ICNSC), Mar. 2018, pp. 1–6.

[15] Z. Zhang, L. Chen, Q. Liu, and P. Wang, ‘‘A fraud detection method for low-frequency transaction,’’ IEEE Access, vol. 8, pp. 25210–25220, 2020.

[16] S. Khatri, A. Arora, and A. P. Agrawal, ‘‘Supervised machine learning algorithms for credit card fraud detection: A comparison,’’ in Proc. 10th Int. Conf. Cloud Compute., Data Sci. Eng. (Confluence), Jan. 2020, pp. 680–683.