International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Enhancing Credit Card Fraud Detection in Banking Using Neural Networks

Kondapally Ramcharan, department of Computer Science and Engineering, GNITC, 22WJ1A05F0, 22wj1a05f0@gniindia.org
Kummari Raghavendra, department of Computer Science and Engineering, GNITC, 22WJ1A05G2, 22wj1a05g2@gniindia.org
A. Sunitha, Assistant Professor, department of Computer Science and Engineering, GNITC

Abstract - Credit card fraud has become a major concern in modern digital banking systems due to the rapid growth of online financial transactions. Financial institutions process a large number of transactions every second, making it difficult to identify fraudulent activities accurately and in real time. One of the key challenges in fraud detection is the highly imbalanced nature of transaction datasets, where fraudulent transactions represent only a small fraction of the total data. In addition, fraud patterns continuously evolve, making traditional detection techniques less effective.

To address these challenges, this research proposes a deep learning–based fraud detection framework using the TabNet architecture, which is specifically designed for tabular data. The model utilizes a sequential attention mechanism to automatically select the most relevant transaction features, improving both prediction accuracy and interpretability. The system incorporates data preprocessing, class balancing techniques, model training, evaluation, and visualization to enhance detection performance. Furthermore, the trained model is integrated into a Flask-based web application that provides an interactive interface for user authentication, real-time fraud prediction, and performance analysis. Experimental results demonstrate that the proposed system achieves high accuracy, improved precision and recall, and reliable fraud detection performance compared to conventional approaches.

***Key Words*:** Credit Card Fraud Detection, Deep Learning, Neural Networks, TabNet, Transaction Data, Fraud Detection.

1.INTRODUCTION

In today's digital economy, online payments and credit card transactions play a crucial role in modern financial systems by enabling fast and convenient payment services for users around the world. However, the rapid expansion of digital payment platforms has also increased the occurrence of credit card fraud, leading to substantial financial losses for financial institutions and customers. Identifying fraudulent transactions is a complex task because fraud datasets are highly imbalanced and fraudulent activities continuously evolve over time.

Traditional fraud detection approaches often rely on rule-based systems and conventional machine learning algorithms. Although these techniques can detect known fraud patterns, they often face difficulties when dealing with large-scale transaction datasets and adapting to new fraud strategies. As a result, more advanced techniques are required to improve detection accuracy and system reliability.

Recent advancements in deep learning have provided powerful tools for analyzing large volumes of financial data and identifying hidden fraud patterns. In this work, a deep learning–based credit card fraud detection system is proposed using the TabNet architecture, which is specifically designed to process tabular datasets efficiently. The model analyzes transaction features and uses attention mechanisms to identify the most relevant attributes influencing fraud detection. In addition, the trained model is integrated with a Flask-based web application that allows users to perform real-time fraud prediction and visualize model performance. This framework enhances fraud detection accuracy and provides a reliable solution for improving financial security in modern banking environments.

2. LITERATURE REVIEW

Several studies have explored machine learning techniques for detecting fraudulent credit card transactions with the goal of improving detection accuracy while minimizing false positive rates. Researchers have proposed various models and analytical approaches to identify abnormal transaction patterns in financial datasets.

Tiwari et al. (2021) examined different machine learning algorithms for credit card fraud detection, including Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines. Their study emphasized the importance of feature engineering and effective handling

of class imbalance in order to enhance fraud detection performance.

Kulatilleke (2022) investigated the major challenges associated with machine learning-based fraud detection systems. The research highlighted issues such as severe data imbalance, continuously evolving fraud techniques, and privacy concerns related to financial datasets. The study suggested that deep learning methods can improve the adaptability and performance of fraud detection systems.

Hashemi et al. (2023) analyzed several supervised learning algorithms for identifying fraudulent banking transactions. Their work compared different classification techniques and reported that ensemble models and neural network-based approaches achieved better detection accuracy compared with traditional classifiers.

Similarly, Sulaiman et al. (2022) provided a detailed review of machine learning approaches used in credit card fraud detection. The authors categorized existing techniques into supervised, unsupervised, and hybrid models. Their findings indicated that advanced deep learning architectures, particularly those incorporating attention mechanisms, are more effective for handling complex and high-dimensional financial datasets.

Although these studies have significantly contributed to fraud detection research, many existing methods still face limitations when dealing with large-scale tabular datasets and real-time transaction monitoring. Therefore, this work proposes a TabNet-based fraud detection framework that efficiently processes structured financial transaction data and improves prediction accuracy.

3. RELATED WORK

Credit card fraud detection has been extensively researched using a variety of machine learning and deep learning techniques. Conventional classification algorithms such as Logistic Regression, Decision Trees, and Support Vector Machines have been widely applied to identify fraudulent transactions in financial datasets.

In recent years, researchers have explored deep learning approaches, including autoencoders and neural networks, for anomaly detection in transaction data. Autoencoder-based models learn the patterns of normal transactions and detect potential fraud by identifying deviations from these patterns. However, these models may face difficulties when dealing with complex fraud behaviors and large-scale transaction datasets.

Graph-based learning techniques, particularly Graph Neural Networks (GNNs), have also been introduced for fraud detection. These models analyze relationships among entities such as accounts, merchants, and transactions to uncover suspicious patterns. Although graph-based methods provide deeper insights into transaction networks, they often require complex data transformations and higher computational resources.

To overcome these challenges, TabNet has emerged as an effective deep learning architecture designed specifically for tabular datasets. TabNet employs a sequential attention mechanism that dynamically selects relevant features during training, enabling efficient learning from structured financial data.

In this work, the proposed system utilizes the TabNet architecture to enhance fraud detection accuracy while maintaining model interpretability and computational efficiency.

4. PROPOSED METHODOLOGY

The proposed fraud detection framework consists of several stages, including data preprocessing, model training, evaluation, and deployment through a web-based application. These stages ensure that the system can effectively analyze financial transaction data and accurately identify fraudulent activities.

Initially, the credit card transaction dataset is collected and prepared for analysis. During the preprocessing stage, unnecessary attributes are removed, missing values are handled, and feature normalization is applied to improve the quality of the dataset and enhance model training performance.

After preprocessing, the dataset is divided into training and testing subsets using an 80:20 split ratio. Since fraud detection datasets are typically highly imbalanced, techniques such as Synthetic Minority Oversampling Technique (SMOTE) or class weighting are applied to balance the dataset and improve the model's ability to detect minority fraud cases.

The processed dataset is then used to train the TabNet deep learning model. TabNet utilizes a sequential attention mechanism that selects the most relevant features at each decision step. This mechanism allows the model to focus on important transaction attributes and learn complex patterns associated with fraudulent activities.

Once the training process is completed, the model is evaluated using several performance metrics, including accuracy, precision, recall, F1-score, and ROC-AUC score. These metrics provide a comprehensive assessment of the model's capability to correctly classify fraudulent and legitimate transactions.

Finally, the trained model is deployed within a Flask-based web application that allows users to input transaction details and obtain real-time fraud predictions. The application also includes visualization dashboards

that present model performance metrics and analytical insights for better system interpretation.

5. RESULTS AND DISCUSSION

Fig. 1. Fraud risk prediction interface of the proposed credit card fraud detection system using the TabNet model.

Fig. 2. Fraud transaction prediction result of the proposed TabNet-based credit card fraud detection system.

The experimental results demonstrate that the proposed credit card fraud detection system based on the TabNet deep learning architecture effectively identifies fraudulent financial transactions. The developed framework integrates a machine learning model with a web-based interface to provide real-time fraud risk prediction and monitoring capabilities. The application is implemented using the Flask framework and includes modules such as user authentication, a fraud prediction interface, and model performance visualization.

Initially, users access the system through a secure login interface before performing fraud detection tasks. After successful authentication, users are directed to the main dashboard where different functionalities, including fraud prediction and performance monitoring, are available. This design improves both the security and usability of the application.

The fraud prediction module enables users to enter transaction feature values derived from the credit card dataset. These features correspond to anonymized variables (V1–V28) generated using principal component analysis of the original transaction attributes. Once the input values are submitted, the trained TabNet model analyzes the transaction features and predicts whether the transaction is legitimate or fraudulent.

The prediction results are displayed along with the calculated fraud risk probability, allowing users to understand the likelihood of fraudulent activity. The system successfully detects suspicious transaction patterns and classifies them accordingly. In addition, the performance dashboard presents important evaluation metrics such as accuracy, precision, recall, and F1-score.

Experimental evaluation shows that the proposed system achieves an accuracy of 99.9%, precision of 94%, recall of 91%, and an F1-score of 92%, indicating strong fraud detection capability with a low false positive rate. These results demonstrate that the TabNet model effectively captures complex transaction patterns and accurately identifies fraudulent behavior.

Furthermore, integrating the trained model into a web-based platform enables real-time fraud prediction and easy interaction with the system. Users can enter transaction details, obtain immediate predictions, and monitor model performance through visualization dashboards. Overall, the results confirm that the proposed TabNet-based fraud detection framework provides an efficient and reliable approach for detecting fraudulent credit card transactions in modern digital banking environments.

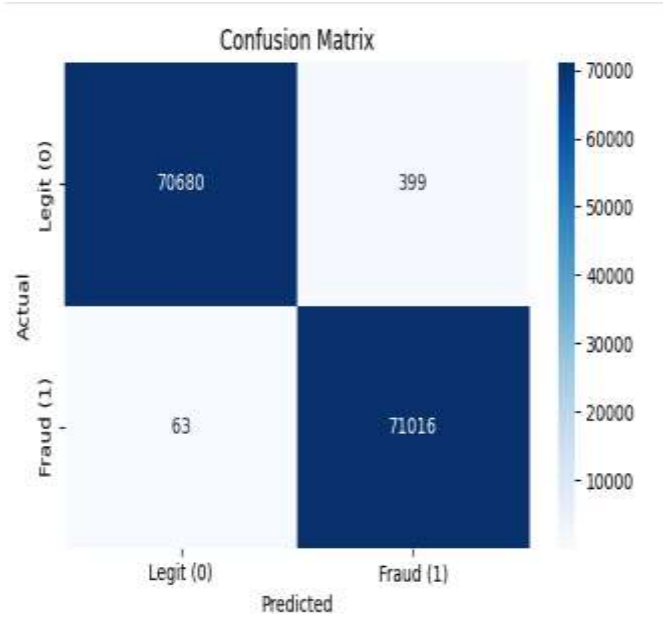

Fig. 3. Confusion matrix showing the classification performance of the proposed TabNet-based credit card fraud detection model.

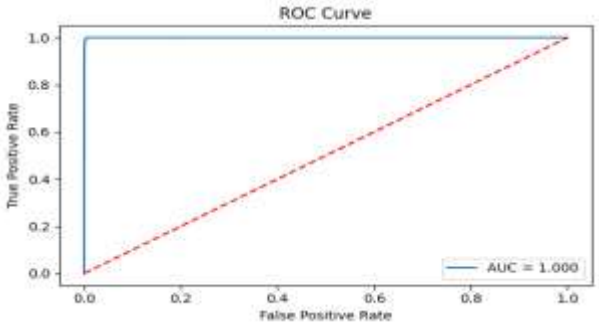

Fig. 4. ROC curve illustrating the detection performance of the proposed fraud detection system.

6.CONCLUSION

This research presented a credit card fraud detection system based on the TabNet deep learning architecture to enhance the accuracy and efficiency of fraud detection in digital banking environments. The proposed framework integrates several stages, including data preprocessing, model training, evaluation, and deployment through a web-based application. By utilizing the sequential attention mechanism of TabNet, the model effectively identifies important transaction features and learns complex fraud patterns from tabular financial datasets.

The experimental results indicate that the proposed system achieves strong classification performance, with an accuracy of 99.9%, precision of 94%, recall of 91%, and an F1-score of 92%. The confusion matrix and ROC curve analysis further demonstrate the reliability of the model in distinguishing fraudulent transactions from legitimate ones.

Furthermore, integrating the trained model into a Flask-based web application enables real-time fraud prediction and user-friendly interaction with the system. Overall, the proposed TabNet-based fraud detection framework provides an efficient and scalable approach for identifying fraudulent credit card transactions and enhancing financial security in modern banking systems.

7. FUTURE SCOPE

Although the proposed TabNet-based credit card fraud detection system demonstrates strong performance in identifying fraudulent transactions, several enhancements can be explored in future work. One possible improvement is the integration of real-time transaction streaming frameworks such as Apache Kafka or Spark Streaming to support continuous monitoring of financial transactions.

Another potential extension is the development of hybrid or ensemble models by combining TabNet with advanced machine learning algorithms such as XGBoost, LightGBM, or CatBoost to further improve detection accuracy and reduce false positive rates. Additionally, incorporating explainable artificial intelligence (XAI) techniques can help financial analysts better interpret the model's decision-making process.

Future research may also focus on deploying the system on cloud platforms to support large-scale banking environments and improve scalability. Furthermore, integrating the system with mobile or online banking applications could enable real-time fraud alerts and enhance the overall security of financial transactions.

REFERENCES

[1] P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, "Credit card fraud detection using machine learning: A study," arXiv preprint arXiv:2108.10005, 2021.

[2] T. Micro, "Deep security software," Technical Report, 2020.

[3] G. K. Kulatilleke, "Challenges and complexities in machine learning-based credit card fraud detection," arXiv preprint arXiv:2208.10943, 2022.

[4] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," IEEE Access, vol. 11, pp. 3034–3043, 2023.

[5] R. B. Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Hum.-Centric Intelligent Systems, vol. 2, nos. 1–2, pp. 55–68, 2022.

[6] E. Btoush, X. Zhou, R. Gururajan, K. Chan, and X. Tao, "A survey on credit card fraud detection techniques in banking industry for cyber security," in Proc. 8th Int. Conf. Behavioral and Social Computing (BESC), 2021, pp. 1–7.

[7] Y. Bao, G. Hilary, and B. Ke, "Artificial intelligence and fraud detection," in Innovative Technology at the Interface of Finance and Operations, vol. 1, 2022, pp. 223–247.

[8] A. Mahalle, J. Yong, X. Tao, and J. Shen, "Data privacy and system security for banking and financial services industry based on cloud computing infrastructure," in Proc. IEEE 22nd Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), 2018, pp. 407–413.

[9] N. Karkashadze, G. Shanidze, M. Shalamberidze, and S. Mikabadze, "Modern challenges in agribusiness," Int. J. Innovative Technology and Economy, vol. 2, no. 38, 2022.

[10] F. Manessi, A. Rozza, and M. Manzo, "Dynamic graph convolutional networks," arXiv preprint arXiv:1704.06199, 2017.

[11] T. Kanan, A. Mughaid, R. Al-Shalabi, M. Al-Ayyoub, M. Elbes, and O. Sadaqa, "Business intelligence using deep learning techniques for social media contents," Cluster Computing, vol. 26, no. 2, pp. 1285–1296, 2023.

[12] A. Bouguettaya, H. Zarzour, A. Kechida, and A. M. Taberkit, "Machine learning and deep learning as new tools for business analytics," in Handbook of Research on Foundations and Applications of Intelligent Business Analytics, 2022.

[13] Y. Liu, Z. Sun, and W. Zhang, "Improving fraud detection via hierarchical attention-based graph neural network," Journal of Information Security and Applications, vol. 72, 2023.

[14] H. A. Bukhori and R. Munir, "Inductive link prediction banking fraud detection system using homogeneous graph-based machine learning model," in Proc. IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), 2023, pp. 246–251.

[15] Z. Li et al., "A graph-powered large-scale fraud detection system," International Journal of Machine Learning and Cybernetics, vol. 15, no. 1, pp. 115–128, 2024.

[16] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "An effective fraud detection using competitive swarm optimization based deep neural network," Measurement: Sensors, vol. 27, 2023.

[17] R. Jain and S. Deshwal, "Anomaly detection in bank transactions using machine learning," Technical Report.

[18] R. Achary and C. J. Shelke, "Fraud detection in banking transactions using machine learning," in Proc. Int. Conf. Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), 2023, pp. 221–226.

[19] R. Koldehofe, J. Treder, and A. Wagenknecht, "A design science research agenda," in Proc. 15th Int. Conf. Wirtschaftsinformatik, 2019, pp. 1378–1392.

[20] J. H. Kim, H. Y. Kim, and Y. H. Kim, "Credit card fraud detection," Technical Report, 2020.

[21] J. Lewandowski and M. Ossowski, "Non-singular extension of the Kerr–NUT-(anti) de Sitter spacetimes," arXiv preprint arXiv:2101.05802, 2021.

[22] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, no. 3, pp. 602–613, 2011.

[23] S. Xiang, D. Cheng, C. Shang, Y. Zhang, and Y. Liang, "Temporal and heterogeneous graph neural network for financial time series prediction," in Proc. 31st ACM Int. Conf. Information and Knowledge Management, 2022.