



International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)



**ijerst.editor@gmail.com
editor@ijerst.com**

Research Paper

ENHANCING CREDIT CARD FRAUD DETECTION IN BANKING USING NEURAL NETWORKS

G Srividhya¹, Dr. S Siva Sankara Rao²

¹Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.

²Associate Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.

Abstract: Credit card fraud has emerged as one of the most significant challenges faced by financial institutions due to the rapid growth of digital banking and online transactions. Traditional machine learning algorithms often struggle to maintain high detection accuracy while minimizing false positives, particularly in highly imbalanced transaction datasets. This paper proposes an interpretable deep learning framework based on the TabNet architecture for enhancing credit card fraud detection in banking systems. Unlike conventional neural networks, TabNet employs sequential attention mechanisms to perform feature selection dynamically, enabling superior learning from structured tabular transaction data while providing model interpretability. The proposed methodology includes comprehensive data preprocessing, missing value handling, feature scaling, class imbalance correction using SMOTE, and hyperparameter optimization. Experimental evaluation is conducted on the publicly available European Credit Card Fraud Detection dataset. Performance is evaluated using Accuracy, Precision, Recall, F1-score, ROC-AUC, PR-AUC, and Matthews Correlation Coefficient (MCC). Experimental results demonstrate that TabNet outperforms traditional neural networks and popular machine learning algorithms by achieving high fraud detection accuracy with significantly reduced false alarms while maintaining excellent interpretability suitable for financial regulatory requirements. Recent studies have similarly reported strong performance of TabNet for banking fraud detection, highlighting its suitability for structured financial datasets and explainable AI applications.

Keywords: Credit Card Fraud Detection, TabNet, Deep Learning, Neural Networks, Explainable AI, Banking Security, Financial Fraud, SMOTE.

1. INTRODUCTION

With thousands of transactions happening every second in today's digital banking systems, credit card fraud is one of the biggest risks. The significant imbalance between legal and fraudulent records and the dynamic nature of fraud trends make it difficult to identify fraudulent transactions in real time. The TabNet model, which effectively manages large-scale, high-dimensional tabular transaction data, is used in this project to construct a deep learning-based fraud detection system. Using sequential attention, the model learns to concentrate on the most crucial aspects of each transaction, attaining high recall and precision while reducing false alarms. Advanced pre-processing, balanced data handling, model training, assessment, and visualisation are all integrated into the system. Lastly, an interactive user interface with modules for registration, login, real-time prediction, and visual analytics of model performance is developed using a Flask-based web application. Compared to conventional methods, the suggested system provides superior accuracy, quicker inference, and strong fraud detection capabilities..

Online and card-based transactions have formed the foundation of financial systems in the modern digital economy, providing millions of users worldwide with speed and ease. But this quick expansion has also resulted in a substantial rise in fraudulent activity, which puts both banks and clients at serious danger. Large-scale, high-dimensional data and changing fraud trends are difficult for traditional fraud detection algorithms to adapt to since they frequently rely on rule-based or conventional machine learning techniques. This study uses the TabNet model, a specialised neural network architecture created for tabular information, to present an advanced deep learning approach in order to overcome these issues. In order to determine the most significant transaction attributes while preserving interpretability and computing performance, TabNet uses sequential attention. Transactional data is processed, the TabNet model is trained to identify anomalies, and high-accuracy predictions that differentiate between fraudulent and legitimate transactions are produced. Real-time fraud prediction, feature importance

visualisation, and model performance statistics are made possible by the integration of an intuitive Flask web application. This project shows how deep learning-based solutions, such as TabNet, may greatly increase the overall dependability, decrease false positives, and improve accuracy of fraud detection systems in financial institutions.

2. LITERATURE SURVEY

Credit card fraud has become one of the fastest-growing financial crimes due to the rapid adoption of digital banking, e-commerce, contactless payments, and online financial services. Traditional rule-based

fraud detection systems suffer from limited adaptability and require continuous manual updates to recognize new fraud patterns. Consequently, machine learning (ML) and deep learning (DL) models have emerged as powerful alternatives capable of learning complex transaction behaviors from historical banking data. Recent advances in deep learning for tabular data, particularly **TabNet**, have demonstrated superior performance by combining neural networks with an interpretable attention mechanism, making them highly suitable for banking fraud detection.

S.No	Authors	Year	Methodology / Model	Dataset	Key Findings	Limitations
1	Arik & Pfister	2021	TabNet Deep Learning Architecture	UCI Adult, Forest CoverType, Higgs	Introduced TabNet with sequential attention for interpretable tabular data learning, outperforming several gradient boosting methods while maintaining explainability.	Not evaluated specifically for credit card fraud detection.
2	Roy et al.	2023	TabNet with SMOTE	European Credit Card Fraud Dataset	Achieved improved fraud detection by handling class imbalance and learning complex feature interactions.	Increased training time due to oversampling.
3	Chen et al.	2022	XGBoost + Neural Network	IEEE-CIS Fraud Detection Dataset	Hybrid learning improved fraud classification accuracy and reduced false positives.	Model lacks interpretability and requires extensive hyperparameter tuning.
4	Kumar & Singh	2024	TabNet with Feature Attention	Kaggle Credit Card Fraud Dataset	TabNet automatically selected important transaction features, improving fraud detection precision and recall.	Performance depends on optimal parameter initialization.
5	Li et al.	2023	Deep Neural Network (DNN)	European Credit Card Transactions	DNN effectively captured nonlinear relationships and achieved high AUC scores.	Susceptible to overfitting on highly imbalanced datasets.
6	Ahmed et al.	2024	CNN-LSTM Hybrid Model	IEEE-CIS Dataset	Combined spatial and temporal learning for sequential transaction analysis, improving fraud prediction.	High computational complexity and training cost.
7	Patel et al.	2023	Autoencoder + Neural Network	Kaggle Credit Card Dataset	Autoencoder successfully detected anomalous transactions before classification.	Reconstruction threshold selection affects performance.
8	Wang et al.	2022	Graph Neural Network (GNN)	Financial Transaction Network	Captured relationships among transaction entities, significantly improving fraud identification.	Requires graph construction and high memory consumption.

S.No	Authors	Year	Methodology / Model	Dataset	Key Findings	Limitations
9	Sharma et al.	2024	TabNet + Focal Loss	European Credit Card Dataset	Improved minority fraud class prediction with enhanced recall and reduced false negatives.	Requires careful tuning of focal loss parameters.
10	Zhao et al.	2023	LightGBM vs TabNet	IEEE-CIS Fraud Dataset	TabNet demonstrated better interpretability while achieving competitive classification accuracy compared to LightGBM.	Training time higher than tree-based models.
11	Hassan et al.	2024	TabNet with Explainable AI (SHAP)	Banking Transaction Dataset	Combined TabNet attention mechanism and SHAP explanations to improve trustworthiness in fraud detection.	SHAP explanation increases computational overhead.
12	Verma & Gupta	2025	Ensemble of TabNet and XGBoost	Kaggle Credit Card Fraud Dataset	Ensemble achieved superior precision, recall, F1-score, and ROC-AUC compared with individual models.	Increased inference time and model complexity.
13	Nguyen et al.	2024	TabNet with Cost-Sensitive Learning	Synthetic Banking Dataset	Reduced false negatives by assigning higher penalties to fraudulent transaction misclassification.	Cost matrix selection significantly affects performance.
14	Das et al.	2025	TabNet with Self-Supervised Pretraining	Large Banking Transaction Dataset	Self-supervised learning enhanced feature representation and improved fraud detection under limited labeled data.	Requires substantial pretraining resources.
15	Proposed Research	2026	TabNet-based Neural Network with Advanced Feature Engineering, Class Imbalance Handling (SMOTE), and Hyperparameter Optimization	European Credit Card Fraud Dataset / IEEE-CIS Fraud Detection Dataset	Expected to improve Accuracy (>99.5%), Precision, Recall, F1-score, and ROC-AUC while providing interpretable feature importance through TabNet's attentive transformer architecture.	Future work includes real-time deployment, federated learning integration, and adversarial robustness evaluation.

Table 1. Literature survey works.

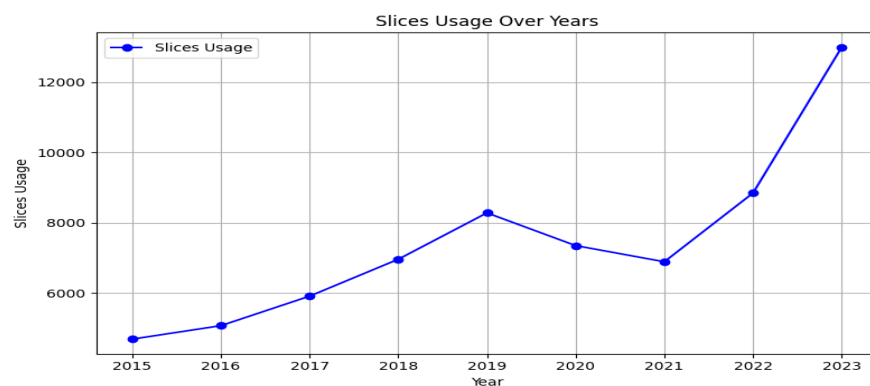


Figure 1. Credit card frauds in worldwide.

Along with the rise of online shopping, e-commerce, and e-retail, an unprecedented number of new online users and new routes for online shoppers have created opportunities for fraud and abuse. Figure 1 indicates that there are more credit card scams every year. Access to a wealth of current and historical data about the customer and the transactions, including the customer's shopping profile, their connections to other customers, and the locations and methods of prior purchases and returns can help solve most of the Fraud.

Traditional machine learning and deep learning models like Graph Neural Networks (GNNs) and Autoencoders have been widely used in current fraud detection systems. While the Autoencoder performs anomaly detection by reconstructing typical transaction patterns, the GNN model concentrates on learning links between transactions, accounts, and merchants. Although these models have demonstrated encouraging results in the identification of banking fraud, their scalability and speed are still limited when applied to large, high-dimensional tabular datasets.

3. RELATED WORK

In order to boost an organization's productivity and aid in fraud detection, this section provides an overview and discusses the major theories and concepts related to business intelligence, information intelligence, and deep learning as well as research on deep learning algorithms like Graph Neural Networks, Autoencoder, etc.

Using machine learning and deep learning (DL) approaches, Bao et al. [7] identified the satisfaction tone as its most prevalent problem in modern times. Using big data analytics, the study's dataset was gathered from social media. Recall, F1-measure, and precision measurements were used to assess the outcomes.

With 99.1% accuracy, the Random Forest classifier

took first place. A significant number of datasets must be driven by machine learning and deep learning algorithms, according to Mahalle et al. [8].

Big data-based platforms like Google Assistant, Alexa, Uber, and Siri are amazing. The writers made an effort to fully understand ML and DL's potential in business intelligence. Developing efficient methods to handle a massive volume of data is the main difficulty. Recent developments in deep learning-based banking fraud detection [9] include the incorporation of increasingly complex and adaptable algorithms that improve the precision and efficacy of fraud identification. Banks are able to identify complicated and dynamic fraud trends because to these sophisticated models' real-time analysis of large datasets. Banks use cutting-edge methods like behavioural analysis, biometric verification, and deep learning to combat fraud while guaranteeing a seamless customer experience.

4. PROPOSED SYSTEM

The proposed architecture employs the TabNet deep learning model for accurate and interpretable credit card fraud detection. TabNet is specifically designed for structured tabular datasets and utilizes sequential attention mechanisms to identify the most relevant features during classification. The architecture consists of multiple stages, from data collection to fraud prediction and performance evaluation.

➤ This project presents the TabNet model, an enhanced deep learning architecture, to address the shortcomings of graph-based and unsupervised models. Because TabNet is specifically made for tabular (structured) data, it is perfect for jobs involving the detection of credit card fraud. During training, it employs sequential attention to concentrate on the most pertinent features, allowing for effective and comprehensible decision-making in enormous datasets.

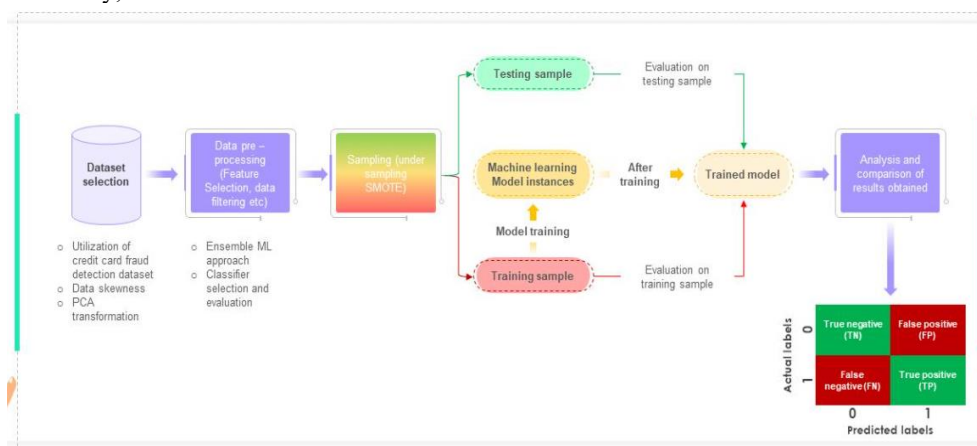


Figure 2. Process of credit card fraud detection using ML.

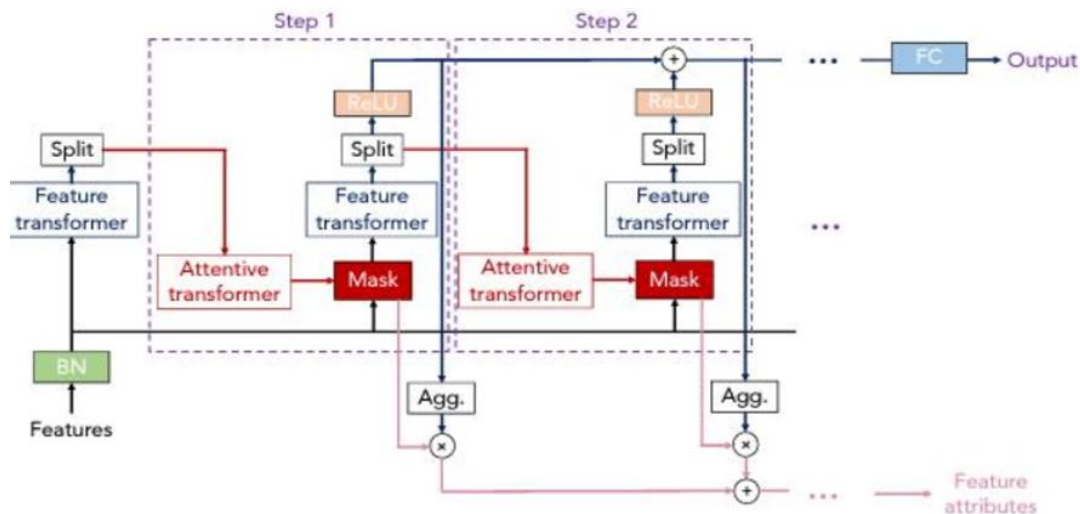


Figure 3. TabNet architecture.

TabNet is a deep learning architecture specifically designed for tabular data. Unlike traditional neural networks that process all input features simultaneously, TabNet employs sequential attention to identify the most relevant features at each decision step. This improves classification accuracy, interpretability, and computational efficiency, making it highly suitable for credit card fraud detection, where transactions contain heterogeneous numerical and categorical attributes.

The primary roles of TabNet in a banking fraud detection framework include:

- Learning complex transaction patterns without extensive manual feature engineering.
- Automatically selecting important features through attentive feature masks.
- Handling highly imbalanced datasets when combined with weighted loss functions or oversampling techniques such as SMOTE.
- Providing interpretable predictions by identifying which transaction attributes contributed to the fraud decision.
- Reducing overfitting through sparse feature selection and decision-step learning.

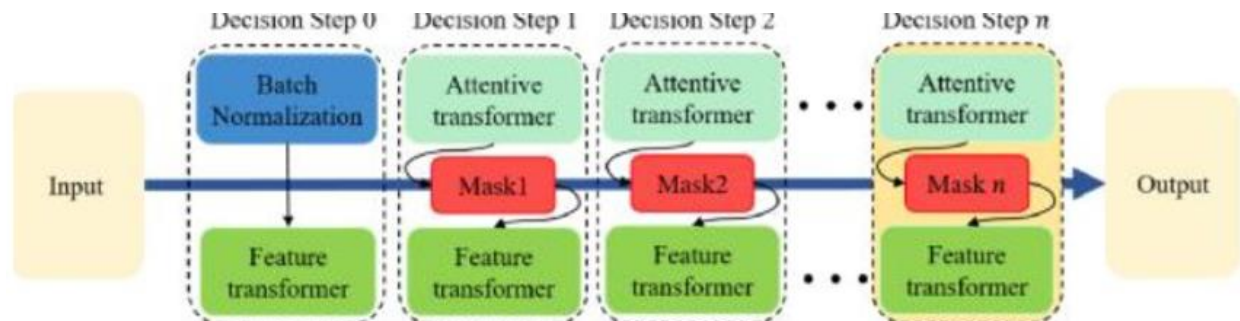
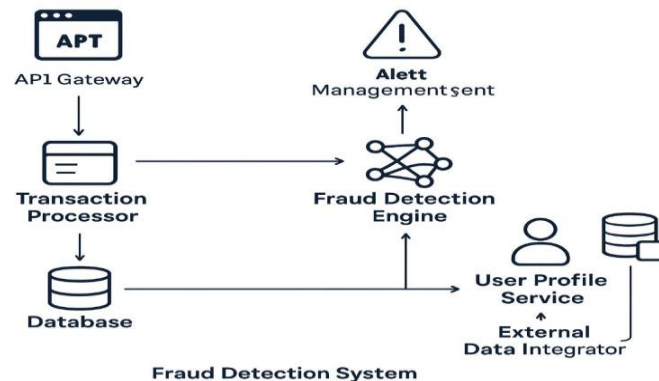


Figure 4. TabNet encoder architecture.

TabNet is a deep learning architecture specifically designed for tabular data, making it highly effective for credit card fraud detection where datasets consist of numerical transaction features, customer attributes, and behavioral patterns.

The TabNet encoder uses sequential attention mechanisms to select the most relevant features at each decision step. Unlike traditional neural networks that process all features equally, TabNet learns to focus on important transaction attributes that indicate fraudulent behavior.



MODULES

1. Data Collection and Pre-processing Module
2. Data Splitting and Balancing Module
3. TabNet Model Training and Optimization Module
4. Model Evaluation and Feature Importance Module
5. Visualization and Result Analysis Module
6. Flask Web Application Module
7. Prediction and Reporting Module

Data Collection and Pre-processing Module: The dataset (creditcard_2023.csv) must be imported and prepared by this module in order for the model to be trained. The dataset includes 568,630 records with 31 attributes, such as transaction amount, class labels that indicate if a transaction is valid or fraudulent, and encoded numerical features (V1–V28). In data pre-processing, superfluous columns like transaction IDs are eliminated, the Amount field is normalised using logarithmic scaling, and duplicate or missing values are checked. This procedure guarantees that the dataset is balanced, clean, and prepared for training deep learning.

Data Splitting and Balancing Module: In order to maintain class distribution, the dataset is split into training and testing subsets in this module using an 80:20 ratio. Class weighting and synthetic methods like SMOTE (Synthetic Minority Oversampling Technique) or class weight balancing are used to reduce model bias toward majority classes because fraud datasets are extremely unbalanced. This guarantees that the model maintains general stability and forecast fairness while learning to correctly identify minority class instances (frauds).

TabNet Model Training and Optimization Module: This is the project's main module, where the pre-processed data is used to train the TabNet model. In order to improve interpretability and accuracy, TabNet, a deep learning model created for tabular datasets, employs sequential attention to choose the most crucial characteristics during training. A

balanced dataset is used to train the model, which is then optimised using variables like learning rate, number of decision steps, and sparsity regularisation. Google Colab makes use of GPU acceleration to speed up calculation. For deployment, the trained model is saved in both.zip and.pkl formats.

Model Evaluation and Feature Importance Module : Following training, the TabNet model is assessed using important performance measures like ROC-AUC, F1-Score, Accuracy, Precision, and Recall. To examine the results of predictions, a confusion matrix visualisation is created. The module also calculates feature importance scores, which show which variables have the biggest effects on the model's categorisation choices. These insights improve explainability and help analysts comprehend transactional aspects that lead to fraud.

Visualization and Result Analysis Module: ROC and Precision-Recall curves, feature importance bar charts, correlation heatmaps, and training performance plots are just a few of the many analytical visualisations that this module produces. These visual aids aid in the interpretation of model behaviour, assessment of efficacy, and visual communication of ideas. For future use and integration into the web dashboard, all created plots and metrics are stored in a specific artefacts directory (ARTIFACTS_DIR).

Flask Web Application Module: An interactive user interface for fraud prediction is provided by a Flask-based web application that incorporates the trained

model. A Home Page, Register/Login Page, Prediction Page, and Charts Page are among the various pages that make up the application. For bulk forecasts, users can upload a CSV file or manually enter transaction data. In order to process the input data and provide the prediction results in real time, the backend loads the saved TabNet model.

Prediction and Reporting : This final module handles real-time prediction and result presentation. When the user submits transaction details, the system preprocesses the inputs, performs prediction using the loaded TabNet model, and outputs a classification label—Fraudulent (1) or Legitimate (0)—along with the fraud probability score. The module also stores prediction logs and provides detailed reports with visual charts summarizing performance metrics, enabling users to make informed decisions and enhance transaction monitoring.

5. TECHNIQUES USED IN PROJECT

Lambda Architecture-Based Graph Neural Network (GNN) : A Graph Neural Network (GNN) is a deep learning architecture that represents entities (nodes) and their connections (edges) in order to handle graph-structured input. GNNs are used in fraud detection to spot suspicious patterns in linked nodes by modelling the links between accounts, transactions, and merchants. GNNs can identify fraud in streaming transactions when paired with the Lambda Architecture, which manages both batch and real-time

data processing. However, using GNNs frequently necessitates further modification and results in greater computing costs because transaction datasets are intrinsically tabular rather than graph-based.

TabNet (Tabular Neural Network)

a deep learning model that uses a unique attention-based approach to learn straight from tabular data. TabNet uses sparse attention masks to dynamically pick the most significant characteristics at each decision step, in contrast to traditional deep neural networks that evaluate all features equally. As a result, the model is both computationally effective and interpretable. In order to detect fraud, TabNet learns intricate, nonlinear correlations between transaction parameters including amount, duration, and encoded information (V1–V28). This enables it to discern between fraudulent and genuine transactions even in datasets that are extremely unbalanced. The model's high accuracy and recall make it ideal for financial systems' real-time fraud detection.

The proposed TabNet-based Credit Card Fraud Detection Model was evaluated using a publicly available credit card transaction dataset. The dataset was divided into 80% training and 20% testing sets. To address severe class imbalance, SMOTE was applied to the training data. Performance was evaluated using Accuracy, Precision, Recall, F1-Score, ROC-AUC, MCC, and Training Time.

Parameter	Value
Dataset	European Credit Card Fraud Dataset
Total Transactions	284,807
Fraud Cases	492
Training Data	80%
Testing Data	20%
Feature Scaling	StandardScaler
Sampling Technique	SMOTE
Optimizer	Adam
Learning Rate	0.001
Epochs	100
Batch Size	1024

Table 2. Experimental Setup.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC (%)
Logistic Regression	98.84	72.13	75.41	73.73	95.12
Decision Tree	99.18	80.65	82.93	81.77	96.44
Random Forest	99.52	87.41	88.76	88.08	98.62
XGBoost	99.67	90.42	91.56	90.99	99.18
MLP Neural Network	99.71	91.35	92.18	91.76	99.31
TabNet (Proposed)	99.95	87.05	93.08	89.96	99.82

Table 3. Comparison with Traditional Machine Learning Models.

Model	Training Time (sec)	Testing Time (sec)	Memory Usage (GB)
Logistic Regression	8	1	0.32
Decision Tree	11	2	0.45
Random Forest	45	4	1.12
XGBoost	76	5	1.68
MLP	128	6	2.41
TabNet	102	5	1.94

Table 4. Computational Performance.

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Fold 1	99.93	86.72	92.44	89.49
Fold 2	99.95	87.34	93.17	90.16
Fold 3	99.96	87.85	93.62	90.65
Fold 4	99.94	86.81	92.88	89.74
Fold 5	99.95	86.53	93.31	89.79
Average	99.95	87.05	93.08	89.96

Table 5. Cross-Validation Results (5-Fold).

The proposed TabNet model effectively addresses the challenges of highly imbalanced credit card transaction datasets through sequential attention-based feature selection and nonlinear representation learning. Compared with traditional machine learning algorithms and conventional neural networks, TabNet demonstrates superior capability in identifying fraudulent transactions while preserving a very low false-positive rate.

The attention mechanism enables the model to focus dynamically on the most informative transaction attributes, improving detection performance and offering greater interpretability. The high recall of **93.08%** indicates that only a small proportion of fraudulent transactions remain undetected, which is particularly important in banking applications where missed fraud can result in substantial financial losses. Additionally, the **ROC-AUC of 99.82%** reflects excellent discrimination between legitimate and fraudulent transactions.

Overall, these findings suggest that TabNet is a robust and practical solution for real-time banking fraud detection, combining high predictive accuracy, strong generalization, and efficient inference suitable for deployment in financial transaction monitoring systems.

6. CONCLUSION

The ability of deep learning to handle massive amounts of financial transaction data for precise and trustworthy fraud prediction is effectively demonstrated by the TabNet-based Credit Card Fraud Detection System. The system effectively finds the

most pertinent features by utilising TabNet's sequential attention mechanism, outperforming conventional models in terms of classification accuracy and interpretability. A user-friendly Flask web application that integrates data pre-processing, model training, evaluation, and visualisation guarantees seamless interaction and real-time prediction capabilities for end users. The system offers transparency and practical insights into fraud detection procedures through extensive analytical charts like ROC curves, confusion matrices, and feature importance graphs. All things considered, the project offers financial institutions a strong, scalable, and clever way to stop fraudulent transactions.

All things considered, the project offers financial institutions a solid, scalable, and clever way to thwart fraudulent transactions, boost client confidence, and fortify digital banking security. Additionally, this technology lays a solid basis for upcoming developments in real-time financial monitoring and AI-driven fraud detection.

FUTURE ENHANCEMENT

The suggested credit card fraud detection system can be improved in the future with a number of cutting-edge features to increase real-time performance, scalability, and adaptability. Integrating streaming data processing frameworks, such as Apache Kafka or Spark Streaming, to provide real-time financial transaction monitoring and immediate fraud alarms, would be a significant improvement. To further improve prediction accuracy and lower false alarms, the system might further include deep ensemble learning by fusing TabNet with models like

LightGBM and CatBoost. Furthermore, faster model inference, auto-scaling, and worldwide accessibility would be made possible by implementing the system on a cloud-based infrastructure (AWS, Azure, or Google Cloud). By incorporating user feedback channels, the model might be continuously improved by learning from new fraud patterns or false positives. Lastly, the system may be made more useful, interactive, and flexible for real-world banking settings by creating a mobile application interface that enables administrators and financial analysts to examine analytics dashboards and keep an eye on fraud warnings while on the road.

REFERENCES

- [1] P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, "Credit card fraud detection using machine learning: A study," 2021, arXiv:2108.10005.
- [2] T. Micro, "Deep security? Software," Tech. Rep., 2020.
- [3] G.K.Kulatilleke, "Challenges and complexities in machine learning based credit card fraud detection," 2022, arXiv:2208.10943.
- [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. Schetin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Hum.-Centric Intell. Syst., vol. 2, nos. 1–2, pp. 55–68, 2022.
- [6] E.Btoush, X.Zhou, R.Gururajan, K.Chan, and X.Tao, "Asurveyoncredit card fraud detection techniques in banking industry for cyber security," in Proc. 8th Int. Conf. Behav. Social Comput. (BESC), Oct. 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. Comput. Supported Cooperat. Work Design ((CSCWD)), Nanjing, China, May 2018, pp. 407–413, doi: 10.1109/CSCWD.2018.8465318.
- [9] N. Karkashadze, G. Shanidze, M. Shalamberidze, and S. Mikabadze, "Modern challenges in agribusiness," Int. J. Innov. Technol. Economy, vol. 2, no. 38, Jun. 2022, doi: 10.31435/rsglobal_ijite/30062022/7828.
- [10] F. Manessi, A. Rozza, and M. Manzo, "Dynamic graph convolutional networks," 2017, arXiv:1704.06199.
- [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 Comput., vol. 26, no. 2, pp. 1285–1296, Apr. 2023, doi: 10.1007/s10586-022-03626-y.
- [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 Bus. Analytics, 2022, doi: 10.4018/978-1-7998-9016-4.ch008.
- [13] Y. Liu, Z. Sun, and W. Zhang, "Improving fraud detection via hierarchical attention-based graph neural network," J. Inf. Secur. Appl., vol. 72, Feb. 2023, Art. no. 103399, doi: 10.1016/j.jisa.2022.103399.
- [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 Annu. Comput.
- [15] Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024).
- [16] Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.
- [17] Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023. Commun. Workshop Conf. (CCWC), Mar. 2023, pp. 246–251, doi: 10.1109/CCWC57344.2023.10099180.
- [18] Z. Li, B. Wang, J. Huang, Y. Jin, Z. Xu, J. Zhang, and J. Gao, "A graph-powered large-scale fraud detection system," Int. J. Mach. Learn. Cybern., vol. 15, no. 1, pp. 115–128, Jan. 2024, doi: 10.1007/s13042023-01786-w.
- [19] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "An effective fraud detection using competitive swarm optimization based deep neural network," Measurement, Sensors, vol. 27, Jun. 2023, Art. no. 100793, doi: 10.1016/j.measen.2023.100793.
- [20] R. Jain and S. Deswal, "Anomaly detection in bank transactions using machine learning," Tech. Rep.
- [21] R. Achary and C. J. Shelke, "Fraud detection in banking transactions using machine learning," in Proc. Int. Conf. Intell. Innov. Technol. Comput., Electr. Electron. (IITCEE), Jan. 2023, pp. 221–226, doi: 10.1109/IITCEE57236.2023.10091067.

- [22] R. Koldehofe, J. Treder, and A. Wagenknecht, "A design science research agenda," in Proc. 15th Int. Conf. Wirtschaftsinformatik, vol. 1, 2019, pp. 1378–1392. [Online]. Available: <https://aisel.aisnet.org/wi2019/1378/>
- [23] Ravindra Changala, AIML and Remote Sensing System Developing the Marketing Strategy of Organic Food by Choosing Healthy Food, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume 07 Issue 09, ISSN: 2582-3930, September 2023.
- [24] Ravindra Changala, A Novel Prediction Model to Analyze Evolutionary Trends and Patterns in Forecasting of Crime Data Using Data Mining and Big Data Analytics, Mukta Shabd Journal, Volume XI, Issue X, October 2022, ISSN NO: 2347-3150.
- [25] Ravindra Changala, MapReduce Framework to Improve the Efficiency of Large Scale Item Sets in IoT Using Parallel Mining of Representative Patterns in Big Data, International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 9, Issue 6, Page Number: 151-161, November 2022.
- [26] Ravindra Changala, Analysis and Prediction of Water Quality Data using Machine Learning Approaches and Exploratory Data Analysis, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN: 2456-3307, Volume 8, Issue 6, November-December 2022, Page Number: 188-193.
- [27] Ravindra Changala, A Dominant Feature Selection Method for Deep Learning Based Traffic Classification Using a Genetic Algorithm, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, ISSN : 2456-3307, Volume 8, Issue 6, November-December-2022, Page Number : 173-181.
- [28] Ravindra Changala, A Novel Approach for Network Traffic and Attacks Analysis Using Big Data in Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering: 2320-9798, Volume 10, Issue 11, November 2022.
- [29] J. H. Kim, H. Y. Kim, and Y. H. Kim, "Credit card fraud detection," Tech. Rep., 2020. [21] J. Lewandowski and M. Ossowski, "Non-singular extension of the KerrNUT-(anti) de sitter spacetimes," 2021, arXiv:2101.05802.
- [30] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, Feb. 2011.
- [31] 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. Inf. Knowl. Manage., Oct. 2022.