International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Cybersecurity in Digital Banking: Advanced Fraud Detection Mechanisms for Financial Transactions

Bhalchandra Bapat
Independent researcher
bhalchandra@ssbm.ch

***Abstract*—Fraud detection in digital banking is increasingly important as more transactions are conducted online, and fraudsters become more sophisticated in their methods. In this paper, present a successful approach to fraud detection using a Recurrent Neural Network (RNN) on the IEEE-CIS fraud detection dataset. The proposed data preprocessing ensured the data was high-quality and suitable for the model to learn from. The proposed RNN model can learn temporal relationships in transaction data, which is vital for fraud detection. The proposed model showed great performance in the experiment, with an accuracy (acc), precision (prec) and F1-score (F1) of 94.34% and a recall (rec) of 94.38%. The model correctly classified both legal and illegal transactions, as shown by the confusion matrix, and the accuracy and loss curves indicated stable model training and low overfitting. Comparing the proposed RNN model with more traditional machine learning (ML) models, such as Support Vector Machine (SVM), Logistic Regression (LR), and Random Forest (RF), showed that the proposed model performed better. The findings demonstrate that the proposed RNN is effective for digital banking fraud detection.**

Keywords—financial cybercrime, fintech, fraud detection, banking security, machine learning, anomaly detection, financial security.

I. INTRODUCTION

In recent years, people have not only become increasingly relying on and accepting of digital financial services, but also led to increasingly complex types of financial cybercrimes and online banking fraud [1]. Banking fraud is a severe problem that has led to significant financial losses and a decline in consumer confidence [2]. In light of the internet and mobile devices, the banking sector has seen a substantial shift, which has supplanted traditional storefronts in the digital era [3][4]. Customers may now conduct transactions at any time and from any location, due to the growth of digital banking and its advantages [5][6]. Customers may now manage their accounts, send money, and this shift has fundamentally altered how consumers engage with their financial institutions by enabling them to pay bills online [7][8]. Prevention and identification of fraud is significant towards securing financial institutions and their customers [9]. Financial transaction fraud is a serious issue that impacts individuals, companies, and institutions worldwide. Additionally, it presents structural hazards to the economy's stability.

Traditional fraud detection techniques used pre-established criteria and manually created indications based on previous fraud incidents [10]. These techniques were effective in the early stages of the financial system, but they are now having difficulty keeping up with the amount, speed, and complexity of transaction data. Moreover, the methods of fraud continue to evolve and are decreasing the effectiveness of static models for fraud detection. need to therefore have more sophisticated and more flexible detection methods which can learn to detect the fraud immediately [11][12]. AI-based systems that employ ML and DL are being applied more and more to reduce financial losses, identify anomalous patterns in large volumes of data, and recognize fraudulent activity in real time [13]. These types of problems may be solved in a data-driven way by ML, a crucial component of AI. ML models are able to identify complex relations and minor variations that are difficult to observe using more traditional techniques because of the consideration of both past and current transaction data [14][15]. Because they can adapt by continually learning, they are especially well-suited for areas where dangers are always changing.

A. Motivation and Contribution

This study is motivated by the growing challenge of identifying fraudulent activity in online transactions, where the overwhelming majority of data indicate normal behaviour; thus, fraud cases are few and far between and hard to detect. Conventional ML approaches tend to execute poorly under such class imbalance and may fail to identify complex, sequential patterns in transactional data. As such, the analysis uses advanced deep learning techniques best suited to capturing the temporal relationships and irregularities in transactions. The research aims to develop a more efficient fraud detector capable of identifying smaller-scale fraud in data. The report makes a range of important contributions to cybersecurity practice:

- Employed Kaggle's IEEE-CIS fraud detection data set, which provides a thorough and accurate evaluation of fraud detection algorithms.
- The suggested model shows a significant capacity to differentiate between authentic and fraudulent transactions by effectively learning hidden temporal relationships within transaction data.
- To confirm the efficacy of the suggested method, a thorough comparison with popular ML models is carried out.
- Provided a generalized framework that can be adapted to other imbalanced and high-dimensional financial datasets for real-world fraud detection.
- Assessed for trustworthy validation, the model makes use of standard metrics including ROC curves, F1, rec, acc, and prec.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

B. *Justification and Novelty*

The suggested work is unusual because it has developed an RNN-based fraud detection system capable of modeling sequential dependencies in high volumes of financial transactions. In contrast to traditional machine learning methods, which primarily model feature relationships, the presented model leverages temporal information to identify more complex, hidden fraud cases. The ability is especially valuable in fraud detection cases with a high degree of imbalance. The efficiency of the suggested solution is supported by extensive experimental testing and comparative analysis, which demonstrate enhanced detection quality and reliability compared to traditional prediction models.

II. Literature Review

Several significant research studies on fraud detection in financial transactions have been reviewed and analyzed to guide and strengthen the development of this work.

Yapp and Yeh (2026) ascertain whether the change is statistically significant in the approaches' performance for a certain assessment metric across all data sets, apply the corrected Friedman test. The approach with the best overall performance is then identified by adding the scores across all assessment parameters. XGBoost and random forest outperformed AutoKeras on all evaluation metrics. However, at the company-imposed 5% FPR and recall constraint, The best FPR ratio was attained by the most advanced convolutional spiking neural networks (CSNN) for both young and senior clients [16].

Multani et al. (2025) examine the development of a cybersecurity framework using ML algorithms to avoid financial fraud. Accurate comparisons have been made between LR, RF, and XGBoost. The findings demonstrate that ensemble models outperformed LR, with both RF and XGBoost attaining over 91% accuracy and excellent discriminating power [17].

Han and Joe (2025) propose a systematic approach integrating IQR-based outlier removal, PowerTransformer normalization, Principal Component Analysis (PCA)-based feature selection, and advanced resampling techniques. Ensemble models, including LightGBM, XGBoost, and CatBoost, are trained and optimized, achieving substantial performance gains over baseline models (ROC-AUC: 0.9132 → 0.9916). Further improvements are observed with Voting and Stacking ensemble strategies, leading to ROC-AUC 0.9947. Additionally, Stochastic Weight Averaging (SWA) is applied, enhancing the final performance to ROC-AUC 0.9970 [18]. Jagwani et al. (2025) integrated machine learning and multi-factor authentication to secure online financial transactions. The suggested model uses spatio- TGCN for training. they found that the proposed model outperforms GCN and CNN. Comparing to other models, the framework's 91.40% accuracy rate suggests it could safeguard online financial transactions. This method may make internet financial transactions safer [19].

Deo et al. (2024) used to identify the online fraud transactions in the real world. The study above identifies and highlights the importance of explanatory methods in addressing online payment fraud in transactions, and offers tips for avoiding fraud in business to protect financial interfaces and maintain customer trust. Accuracy found upto 95% by implementing the things within the machine learning platform [20]. Thakre et al., (2024) intends to investigate a novel CNN-based method with attention mechanisms for enhanced fraud detection methods. The suggested model outperforms conventional methods and fundamental models like TransUNet, MedT, and FAT-Net by 19.36% with a high accuracy of 99.12%. This study's foundation was a systematic performance evaluation with demonstrated applications [21].

Despite notable progress in fraud detection, several challenges remain (Table I). Existing models are very precise and, in many cases, they are not very flexible and understandable to use in real-time. Ensemble and DL methods have issues of scalability, efficiency, and cross-dataset generalization. Besides, their resilience to changing methods of fraud and the seamless incorporation of real-time monitoring systems remains weak, and more resilient and deployable fraud detection systems are required.

TABLE I. Overview of Recent Studies on Fraud Detection in Digital Banking using Machine Learning

Author	Proposed Work	Dataset	Key Findings	Challenges/recommendation
Yapp and Yeh, (2026)	Applied ML method like XGBoost and random forest	9 fraud-related datasets	Overall performance of 5% false positive rate (FPR)	There is currently little comprehensive experimental comparison of these approaches
Multani et al. (2025)	Cybersecurity framework for fraud prevention using ML (LR, RF, XGBoost)	200,000 transactions (LOL Bank Pvt. Ltd.)	RF and XGBoost achieved >91% accuracy, outperforming LR	Need adaptive and interpretable AI models for real-time detection
Han & Joe (2025)	Ensemble models with ADASYN, SWA, Voting & Stacking	Financial transaction dataset	ROC-AUC improved from 0.9132 → 0.9970	Enhance model generalization while maintaining efficiency
Jagwani et al. (2025)	ML + multi-factor authentication using spatio-TGCN	Financial transactions dataset	Proposed model achieved 91.40% accuracy, outperforming GCN & CNN	Improve robustness and scalability for large-scale deployment
Deo et al. (2024)	ML models for detecting online payment fraud	Kaggle online payment transactions	Accuracy up to 95%, improved fraud identification and prevention	Need stronger real-time detection mechanisms
Thakre et al. (2024)	CNN with attention mechanism for fraud detection	Kaggle transaction dataset	Accuracy of 99.12%, surpassing baseline models	Reduce noise sensitivity and validate across larger datasets

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

III. Research Methodology

The proposed fraud methodology based on the IEEE-CIS dataset starts with rigorous data preprocessing, including handling missing data, outliers and feature normalization by scaling values to 0-1 using the min-max approach. SMOTE is used to balance the dataset, while PCA is used for feature selection to overcome excessive dimensionality. To generate temporal patterns for fraud detection, the data is divided 80/20 between training and testing. The ROC curves, F1, rec, acc, and prec are used to evaluate the model's performance. The complete workflow is depicted in Fig. 1.

The steps in the suggested flowchart for financial transaction fraud detection are explained in detail below.

A. Data Collection

The IEEE-CIS datasets obtained from Kaggle were utilized in the present study. There are 513,036 non-fraudulent and 18,450 fraudulent transactions out of 531,486 in the dataset. Additionally, it contains 269 features. Fraud is a binary target that classifies transactions as legal (0) and illegal (1), Fraud distribution, feature correlations, etc., are discussed in bar plots and heatmaps as follows:

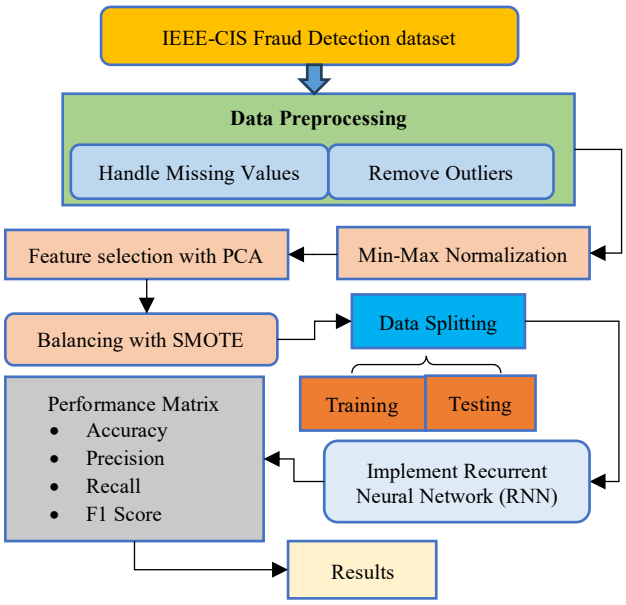

Fig. 1. Proposed flowchart for Fraud Detection for Financial Transactions.

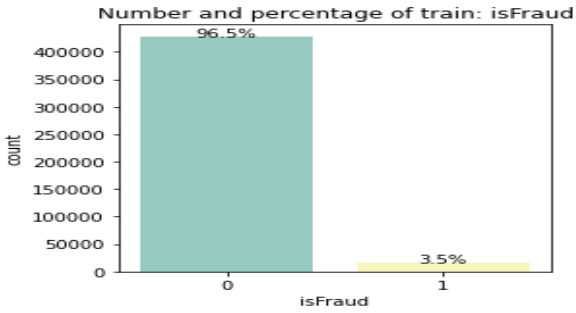

Fig. 2. Target variable distribution in the IEEE-CIS dataset.

Fig. 2 shows the class distribution of the training data for the Fraud variable. It shows that there is a huge imbalance, and the result is that most of the transactions (96.5%) are non-fraudulent (class 0) with only 3.5% being fraudulent transactions (class 1). Such an imbalance underscores the challenge of fraud detection, where models can be biased toward the non-fraud category unless appropriate handling measures, such as resampling, class weights, or anomaly detectors, are employed to improve sensitivity to minority fraud cases.

B. Data Pre-Processing

The IEEE-CIS Fraud Detection dataset was used to prepare the data, which was subsequently concatenated, cleansed, and had relevant features extracted. Missing values are handled to maintain data quality, and outliers are eliminated[22]. The data is then transformed and normalized. The advanced preprocessing steps are as follows:

- **Handle missing values:** An important step in the data preparation is covering missing values to ensure that information gathering is accurate and reliable to be used in ML or analysis. The approach used depends on the nature and level of the missingness.
- **Remove Outliers:** The process of data preprocessing to remove outliers includes identifying and treating data items that clearly stand out among most of the data. This is often done to improve the usefulness and validity of statistical procedures or ML algorithms, since outliers can introduce bias into their results and negatively affect model training.

C. Data Normalization

The min-max normalization is an algorithm that scales data to the interval between [0, 1]. This is done to ensure that the influence of outliers is minimized and the maximization of the use of the classifiers used. Normalization is done by the following mathematical Equation (1):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where X is the feature's initial value, X' is its normalized value, X_{min} is its minimum value, and X_{max} is its highest value.

D. Feature selection using PCA

To enhance performance, accuracy, and interpretability of an ML model and reduce computational costs, identifying and selecting the most pertinent features (input variables) of a dataset is known as feature selection. The PCA-based feature selection method selects pertinent original features by utilizing PCA's capacity to find important underlying patterns and variation in the data, rather than treating the extracted principal components as new features. PCA is a method for simplifying data, reducing its complexity while retaining meaningful linkages and patterns.

E. Data balancing using Synthetic Minority Over-sampling Technique (SMOTE)

Data balancing is the process of addressing class imbalance in a dataset, where one or more classes have significantly fewer samples than others, to prevent an ML model from being biased towards the majority class. In ML,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

SMOTE is a popular oversampling technique for dealing with unbalanced datasets.

Fig. 3. Count Plot for data balancing.

Fig. 3 illustrates the equally distributed classes, with an equal number of fraud and non-fraud samples. This balancing, which can be done through methods such as generating synthetic data, oversampling, or under sampling, is essential for training ML models so that they are not biased towards the majority class and can identify fraudulent transactions.

F. Data Splitting

The dataset has been divided into training and testing subsets in order to assess the model's effectiveness. Specifically, 80% of the data is used for training to learn and refine the model parameters, while 20% is reserved for testing to validate the model's efficacy.

G. Proposed Recurrent Neural Network (RNN)

RNN units are designed to memorize prior states, and they can successfully handle sequential data[23]. The current state is computed using this memory feature. As a result, Units of RNN accept two inputs: the value of the previous output and the current input. RNN unit mechanics may be described as (2).

$$y(t) = f\big(x(t) + y(t-1)\big) \tag{2}$$

Where $x(t)$ is current input, $y(t)$ is current output, and $y(t-1)$ is past output. The function that models this relation is represented by $f(x)$. The function $f(x)$ in Because of its tendency toward unstable gradients, the RNN context is A simple hyperbolic tangent function with nonlinearity. The rectified linear unit function is an example of a non-saturating activation function that allows gradients to grow arbitrarily large. The recurrent layers enable 128 batches. Every recurrent layer contains 30 time steps and 100 units. After receiving the outputs from the recurrent layers, the dense layer produces a single number indicating how many queries are expected. RNN units store state information in this manner and pass it to subsequent time steps. Longer orders are preferable for stateful RNN models, but they take longer to train and may perform badly because of high batch correlation.

H. Evaluation Metrics

The efficacy of the suggested design is assessed using a range of performance metrics. To identify True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN), model predictions are contrasted with real data. Key assessment metrics, including accuracy, precision, recall, and F1-score, are provided and discussed based on these results. Equations from (3) to (6) are shown below:

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \tag{3}$$

$$Precision = \frac{TP}{TP+FP} \tag{4}$$

$$Recall = \frac{TP}{TP+FN} \tag{5}$$

$$F1-score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \tag{6}$$

The number of occurrences that Accuracy is the degree to which the trained model correctly predicted each incident in the dataset. Precision is the proportion of TP estimations among all positive projections. Conversely, recall measures the model's sensitivity to relevant events, which is evaluated using the ratio of properly recognized positive examples to all TP occurrences. FP and FN are taken into consideration by the balanced F1 score, which has a range of 0 to 1. The harmonic mean of recall and accuracy is used to calculate it.

IV. Results and Discussion

The suggested DL model is applied to a system based on the Intel core i7, 16GB RAM, Ubuntu, 20.04 LTS and NVIDIA GTX 1080. Development and evaluation are done in Python 3.8, which uses TensorFlow 2.5, Pandas and NumPy. Table II compiles the performance evaluation criteria, which include rec, acc, prec, and F1. The model has achieved the highest accuracy of 94.34%, indicating it can classify most transactions correctly. The accuracy of the RNN is 94.34%, which is a high value that prevents FP, as the real transactions are rarely classified as fraud. It has a high recall rate of 94.38%, which means it is very sensitive to the detection of fraud and, therefore, has great strength in detecting almost all fraudulent activities. Furthermore, the RNN is a very dependable and effective model for identifying fraud in digital banking, with an F1-score of 94.34% confirming a favorable trade-off between recall and accuracy.

TABLE II. Experiment Results of Proposed Models for Fraud Detection on the IEEE-CIS Dataset

Performance Matrix	Recurrent Neural Network (RNN)
Accuracy	94.34
Precision	94.34
Recall	94.38
F1-score	94.34

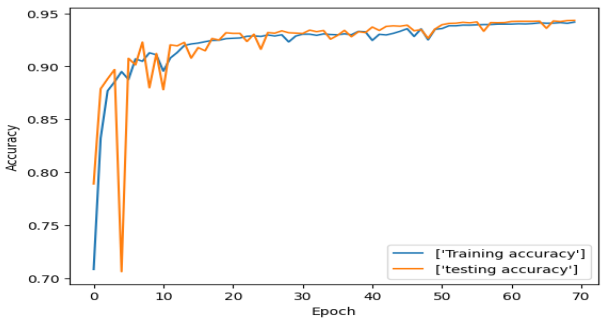

Fig. 4. Accuracy curves for the RNN Model.

The RNN model's training and testing accuracies over 70 epochs are shown in Fig. 4. The steepness of the two curves in

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

the early epochs indicates how quickly the model adapts to the data's underlying patterns. The accuracy levels off after approximately 10 epochs, then improves over time to approximately 95%. The testing and training accuracy lines are almost parallel, indicating the model generalizes without overfitting. Overall, the graph demonstrates that the RNN model has high and steady accuracy and is efficient and dependable for the task at hand.

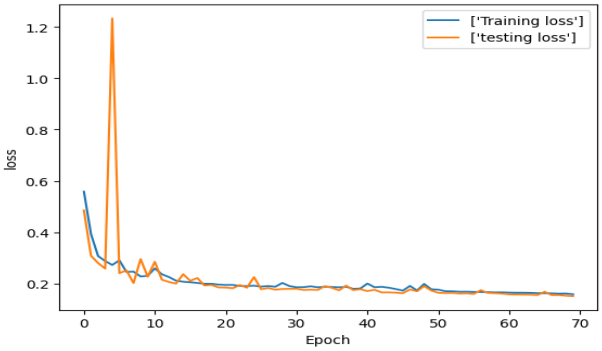

Fig. 5. Loss curves for the RNN Model.

The RNN model's training and testing losses during 70 epochs are displayed in Fig. 5. In the beginning, both losses are rather high, and the testing loss shows a short-term peak in the early epochs, indicating that the initial learning process is unstable. Yet, with increased training, the curves tend towards lower values, then become steeper and, approaching 0.15, begin to level off. This is indicated by the fact that training and testing losses are tight during the later epochs, suggesting that the model is well-optimized, with limited evidence of overfitting, and that it has produced stable performance during learning.

The model's effectiveness in categorizing fraud detection data is illustrated in Fig. 6. Among all the predictions, the model identified 98,395 fraudulent cases and 95,198 normal cases, which is a good indication that the model can distinguish between the two types. In the meantime, it misclassified 7,368 fraud cases and 4,254 normal cases. In general, the matrix demonstrates that the model is accurate and balanced in its performance on both fraud and normal transaction classification, thereby minimizing misclassifications.

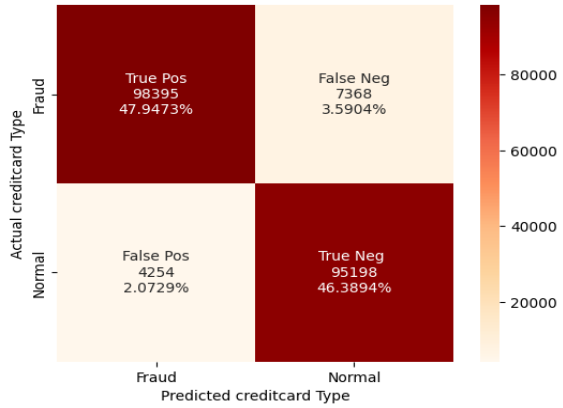

Fig. 6. Plot Confusion matrix for RNN.

A. *Comparative Analysis*

To illustrate the efficacy of the suggested RNN model, Table III presents a comparative accuracy study with other current models. In this comparison, the accuracy of Random Forest (RF) reached 90.3%, while Support Vector Machine (SVM) and Logistic Regression (LR) achieved 56.2% and 89%, respectively. The suggested Recurrent Neural Network (RNN) achieves the best overall performance, with the highest recall (94.34%), accuracy (94.34%), and precision (94.38%), and an F1-score of 94.34%. It is also the best at identifying fraudulent transactions, with the fewest FP and FN, due to its high recall.

TABLE III. PERFORMANCE COMPARISON OF DIFFERENT PREDICTIVE MODELS OF FRAUD DETECTION

Model	Accuracy	Precision	Recall	F1-Score
SVM[24]	56.2	50.9	92.8	66.3
LR[25]	89	71	65	68
RF[26]	90.30	66	91	-
RNN	94.34	94.34	94.38	94.34

The developed RNN model, with an accuracy of 94.34, is an important tool for fraud detection because it effectively captures sequential patterns in transaction data, enabling it to identify complex, hidden relationships that conventional models may miss. This is due to its low false alarm rate, effectiveness in detecting fraudulent activity, and excellent reliability and robustness. The given balance is particularly well-suited to the RNN in the digital banking environment, where timely and accurate fraud detection is paramount to security and customer confidence.

V. CONCLUSION AND FUTURE STUDY

Digital banking has revolutionized the mode of banking in the past decade. Instead of people going to the bank, digital banking via web, mobile, tablet has now reached at people's homes at their fingertips. However, this has also brought in a significant cyber threat of financial exploitation, particularly impacting senior people. The paper develops a Recurrent Neural Network (RNN), an effective method of identifying fraud in the complex and imbalanced IEEE-CIS data. The researchers established a solid baseline by balancing the extreme class imbalance with SMOTE oversampling and Min-Max normalization, which enabled the deep learning model to stabilize after 70 epochs. The sequential pattern recognition capability of RNN, which uses a property of memory to recall previous transactions, compared with the conventional models, demonstrated high accuracy and an F1-score of 94.34%. In addition, the comparative analysis shows a high level of improvement over baseline approaches, such as SVM (56.2%) and Random Forest (90.3%). The model is highly sensitive to the minority fraud category, achieving a recall of 94.38% and reducing the risk of illegal transactions going undetected. Finally, the consistency demonstrated in the recommended design is scalable to unknown inputs, as evidenced by training and loss curves, which in turn implies that it is a solid and effective solution for providing the necessary level of security and customer confidence in potentially high-stakes digital banking scenarios.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

A. Limitations and Future Work

The primary limitations of this study are the black-box nature of DL and the high computational and training costs of RNN architectures, which are not always as interpretable as financial auditing requires. Similarly, despite being able to generate synthetic noise or avoid overfitting. The current study may not adequately reflect the dynamic, constantly changing nature of fraud strategies because it is based on static historical data. The next step in research should be the integration of Explainable AI (XAI) layers to provide clear decision-making guidance and the examination of online learning platforms to stay up to date with the dynamic nature of real-time fraud schemes.

REFERENCES

[1] H. AbouGrad and L. Sankuru, "Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations," *Mathematics*, vol. 13, no. 13, p. 2110, Jun. 2025, doi: 10.3390/math13132110.

[2] T. V. Shah, "Leadership in digital transformation: Enhancing customer value through AI-driven innovation in financial services marketing," *Int. J. Sci. Res. Arch.*, vol. 15, no. 3, pp. 618–627, Jun. 2025, doi: 10.30574/ijsra.2025.15.3.1767.

[3] V. Sikarwar, "AI-Powered Process Mining for Intelligent, Personalized Customer Experience in the Insurance Sector," *Int. J. Res. Publ. Eng. Technol. Manag.*, vol. 8, no. 4, pp. 12418–12428, 2025, doi: 10.15662/IJRPETM.2025.0804007.

[4] S. Singamsetty, "Efficacy of Data Governance a Cutting Edge Approach to Ensuring Data Quality in Machine Learning for Banking Industry," in *2024 2nd International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/SCOPES64467.2024.10991944.

[5] S. Kakkar, "Explainable AI Models for Credit Risk Scoring in Banking: Balancing Accuracy and Regulatory Transparency," *Int. J. Financ. Data Sci.*, vol. 3, no. 2, pp. 1–6, Aug. 2025, doi: 10.34218/IJFDS_03_02_001.

[6] K. B. Thakkar and H. P. Kapadia, "The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model," in *2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICTEST64710.2025.11042822.

[7] L. K. Osei, Y. Cherkasova, and K. M. Oware, "Unlocking the full potential of digital transformation in banking: a bibliometric review and emerging trend," *Futur. Bus. J.*, vol. 9, no. 1, p. 30, Jul. 2023, doi: 10.1186/s43093-023-00207-2.

[8] N. A. Zondervan, F. Tolentino-Zondervan, and D. Moeke, "Logistics Trends and Innovations in Response to COVID-19 Pandemic: An Analysis Using Text Mining," *Processes*, vol. 10, no. 12, p. 2667, Dec. 2022, doi: 10.3390/pr10122667.

[9] S. B. Shah, "Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection," in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[10] H. Abbassi, S. El Mendili, and Y. Gahi, "Adaptive, Privacy-Enhanced Real-Time Fraud Detection in Banking Networks Through Federated Learning and VAE-QLSTM Fusion," *Big Data Cogn. Comput.*, vol. 9, no. 7, p. 185, Jul. 2025, doi: 10.3390/bdcc9070185.

[11] G. Mishra, G. Singh, and S. Pathak, "Enhancing Banking Fraud Detection and Risk Mitigation Using Advanced Machine Learning Techniques," *Int. J. Multidiscip. Res.*, vol. 8, no. 1, Jan. 2026, doi: 10.36948/ijfmr.2026.v08i01.65768.

[12] V. Pal and S. K. Chintagunta, "Transformer-Based Graph Neural Networks for RealTime Fraud Detection in Blockchain Networks," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 1401–1411, Jul. 2023, doi: 10.48175/IJARSCT-11978Y.

[13] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, Aug. 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[14] B. Oztas, D. Cetinkaya, F. Adedoyin, M. Budka, G. Aksu, and H. Dogan, "Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry," *Futur. Gener. Comput. Syst.*, vol. 159, pp. 161–171, Oct. 2024, doi: 10.1016/j.future.2024.05.027.

[15] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[16] E. K. Y. Yapp and H.-Y. Yeh, "An extensive experimental comparison of machine and deep learning methods for credit and bank fraud detection," *Financ. Res. Lett.*, vol. 88, p. 109190, Jan. 2026, doi: 10.1016/j.frl.2025.109190.

[17] D. Multani, G. V Radhakrishnan, U. Shankar, K. Upreti, K. Gupta, and A. Tiwari, "Fraud Prevention in Banking: Machine Learning-driven Approaches for Detecting Payment Anomalies," in *2025 International Conference in Advances in Power, Signal, and Information Technology (APSIT)*, IEEE, May 2025, pp. 1–6. doi: 10.1109/APSIT63993.2025.11086276.

[18] Y. Han and I. Joe, "Enhanced Predictive Modeling for Anomaly Detection in Financial Transactions Using Machine Learning," *IEEE Access*, vol. 13, pp. 154438–154449, 2025, doi: 10.1109/ACCESS.2025.3602236.

[19] B. Jagwani, A. H. Hasan, K. Agnihotri, K. Jain, A. Perada, and D. Gobinath, "Multi-Factor Authentication for Secured Financial Transactions Through Spatio-TGCN Model," in *2025 International Conference on Visual Analytics and Data Visualization (ICVADV)*, 2025, pp. 270–275. doi: 10.1109/ICVADV63329.2025.10961247.

[20] S. Deo, M. Adnan, M. Raj, A. I. Abidi, and N. Bansal, "Online Payment Fraud Transaction Detection using Machine Learning," in *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/DELCON64804.2024.10866604.

[21] N. K. Thakre, M. Misba, S. L. Sajja, S. K. Fardale, V. A. Vuyyuru, and M. K. Mohamed Faizal, "Unveiling Market Anomalies: Harnessing Convolutional Neural Networks for Fraud Detection in Finance," in *2024 International Conference on Communication, Control, and Intelligent Systems (CCIS)*, 2024, pp. 1–6. doi: 10.1109/CCIS63231.2024.10931899.

[22] V. Sikarwar, "AI-Driven Data Quality Framework for Modern Data Lakes: An Architecture Overview," *J. Artif. Intell. Gen. Sci.*, vol. 6, no. 1, September, pp. 662–688, 2024, doi: 10.60087/jaigs.v6i1.451.

[23] A. Sherstinsky, "Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network," *Phys. D Nonlinear Phenom.*, vol. 404, p. 132306, Mar. 2020, doi: 10.1016/j.physd.2019.132306.

[24] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[25] C. Reddy, A. Vaid, and S. Prabhagaran, "Deep Learning-Based Real-Time Credit Card Fraud Detection in Financial Transactions," *Int. J. Adv. Res. Eng. Technol.*, vol. 15, no. 6, pp. 20–30, 2024.

[26] A. Orelaja and A. F. Adeyemi, "Developing Real-Time Fraud Detection and Response Mechanisms for Financial Transactions," vol. 8, no. 1, pp. 573–582, 2024.