An Intelligent Method for Improving Credit Card Fraud Detection Using a Hybrid LSTM and Deep Neural Network Framework

ANAM AHSAN[1], SANAA ASHIQ[2], MUHAMMAD JUNAID[1], SAJID IQBAL[3], GHULAM FAROOQUE[3], IFTIKHAR AHMED KHAN[3]

[1]Department of Computer Science, The University of Lahore, Sargodha Campus, Sargodha 40162, Pakistan
[2]Department of Software Engineering National University of Modern Languages, Rawalpindi, Pakistan
[3]Department of Computer Science and IT, The University of Lahore, Lahore 54000, Pakistan

Abstract: E-commerce has caused a great transformation in the chain of operations through which companies all over the world transact their businesses. However, with the rapid increase in online shopping, the prevalence of online fraud, particularly credit card fraud has emerged as one of the major security threats connected with e-commerce. The classical models of fraud detection easily address the problems of imbalanced data, pattern of the poorly-sequentially recorded data, and the need to detect the fraud instantly. To address the challenges mentioned in this study, a hybrid architecture which is a fusion of Long Short-Term Memory (LSTM) unit and Deep Neural Network (DNN) modules is propsoed. The DNN component is meant to discover complex interrelatedness of diverse features. Whereas, the LSTM layer establishes a temporal connection which exists in a series of dealings. The preprocessing stage applies the method of the Synthetic Minority Over-Sampling Technique (SMOTE) to solve the issue of unrepresentative classes. The model is tested on the publicly available credit card frauds dataset. It is observed that the proposed model shows a better performance with 99.6% accuracy, 94.5% precision, recall of 91.2% and ROC-AUC of 97.3%, respectively. The comparative study reveals that the hybrid model is superior to the traditional algorithms, including logistic regression, decision trees, LightGBM, and single-created LSTM models, with regard to prediction performance. The presentation of the confusion matrices, the precision-recall curves, and the learning curves is also used to justify the measures of the soundness of the model and its generalizability, without showing the training and validation loss. To conclude, all of these visual tests confirm the reliability of the system under various conditions of the working environment. On the whole, the study adds significantly to the development of a more efficient and scalable fraud detection system, the overall purpose of which is to enhance the level of safety of virtual transaction setups and employ it to other industrial domains, such as energy.

Index Terms: credit card fraud detection, cybersecurity, imbalanced data handling, machine learning, real-time fraud prevention

I. Introduction

It has been observed that e-commerce has significantly influenced the global economy over the last ten years, while exerting a significant effect on consumer purchasing behavior and business dynamics. The Internet has facilitated communication between buyers and sellers and digital transactions have become a natural aspect of life for millions of individuals across the world [1]. It is projected that the application/number of digital transactions will increase and the global e-commerce money will surpass seven trillion dollars by 2025. Not only online payments make purchasing easier and faster, but they also assist in forming a more interconnected global economy [2]. Nevertheless, such a sudden transition to digital business has caused significant cybersecurity challenges. E-commerce is, therefore, growing but the risks associated with it are growing along with it. Credit card fraud is one of the most common and dangerous risks in the online environment [3]. Illegal transactions cause a significant loss of money to the

consumers and businesses, tarnish the reputation of the institution, and reduce the credibility of online payments as safe.

The Nilson Report stated that in 2020, world card payment fraud totaled 28.65 billion dollars and this number will continue to increase as fraudsters employ even more sophisticated practices [4]. The existing fraud detection system is rather efficient but constrained by a set of limitations. Traditional machine learning, such as Light Gradient Boosting (Light-GBM) [5] and Support Vector Machine (SVM) [6] often face the challenge of detecting a pattern in a sequence of transactions or providing real-time detection services. Moreover, false negative rates are large and model accuracy remains low because there are more instances of fraudulent transactions than legitimate ones in imbalanced datasets [7], which leads to large curves on this imbued model [8]. Such requirements, in their turn, demand high-tech and flexible solutions. The current paper meets this requirement with the help of the proposed hybrid method that merges the Long Short-Term Memory (LSTM) networks and Deep Neural Networks (DNNs). The ability to learn complex and non-linear relationships is attributed to DNNs. An important property of LSTMs is the ability to learn temporal relationships in sequential data. As part of our research, combining these two methods into one scheme gives better precision, scalability, and real-time performance in detecting fraudulent actions. The problem of imbalanced data sets is completely solved by applying the Synthetic Minority Oversampling Technique (SMOTE) that enhances the identification of uncommon fraudulent transactions.

The major goals of the research are as follows:

- Identifying the most significant cybersecurity vulnerabilities and weaknesses of the primary e-commerce platforms.
- Development and evaluation of a hybrid LSTM-DNN model for real-time fraud detection.
- To give actionable insight into integrating the model into the e-commerce cybersecurity framework.

The above objectives would contribute to further the knowledge of cutting-edge machine learning techniques in addressing cybersecurity issues.

II. Related Work

Many techniques to identify credit card fraud have been developed during the last few decades. Both Machine Learning (ML) and Deep Learning (DL) techniques are used in these methods. This section looks at the benefits and drawbacks of various approaches and how they have affected the creation of sophisticated fraud detection systems. Traditional ML models have been used mainly to detect credit card fraud for a long time. The majority of these models are intended for classification tasks, with the goal of classifying every transaction as authentic or fraudulent. In this area, Decision Tree (DT), Logistic Regression (LR), and Gradient Boosting (GB) are frequently employed models.

A. Decision Trees

Decision Trees (DTs) have been widely used to detect fraud by the virtue that they are simple, easy to interpret, and handle both numerical and categorical data. These models work on a recursive rule where the data is divided in subsets, with each subset based on a definite feature, thus forming tree-like structures that ultimately result in a conclusive classification, which is or isn't a fraud. The transparency of decision-making is one of the greatest advantages of DTs. On the contrary, it has the major disadvantage of the possible overfitting situation, when the model becomes excessively complex and cannot be adequately generalized to new and unknown data. Poor generalization may lead to the lower performance of DTs in the actual fraud detection tasks.

B. Logistic Regression

Logistic Regression (LR) is used widely as a method to predict the likelihood of a fraudulent transaction. It operates by exploring the correlation among a dependent variable and a single or more independent variables. In this regard, the dependent variable may be the incidence of a fraudulent transaction and the independent variable(s) may include the occurrence of different features related to the transaction [11]. LR has been cited as being easy to use and giving a probability-based estimate, useful in risk determination. There are, however, notable shortcomings when dealing with complex, non-linear, and variable relationships, since LR is unable to capture variable interrelationship among various features [12]. Consequently, it might not work as well when handling more complicated datasets characterized by complex relations that are applicable in the detection of fraud.

C. Light-GBM

The Light Gradient Boosting Machine (Light-GBM) has evolved into a very promising instrument in fraud detection in recent years. Light-GBM, which is a form of the Gradient Boosting (GB) approach, constructs a cascade of DTs in a progressive mode to address the limitations of conventional DTs. Light-GBM, as opposed to the standard DTs, depends on a histogram-based approach, which enhances the speed and memory efficiency of using a large dataset [13]. Its high accuracy and efficiency are one of its main advantages that lead to its use in classification problems that involve fraud detection. Light-GBM is also effective in dealing with imbalanced data where more emphasis is put on the minority group, which comprises fraudulent transactions. It is, however, not good at capturing sequential patterns in transaction data, since it does not consider sequential patterns in transactions as single events [14]. A poor grasp of dynamics through time may hinder the ability of this model to establish changes in the patterns of fraudulent activity. Large e-commerce systems may also pose a

challenge to the use of large-scale models like Light-GBM to detect fraud in real-time.

III. Deep Learning Models in Fraud Detection

Deep Learning (DL) techniques have become more popular to detect fraudulent activity as a result of advancements in conventional ML techniques. These techniques use models such as Long Short-Term Memory (LSTM), which can effectively analyze sequential data and capture a variety of temporal relationships.

A. LSTM Networks

LSTM networks are a type of RNN and they are better adaptable to deal with sequential data. These networks are specifically applied to those jobs where timely relationships are critical, such as detection of credit card transaction fraud. LSTMs are able to learn/detect long-term relationships in sorted data. This is why they can identify trends that point to fraudulent activities in the long-run [15]. Indicatively, the use of a combination of a sequence of seemingly innocuous transactions carried out within a very limited duration of time could be an indicator of fraudulent behavior. This is also good in LSTM networks as they are able to retain information in the sequence of previous transactions that enable them to detect patterns that the rest of the traditional ML models might not be aware of. Nevertheless, LSTM network training requires enormous sums [16] of information and tedious calculation, which can never in actual circumstances be an option as regards detection in real time. LSTMs are also vulnerable to overfitting, particularly when dealing with imbalanced datasets, such as those in which fraudulent transactions are a minor percentage of all legitimate transactions.

Large gaps still exist in the success of ML and DL techniques in detecting fraudulent activity. The biggest challenge is posed by models that cannot keep abreast with the dynamics of offenses perpetrated by fraudsters. The ways of committing fraud are evolving and fraudsters continue to alter their methodology in order to evade the fraud detection mechanisms, as so eloquently explained by cite 7. Additional requirements include real-time fraud detection, particularly in large scale e-commerce. In the case of the latter, model [11][12] of Light-GBM and LSTM do not satisfy the important criteria of real-time speed when running on large transaction contents, in most practical applications. Other than that, the majority of the current models fail to solve the issue of data imbalance adequately. The number of actual transactions remains significantly higher in comparison to fraudulent transactions. The impact is high false negatives, that is, fraud transactions being seen as genuine, so that the fraud detecting systems become compromised.

Hence, a new hybrid model is suggested in this paper. This model is a combination of LSTM and DNN. The combined power of these two models is used to amalgamate precision boosting, with improved scalability and real-time fraud detection system enhancement. These two factors are taken into consideration to formulate a solution to large-scale credit card fraud detection in the current research.

IV. Proposed Methodology

This section presents a method for constructing hybrid LSTM models designed to detect credit card fraud. This approach tackles contemporary issues, such as identifying patterns in transaction data and handling dataset bias. It also enables real-time detection of fraudulent activities.

A. Data Gathering

This paper uses the credit card fraud dataset of Kaggle. The data is a set of transaction logs with varied information, such as time, amount, and several anonymous variables. The variable in question, which is called class, is set to become 1 to indicate that a given transaction is a fraudulent one (1), while 0 indicates a legitimate transaction (0). An imbalance is observed in the dataset where the percentage of the transactions expected to be fraudulent is relatively small.

B. Data Preprocessing

The following steps were applied as preprocessing before modeling.

- ***Feature Scaling:*** The columns 'time' and 'amount' were scaled uniformly using the standard scaler to ensure all features have an equal impact on the model's learning process.
- ***Data Splitting:*** To address the class imbalance, the SMOTE technique was used on the training data. SMOTE generates artificial examples of the minority class, which includes fraudulent transactions, to create a more balanced dataset. This approach helps to prevent the model from being biased in favor of the majority class during the training process.

C. Model Architecture

The suggested hybrid model is a blend of the LSTM networks with the Dense Neural Networks (DNNs) in order to utilize both of their advantages. DNNs are better at learning non-linear and complex correlations between attributes, whilst LSTM networks are effective at learning sequential and temporal relationships in the data.

Fig. 1 represents the hybrid neural network architecture used in the experiment. The model has two parallel processes that manipulate input streams. The former is based on a series of dense layers including the input layer with sequence length of 30. Following the dense/input layer is the dense layer which has 128 neurons. Then, there is regularization dropout, that is, another dense layer which has 64 neurons. Lastly, another dropout, that is, dropout 1. The second one utilizes bidirectional LSTM layers to learn

time dependent information. It uses as input another input layer (input layer 1) which, in turn, takes sequences of length 30 as feed. Then, it uses a series of two continuous bidirectional LSTM layers (bidirectional and bidirectional 1), with dropout used between them (dropout 2). The results of the last dense layer of the first branch and the last bidirectional LSTM layer of the second branch are then combined in order to create a conjoint representation. In classification, the output of one neuron is passed to a final dense (dense 2) layer that has a neuron with an implicit sigmoid activation. This gives the ultimate predictions. This model is able to acquire the local patterns of the dense layers and long-range dependencies through bidirectional LSTMs due to its architecture in order to acquire a potentially more detailed representation of the input data. Two bidirectional LSTM layers are involved in the model.

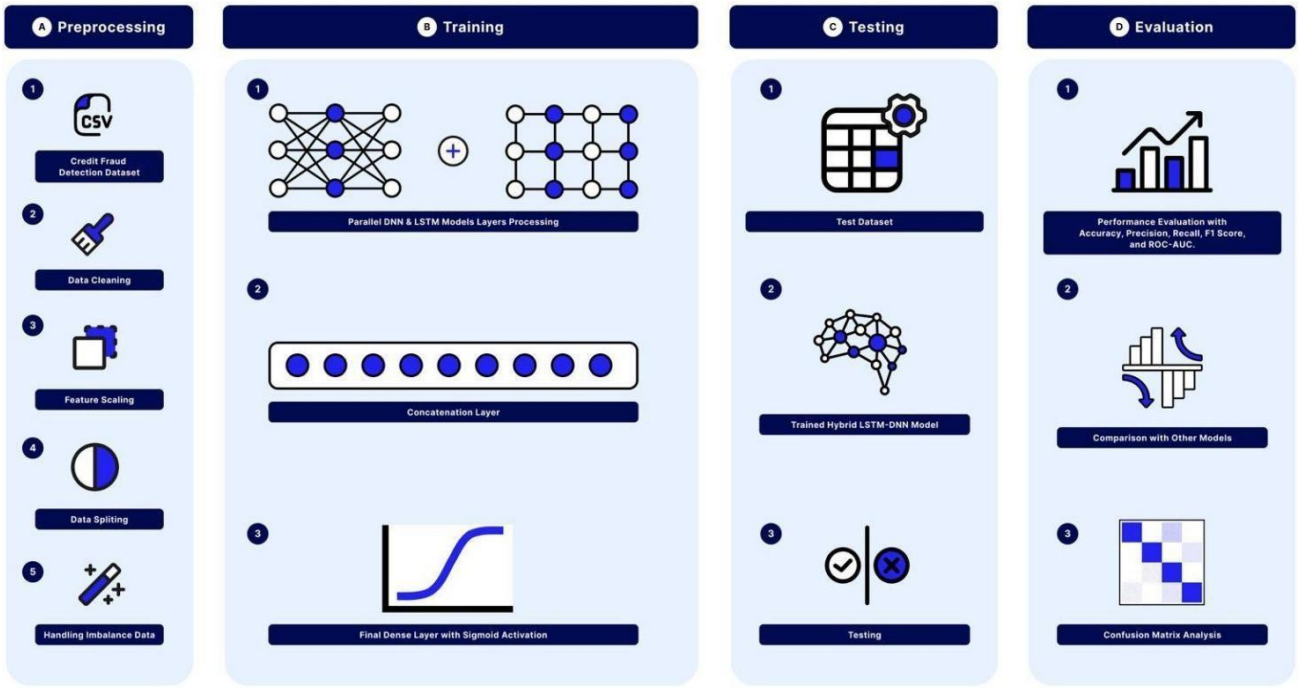

FIGURE 1. Hybrid Proposed Model LSTM-DNN Architecture

The operations of an LSTM unit at time step are defined as follows:

$$f_t = \sigma(W_f h_{t-1}, W_f x_t + b_f), \quad (1)$$

$$i_t = \sigma(W_i h_{t-1}, W_i x_t] + b_i), \quad (2)$$

$$\tilde{C}_t = \tanh(W_C h_{t-1}, W_C x_t] + b_C), \quad (3)$$

$$C_t = f_t C_{t-1} + i_t \tilde{C}_t, \quad (4)$$

$$o_t = \sigma(W_o h_{t-1}, W_o x_t] + b_o), \quad (5)$$

$$h_t = o_t \tanh(C_t). \quad (6)$$

where

- x_t: time step input vector t.
- h_t: At time step, the hidden state t.
- C_t: State of the cell at time stept.
- W_i, W_f, W_o, W_C: Weighted matrices.
- b_f, b_i, b_C, b_o: Bias vectors.
- σ: Sigmoid activation function.
- $\odot$:Multipication based on elements.

Dropout layers are added after each LSTM with a dropout rate of 0.5 to prevent overfitting. The dropout operation is expressed as follows:

$$y_i = \begin{cases} 0, & \text{with probability } p, \\ x_i, & \text{with probability } (1 - p) \end{cases} \quad (7)$$

where the dropout rate of $p = 0.5$.

- Dense layer with rectified linear unit activation and 128 units:

$$y_i = \max(0, z_i), \quad (8)$$

where z_i is the weighted sum of inputs to the i-th neuron.

- A dropout at a 0.5 rate.
- ReLU activation with 64 unit dense layer .
- Another dropout at the rate of 0.5.

The outputs of LSTM and DNN were concatenated. They were then passed through a dense layer with one unit and a sign-up activation. The sigmoid is defined by the following

$$\sigma(z)=1/(1 + e^{-z}), \quad (9)$$

where the neuron's input is denoted by z. This layer outputs/exemplifies the probability of a transaction being fraudulent.

D. Model Training

The model was constructed using the Adam Optimizer, which employs a binary cross-entropy loss function and a learning rate of 0.001. Next, we employed early-stopping, which keeps track of validation losses and halts training after five epochs if no improvement is seen. Further, if validation loss improves throughout the three epochs, then Reduce Learning Rate on Plateau is employed, which lowers learning rate by a factor of 0.5. Using a batch of 512, the model was retrained for 20 epochs.

E. Evaluation Metrics

The following metrics have been used to assess the model's performance.

- *Accuracy: This measures the proportion of correct predictions made by the model*.
- *Precision:* It represents the proportion of correct positive predictions that specifically identify actual fraudulent transactions.
- *Recall:* The model's accuracy is measured by the percentage of genuine instances of fraud that it successfully detects..
- *F1-Score:* This score is a balanced average of precision and recall, calculated as their harmonic mean.
- *ROC-AUC:* This assesses the model's capacity to differentiate between deceptive and authentic transactions across every conceivable classification threshold, as indicated by the area under the ROC curve.

V. Results and Discussion

In this section, the proposed hybrid LSTM-DNN model is described with respect to the experimental setup, evaluation indicators, and the outcomes of this model. The model was tested to understand its ability in discriminating fraudulent transactions by processing imbalanced data and extracting time relationships. An analysis of the hybrid model involving LSTM and DNN to detect credit card fraud was done quantitatively. The obtained insights of the analysis are reported through a series of performance measures and visualisations, including accuracy versus epochs, loss curves, confusion tables, and precision versus recall curves and ROC curves.

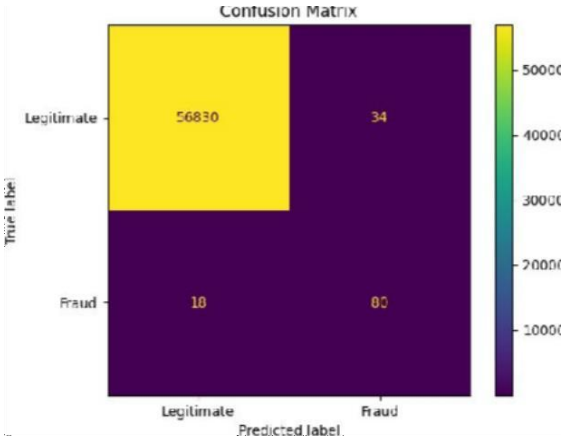

FIGURE 2. Confusion Matrix for Legitimate and Fraud Class

The hybrid LSTM-DNN has better performance parameters than the basic methods. Particularly, it has the best ROC-AUC (0.973), accuracy (0.996), precision (0.945), recall (0.912), and F1-score (0.928). This demonstrates the value of using a mixture of LSTM networks which are good at recognizing the time trends in combination with DNNs which are good at learning complex relationships between features. SMOTE helps to improve model performance, as it helps to manage the performance of the model characterized by an imbalance in the dataset.

In Figure 2, the model is illustrated with results on a set of test data in the form of a confusion matrix. This is a matrix characterized by four major values, that is, True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). The model is able to correctly identify 80 transactions as being fraudulent and 56,830 as legitimate. This indicates that 34 legal transactions have been wrongfully tagged as fraudulent, thus false alarms. The number of fraudulent transactions mistaken as legitimate is 18 and the cases of possible fraudulent transactions go unnoticed. The TP and TN values are high, indicating that the model is a good discriminator based on valid and fake transactions. The left plot in Figure 3 displays the training and validation losses as a function of the epochs. It is evident here that these losses are on a downward trend altogether. Their values remain similar in almost all epochs, which indicates that the model is not overfitted. The values are not very large in the final iterations. Figure 3 shows the Area Under the Curve (AUC) and training in blue and validation in orange. This measure is especially practical when dealing with an uneven sample when it comes to evaluating the performance of classification. The graph shows that the AUC of training and validation sets also starts at the relatively low level but develops steadily until

they approach 1: the model does not make any misclassification. On the contrary, the model is effective in extrapolating unknown data due to the fact that the gap between the two curves does not become extremely large. To conclude, it can be observed that Figure 3 illustrates the effectiveness and stability of the suggested LSTM-DNN model, which once again proves its ability to learn the necessary behavior with the help of training data and maintain the highest performance in terms of generalization.

A. Fraudulent Transactions

Fig. 4 shows the frequency of fraudulent transactions with time, which is scaled using standardized units. The statistics indicate that it has a cyclical set of data with significant peaks at time units -1.0 and 0.0. These spikes can be linked to particular variables such as a response to increase in transaction volumes, which passes periodically or at peak times within online transactions. On the contrary, there are lower levels of frauds around -1.5 and 0.5, which implies the moments of decreased risk. The trend curve is smoothed to indicate that there is non-linear correlation between time and fraud incidence. This cyclic trend is consistent with the past literature, which also showed that the rates of fraud are periodic. However, time is in scaled units, so it is difficult to directly compare it with real-life incidents. Subsequent studies based on real time can offer more knowledge on the temporal dynamics related to fraud.

VI. Conclusion

In this work, we have proposed a hybrid model by integrating LSTM and DNN to address the two crucial problems of data imbalance and temporal dependency. Further, the model is also capable of meeting the requirement of real-time credit card fraud detection. It combines the strengths of LSTM networks to identify sequential patterns and DNNs to capture complex relationships between features. It achieves top-level performance with an accuracy of 99.6%, precision of 94.5%, recall of 91.2%, and an ROC-AUC of 97.3%.

Table 1. Performance Comparison of Different Models

Model	Study	Accuracy	Precision	Recall	F1 Score
Logistic Regression	Smith et al. (2022)	0.978	0.812	0.723	0.765
Decision Tree	Johnson and Lee (2023)	0.985	0.854	0.781	0.816
LightGBM	Chen et al. (2023)	0.992	0.912	0.865	0.888
Standalone LSTM	Wang et al. (2022)	0.994	0.928	0.892	0.910
CNN	Zhang et al. (2021)	0.993	0.921	0.880	0.900
Proposed LSTM-DNN	**This Work**	**0.996**	**0.945**	**0.912**	**0.928**

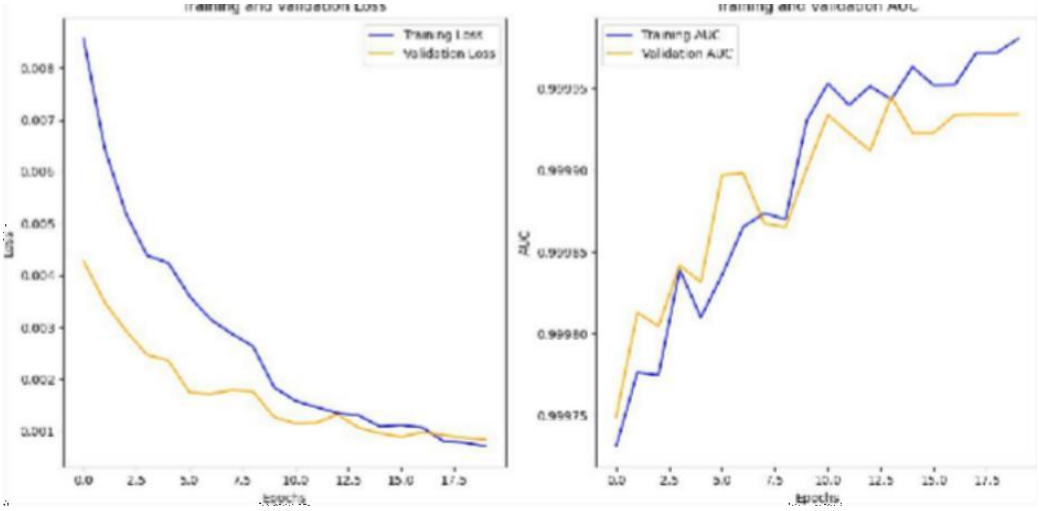

FIGURE 3. Training, Validation Loss, and ROC- AUC of the Proposed LSTM-DNN

The model is more effective than other ML and DL models incldluing Logistic Regression, Decision Trees, and Light-GBM, as evidenced by a comparative analysis. The reliability of the model in question and its generalization capability has been illustrated using visual images, such as the confusion matrix, training-validation loss curves, and AUC plots. Temporal analysis is significant in the detection of fraud because cyclical patterns in fraudulent transactions have been observed in the course of time. In general, the research contributes to the area of fraud detection, as it provides a solution which is efficient and scalable to improve the security of a web-based store and develop trust in online money transfer platforms. The study specializes in the field of energy and industry.

VII. Limitation and Future Work

The study has some limitations such as an imbalanced dataset

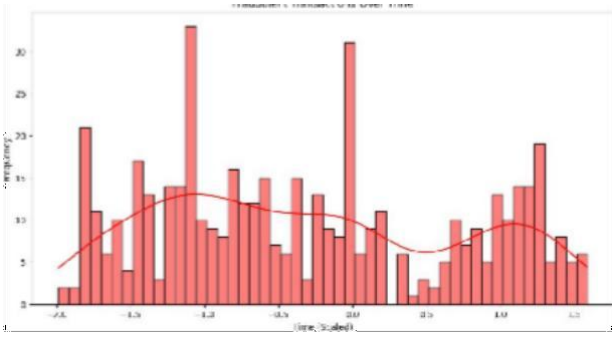

FIGURE 4. Fraudulent Transactions Over Time

and a lack of explainability. In the future, more sophisticated methods should be used to cope with an imbalanced dataset and lower the computation cost. Interpretability could also be improved in future work to achieve higher model robustness by adding more feature engineering approaches and DL structures. Besides, the mechanisms of real-time fraud detection in research should also be included, so as to conform to changing environments. The point would be further analyzed using larger and more diverse data points to affirm the study's generalizability. Lastly, interpretability analysis through the proposed method can be explored through explainable AI methodology, so as to assist in comprehending the patterns of fraud detection better and, therefore, informing its practical application in financial security systems.

References

1. P. Fu, T. Wu, and D. Sarpong, "Gamifying green: Sustainable innovation through digital platform ecosystems," Thunderbird International Business Review, 2025.
2. M. N. Alatawi, "Detection of fraud in iot based credit card collected dataset using machine learning," Machine Learning with Applications, vol. 19, p. 100603, 2025.
3. N. K. Trivedi, S. Simaiya, U. K. Lilhore, and S. K. Sharma, "An efficient credit card fraud detection model based on machine learning methods," International Journal of Advanced Science and Technology, vol. 29, no. 5, pp. 3414–3424, 2020.
4. A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Ade- joh, "Enhancing credit card fraud detection: an ensemble machine learning approach," Big Data and Cognitive Computing, vol. 8, no. 1, p. 6, 2024.
5. S. Zahoor, I. Din, Z. Unnisa, S. Iqbal, R. Alroobaea, O. Saidani, and Law, "Leveraging data-driven insights for esophageal and gastric cancer diagnosis," BMC Medical Informatics and Decision Making, vol. 25, no. 1, p. 338, 2025.
6. S. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, "Credit card fraud detection using support vector machine," in Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2021. Springer, 2022, pp. 27–37.
7. Y. K. Saheed, U. A. Baba, and M. A. Raji, "Big data analytics for credit card fraud detection using supervised machine learning models," in Big data analytics in the insurance market. Emerald Publishing Limited, 2022,pp. 31–56.
8. H. Najadat, O. Altiti, A. A. Aqouleh, and M. Younes, "Credit card fraud detection based on machine and deep learning," in 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE, 2020, pp. 204–208.
9. N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on svm-recursive feature elimination and hyper-parameters optimization," Journal of Information Security and Applications, vol. 55, p. 102596, 2020.
10. R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," in 2020 4th international conference on intelligent computing and control systems (ICICCS). IEEE, 2020, pp. 1264–1270.
11. I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and lstm deep model," Journal of Big Data, vol. 8, pp. 1–21, 2021.
12. E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learn- ing methods for credit card fraud detection using smote and adaboost," Ieee Access, vol. 9, pp. 165 286–165 294, 2021.
13. J. F. Roseline, G. Naidu, V. S. Pandi, S. A. alias Rajasree, and N. Mageswari, "Autonomous credit card fraud detection using machine learning approach," Computers and Electrical Engineering, vol. 102, p. 108132, 2022.
14. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," Ieee Access, vol. 10, pp. 39 700– 39 715, 2022.
15. N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," Electronics, vol. 11, no. 4, p. 662, 2022.
16. T. R. Noviandy, G. M. Idroes, A. Maulana, I. Hardi, E. S. Ringga, and R. Idroes, "Credit card fraud detection for contemporary financial management using XGBoost-driven machine learning and data augmentation techniques," Indatu Journal of Management and Accounting, vol. 1, no. 1, pp. 29–35, 2023