Volume (1) No (11), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Securing Unified Payments Interface: A Deep Learning Approach for Fraudulent Transaction Detection

Sandeep Gupta
SATI, Vidisha
Sandeepguptabashu@gmail.com

***Abstract*—Unified Payments Interface (UPI) is a system that integrates multiple bank accounts into a single mobile application, enabling seamless fund transfers and business payments. The proposed study presents a deep learning-based approach for detecting fraudulent UPI transactions using a large online payments fraud detection dataset containing over 6.3 million transaction records. The dataset is highly imbalanced, with fraud cases forming only a small fraction, making it a realistic yet challenging test for fraud detection methodologies. To address this, a novel model combining BiLSTM and Transformer-based encoders was developed to capture both temporal dependencies and contextual relationships in transaction sequences. The performance of the models was evaluated using accuracy, precision, recall, F1-score, and AUC-ROC metrics. Experimental results demonstrated that the BiLSTM model significantly outperformed conventional machine learning methods such as Logistic Regression, Random Forest, and Decision Tree. The BiLSTM achieved an accuracy of 99.90%, precision of 99.99%, recall of 99.81%, and F1-score of 99.91%. Visualization through accuracy/loss curves, confusion matrix, and ROC analysis further validated the model's robustness and stability. These findings confirm BiLSTM as a reliable and effective real-time fraud detection system for digital payments, enhancing the security and performance of financial transactions compared to traditional approaches.**

***Keywords*—UPI fraud detection, BiLSTM, Transformer, deep learning, online payments, financial security.**

I. INTRODUCTION

Financial institutions are responsible for the critical challenge of maintaining a seamless customer experience while swiftly and accurately identifying and isolating fraudulent transactions. A detection mechanism that reduces delays is necessary to safeguard institutions and consumers from possible problems, and the word "quickly" highlights this necessity [1][2][3]. False positives can cause wasteful allocation of resources, thus it's crucial to detect fraud precisely; "accurately" emphasizes this point.

The Indian government has been pushing for the widespread adoption of electronic payment systems, such as payment applications, since the demonetization of large currency notes in 2016 [4][5]. Previously detected vulnerabilities in payment apps, including Indian payment apps. One such app, an Indian mobile banking service, had a weakness in its PIN recovery mechanism [6][7]. New payment apps may be easily integrated and made to work with UPI thanks to its open backend architecture. There are currently more than 140 banks that support UPI transactions, and approximately 88 UPI payment apps.

One of the most prominent digital payment systems, the Unified Payments Interface (UPI) allows for safe, quick, and easy transactions. Designed to enable instant peer-to-peer and peer-to merchant payments [8][9][10], UPI leverages mobile technology to facilitate transfers using mobile numbers, QR codes, or in-app chat, thereby enhancing convenience for users. The rapid adaption and growth experienced by UPI can be said to be due to its simplicity and ease of use as well as advanced functionality.

Security is also one of the core aspects of UPI design and involves the use of encryption, multi-factor authentication, and fraud detection that secure user data and transactions. Such emphasis on security creates trust among the users in addition to ensuring the integrity of the digital payments ecosystem. The number of UPI transactions and such applications is increasing and security of such transactions cannot be overemphasized [11][12][13]. Though banks have taken serious security precautions to ensure that their customers are safe during transactions, customers are still concerned about the security of their transactions to the extent of fraud prevention and data security [14]. These concerns need to be understood and addressed to ensure further adoption of the digital payment systems and trust are maintained.

The identification of fraudulent transactions has seen extensive application of machine learning (ML) technologies. A wide range of issues are addressed by research that makes use of ML models. A number of industries can benefit from deep learning (DL) algorithms, such as finance, insurance, and computer networks [15][16], as well as mobile cellular networks' intrusion detection capabilities and healthcare institutions' monitoring services for medical fraud [17]. Among their many uses, they aid in detection, home automation, the detection of Android malware, video surveillance, the tracking of whereabouts, medical diagnosis, and the prediction of heart disease. This study delves into the real-world use of ML, particularly deep learning methods, to identify instances of credit card fraud in financial institutions. Methods from the DL subfields of ML are the main focus of DL research.

A. Significance and Contributions of the Study

The growing reliance on the Unified Payments Interface (UPI) as India's primary digital payment system has amplified

the need for robust mechanisms to safeguard transactions against fraud, as even a small fraction of fraudulent activities can undermine user trust and financial stability. Despite UPI's secure architecture incorporating encryption and multi-factor authentication, the increasing sophistication of fraudsters continues to exploit system vulnerabilities, leaving both institutions and customers at risk. This issue is then to create a fraud detection model that can detect and isolate fraud-related transactions with both a high level of accuracy but made in a relatively short time such that the genuine users face the least amount of inconvenience as possible. The value of this study lies in the fact that the research has managed to support the improvement of payment security in the digital economy by using cutting-edge deep learning methods, namely BiLSTM-based architectures, to model the sequence and context of transactions. This methodology directly meets the key challenges of imbalanced datasets, the dynamic nature of fraud patterns and the trade-off between avoiding false positives and ensuring high rates of fraud detection, which in turn foster the trust needed to drive wider use of UPI and other digital payments platforms. The main contributions to the research are the following ones:

- Using Kaggle's open-source Online Payments Fraud Detection dataset, the study provides a consistent yardstick for assessing UPI fraud detection models.
- Data cleaning, normalization, and feature extraction are crucial preprocessing operations that are conducted to guarantee high-quality data and to prepare balanced input for the model.
- The proposed model is a Bidirectional Long Short-Term Memory (BiLSTM), which can take advantage of its ability to model sequential relations and contextual patterns in the transaction flows far more effectively than the previous models could.
- The performance of the model is carefully evaluated through accuracy, precision, recall, F1-score, loss function, and AUC-ROC curves, ensuring overall evaluation of the effectiveness of fraud detection.
- Adapting the proposed paradigm to large-scale, real-time UPI transactions is addressed in the paper, which helps alleviate scalability difficulties in digital financial systems.

B. Organization of the Paper

This paper is structured as follows: Section II presents a review of related work and basics of UPI fraud detection. Section III involves the description of the proposed methodology, including preprocessing of data and building of models. Section IV compares the experimental findings of the BiLSTM model and talks about how it performed. Lastly, Section V contains the conclusion and an identification of potential directions to pursue in terms of future research.

II. Literature Review

A number of research have looked into UPI fraud detection using deep learning (DL), with the hope of addressing the limitations of standard rule-based methods in dealing with complicated, large-scale transaction settings. DL methods offer improved accuracy, efficient feature extraction, and greater scalability, making fraud detection systems more adaptive and effective in real-world financial applications.

U et al. (2025) proposed the system uses a dual phase verification approach involving the use of reliable third-party mobile number fraud detectors coupled with the use of a cloud-based data privacy validation. The model first collects the sender's mobile number and message content, then sends the collected message content via a data privacy-oriented cloud platform to a third-party verification service. The second stage is predicting scam score with the current checkpoint coefficients and assign scam score threshold dynamically using real time criteria; years of experience of the QR Scanner badge and verification of third-party scam confirmations by double checking. They used perceptron's to identify specific objects and backpropagate error values in order to minimize error values, using the M-DBN model. According to the model's confusion matrix, the M-DBN model achieved accuracy as high as 98.4%, precision of 98.1%, recall at 97.8%, and an F1-score of 98.2% [18].

R, H and R (2025) proposed system effectively identifies rogue transactions by pursuing transaction behavior and user activity. Experimental results show that the accuracy of the model based on logistics regression is 97%. Comparative analysis with decision trees, random forests, and Naive Bayesian models checks for excellent performance of logistics regression related to accuracy and recirculation measurements. The system also provides interpretation results by marking illicit transactions and creating timely warnings. Flexible solutions improve security of UPI and guarantee digital payment systems [19].

A, M and J (2025) paper explored the new approach through which an innovative algorithm, such as the Isolation Forest (IF) algorithm, has been used to combat it. It finds the unusual patterns within an imbalanced dataset without the support of labeled data. Their model has focused attention on analyzing transaction behaviors besides detecting anomalies in a given dataset. In this case, the remarkable accuracy recorded was as high as 98%, far more than common usage of techniques like Random Forest, Support Vector Machines (SVM), and Logistic Regression. Real-world datasets were used to test and under such testing, it turned highly effective for real-time fraud detection [20].

Rani, Alam and Javed (2024) article made use of a labelled dataset to train the XGBoost version in order that they may also take gain of its sturdy prediction talents and capacity to handle imbalanced datasets. To help create a system that is less difficult to apprehend and use, feature importance evaluation is used to discover essential symptoms of feasible fraud. After training, the model is covered right into a real-time UPI transaction tracking device, in which it maintains an eye fixed out for any suspicious traits in incoming transactions. In order to lessen the results of fraudulent activity, the system is constructed with 98.2% accuracy to send out instant notifications and take preventive steps. This challenge allows in improving UPI transaction security and advancing economic era are accomplished through demonstrating the performance of machine learning in fraud detection [21].

Tamilselvi et al. (2024) proposed the Unified Payment Interface (UPI) has revolutionized digital transactions in India but has also become a target for fraud. This paper presents an elevated deep learning methodology (EDLM) combining ShuffleNet and Support Vector Machine (SVM) for detecting UPI fraud. The model leverages pointwise group convolutions and channel shuffling in ShuffleNet for efficient feature extraction, which is then classified by SVM. Results show the proposed method achieves a high accuracy of 95 % and

computational efficiency compared to traditional models, thus ensuring secure and reliable UPI transactions [22].

Gupta et al. (2024) research deviated from the usual methods used in this field and adopts a fresh approach by using Recurrent Neural Network (RNN) as an advanced instrument for detecting fraudulent financial transactions. This break with tradition shows that people have now come to terms with the fact that traditional methods have their limits and that CNN and RNN have something special to convey. By applying the algorithm in UPI transaction dataset, they segregated the fraud and legitimate transaction. To evaluate the proposed approach, applied the test data on confusion matrix and got the True Positive Rate (TPR) is 87.5%, and the False Positive Rate (FPR) is 13.4% [23].

Although various models have been proposed for UPI fraud detection, most existing approaches face limitations such as poor handling of sequential dependencies, inability to adapt to evolving fraud patterns, and challenges with highly imbalanced datasets. Traditional machine learning models often rely on static features, while anomaly detection methods lack interpretability and scalability in real-time environments. Even advanced deep learning and hybrid models struggle with minimizing false positives and capturing long-range dependencies within transaction data. To overcome these challenges, the proposed solution employs a BiLSTM-based framework integrated with transformer-based feature encoding, enabling the model to capture both forward and backward temporal dependencies, extract complex feature representations, and adapt effectively to dynamic fraud behaviors. This ensures improved accuracy, reduced false alarms, and robust real-time detection, thereby strengthening the security and reliability of UPI transactions.

Table I provides a summary of existing studies on UPI fraud detection, highlighting the methodologies used, key findings, major strengths, identified limitations, and suggested recommendations from each work.

TABLE I. SUMMARY OF REVIEW ON DETECTING FRAUDS IN UPI TRANSACTIONS

Reference	Methodology	Dataset	Results / Metrics	Research Gaps	Recommendations
U et al., (2025)	Dual-phase verification with third-party fraud detectors, cloud-based privacy validation, and M-DBN (stacked RBMs + gradient descent).	UPI transaction dataset.	Accuracy: 98.4%, Precision: 98.1%, Recall: 97.8%, F1-score: 98.2%.	High computational complexity due to deep stacking; complicated initialization.	Optimize M-DBN initialization; improve scalability for real-time systems.
R, H and R, (2025)	Logistic Regression with comparative analysis against DT, RF, and Naïve Bayes.	UPI transaction dataset (labeled).	Accuracy: 97%.	Limited to static transaction features; lacks advanced sequential modeling.	Integrate temporal behavior analysis and deep learning for improved adaptability.
A, M and J, (2025)	Isolation Forest (unsupervised anomaly detection).	Imbalanced real-world UPI dataset.	Accuracy: 98% (outperformed RF, SVM, LR).	Lacks explainability; relies only on anomaly detection without labels.	Combine with supervised learning or XAI for better interpretability and fraud traceability.
Rani, Alam and Javed, (2024)	XGBoost with feature importance evaluation for imbalanced data.	Labeled UPI transaction dataset.	Accuracy: 98.2%; Real-time fraud alerts integrated.	Model explainability is good, but scalability and adaptability to evolving fraud patterns remain limited.	Enhance adaptability using online learning and integration with streaming data.
Tamilselvi et al., (2024)	Elevated DL Methodology (EDLM) combining ShuffleNet for feature extraction + SVM classifier.	UPI transaction dataset.	Accuracy: 95%.	Moderate accuracy; may struggle with large-scale real-time detection.	Enhance feature extraction using hybrid CNN-LSTM and optimize computational efficiency.
Gupta et al., (2024)	Recurrent Neural Network (RNN) for sequential fraud detection.	UPI transaction dataset.	TPR: 87.5%, FPR: 13.4%.	High false positive rate; lower accuracy compared to DL-based hybrids.	Explore advanced sequential models like BiLSTM/GRU; reduce false alarms with threshold tuning.

III. METHODOLOGY

Detecting frauds in UPI transactions requires a robust and systematic methodology to ensure secure and reliable digital payments. Data cleaning, normalization, and feature extraction are part of the pretreatment procedures taken by the Online Payments Fraud Detection dataset obtained from Kaggle. These steps ensure that the inputs to the proposed framework are of good quality. For proper model learning and evaluation, the data is subsequently partitioned into training and testing sets. A Bidirectional Long Short-Term Memory (BiLSTM) model provides the categorization. Finally, the models are evaluated based on their characteristics and their accuracy, precision, recall, F1-score, loss-based function, and area under the curve (AUC-ROC) performance. The results show that the models are effective in detecting fraudulent transactions and improving UPI security. Figure 1 flowchart of the methodology of Detecting frauds in UPI transactions is as presented below.

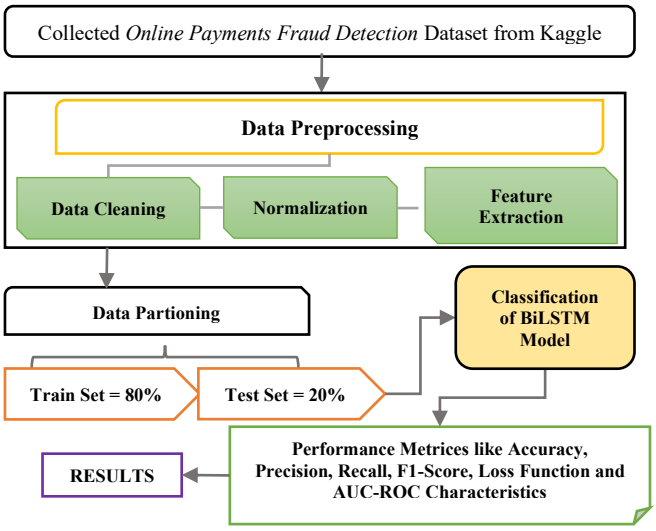

Fig. 1. Flowchart of the Proposed Framework for Detecting frauds in UPI transactions

Each step of the methodology is explained below:

A. Data Collection and Analysis

Data collection refers to the act of amassing information from diverse sources in order to conduct analysis or build models. This research uses the Online Payments Fraud Detection Dataset available on Kaggle. The dataset from Kaggle consists of 6,362,620 transaction records with 10 features, each representing details such as transaction type, amount, and account balances. The dataset is highly imbalanced, as only a very small proportion of the transactions are labeled as fraudulent, making it well-suited for evaluating fraud detection models in real-world payment systems. Some visualizations were generated to provide insights into different aspects of the dataset and are shown below:

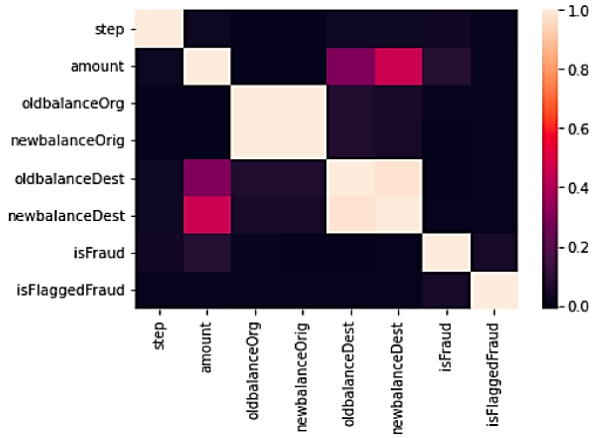

Fig. 2. Correlation Matrix

Figure 2 shows the correlation heatmap of features in the online payment's fraud detection dataset. Strong positive correlations are observed between oldbalanceOrg and newbalanceOrig, and between oldbalanceDest and newbalanceDest, reflecting transaction balance effects. The isFraud feature has moderate correlation with transaction amount and balance variables, highlighting their role in fraud detection, while is FlaggedFraud shows minimal correlation, indicating limited relevance.

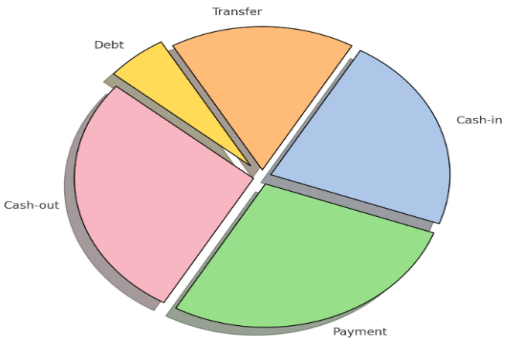

Fig. 3. Pie chart representing different types of transactions

Figure 3 illustrates the distribution of transaction types in the online payments fraud detection dataset using a pie chart. The chart indicates that Cash-out, Payment as well as Cash-in operations have the most significant share in the dataset, making these transactions the most frequent. Transfer and Debit transactions, in comparison, take a small portion of percentages. This distribution emphasizes the transactional trends in the sample where the daily financial transactions like cash withdrawal, payments and deposits are most common and transfer and debit transactions are relatively uncommon. This is a key aspect to consider in-bank during fraud detection modeling efforts because it is an indication of imbalance in the type of transactions.

B. Data Preprocessing

Reliable data analysis relies on data preprocessing, which often handles low-quality data. Cleaning, feature extraction, and normalization are all part of the preparation that the raw data goes through to make sure it's consistent and of high quality. This process makes sure the data is ready to train the model, which improves the system's learning capabilities. Analytical algorithms depend on clean and well-structured data to get reliable results, therefore without correct pretreatment, additional analysis might be infeasible. These steps are discussed below:

1) Data Cleaning:

This step aims to reduce noise and irrelevant information in a dataset to enhance data quality. Cleaning the data (missing values and duplicates) and thus, a dataset that can be analyzed. In payment systems which contain mixed types of data (i.e., categorical and numerical features) [24], an integrated strategy is required during the balancing and feature selection process.

2) Normalization

The goal of normalization is to provide a consistent scale for numerical column values in a dataset while preserving the range of possible values [25]. The values are normalized between 0 and 1, employing the min-max approach, as displayed in Equation (1), in order to address this issue. The NumPy package in Python is used to turn data into an array and reshape it.

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

X_{min} and X_{max} are the minimum and maximum values of the feature, respectively, such that the original distribution of the features is preserved.

3) Feature Extraction:

A classification model's input is the transaction features. Many characteristics are linked to each kind of transaction. A few characteristics of a transaction can be its worth and how often it occurs. The details that might be included in this information include the account that the money is going to, the time it was transferred, the location of the origin and destination, the amount, the entity (the average person, the firm performing the transfer), and the type of transaction (cash, money transfer). For the purposes of identifying and categorizing fraud, all of these are considered essential [26]. After the raw transaction data has its semantic properties extracted, the classifier is fed these features.

C. Data Portioning

The term "data splitting" describes dividing a dataset into smaller pieces for the purposes of training and testing ML models. For this research, trained on 80% of the sequences in the dataset and tested on 20%.

D. Proposed Classification Model: BiLSTM

The scalable and adaptable solutions provided by deep learning have made it a foundational technology for fraud detection. The BiLSTM algorithm is a deep learning system that can analyze massive datasets and identify intricate patterns of fraud.

The BiLSTM layer takes a novel approach by seeing the transaction sequence as two timelines, one for the forward sequence and one for the backward sequence. This is where it takes both historical data and future forecasts into account. In this approach, the model can understand the transaction's context quite well [27]. As seen in the Equation (2), the BiLSTM output considers the fact that it is fed both sides of the information:

$$BiLSTM(X) = LSTM_{\text{forward}}(X) \oplus LSTM_{\text{backward}}(X2) \quad (2)$$

With these two LSTM units producing outputs, the operation that merges them is $\oplus$ [28]. The improved data representation provided by this composite view aids the framework's pattern and anomaly detection capabilities.

The input credit card transaction data is assumed to be a time series $X = \{x_1, x_2, \ldots, x_T\}$, where each x_T is an eigenvector reflecting the transaction information at the t time step and has d dimensions [29]. Use Transformer encoders to feed this input data set. Transformer encoders have a feed-forward neural network and a self-attention mechanism built into each of their coding levels. The following Equation (3) calculates the self-attention mechanism:

$$SelfAttention(x) = \text{Decoder}\big(\text{Encoder}\,(x)\big) \quad (3)$$

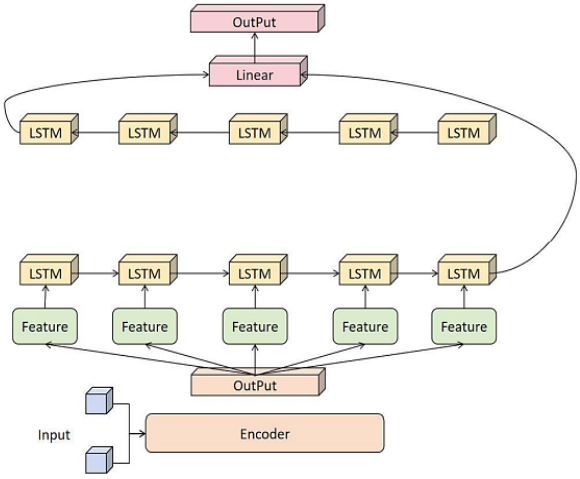

Fig. 4. Fraud Detection Model Architecture Using Transformer-BiLSTM Network

Figure 4 illustrates the architecture of the proposed BiLSTM model for UPI fraud detection. The process begins with the input layer, which is passed through an encoder to extract essential features [30]. These features are then fed into a series of LSTM layers arranged in both forward and backward directions to capture temporal dependencies and contextual information from transaction sequences. The extracted feature representations are processed through additional LSTM layers to enhance learning of sequential patterns [31]. Finally, a linear layer maps the learned features to the output layer, which generates the classification results, distinguishing between fraudulent and legitimate transactions. This hierarchical structure enables the model to effectively capture complex relationships and temporal dynamics within transaction data.

The function Encoder() reduces the dimensionality of the input sequence X. In order to restore the sequence's characteristics and transform it into the target space, Decoder() is employed. The dependent relationships between the input sequence's various time steps can be captured by the Transformer via this approach.

E. Model Evaluation

Evaluation metrics are essential instruments utilized to gauge the efficacy of fraud detection models, guaranteeing their capability to detect and alleviate fraudulent activities [32]. The accuracy, precision, recall, F1-score, and loss curve are the metrics used to measure performance. Listed below are the descriptions of various performance indicators:

- **True positive rate (TPR):** The number of suspicious transactions that the model properly detected as fraudulent.
- **False positive rate (FPR):** Quantity of valid transactions mistakenly marked as fraudulent (false alarms).
- **True negative rate (TNR):** The total amount of transactions that were accurately identified as authentic, meaning they were not fraudulent.
- **False negative rate (FNR):** The quantity of fake transactions that the model incorrectly labels as valid.

Accuracy: The proportion of valid and fraudulent transactions that were accurately categorized [33]. The following is the Equation (4) for accuracy:

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

Precision: The fraction of all transactions that were really predicted to be fraudulent that turned out to be true. This is the result of Equation (5).

$$Precision = \frac{TP}{TP+FP} \quad (5)$$

Recall: The proportion of real fraudulent transactions that the model was able to correctly identify. It is characterized as Equation (6).

$$Recall = \frac{TP}{TP+FN} \quad (6)$$

F1-score: The harmonic mean is the average of accuracy and recall, giving a balance between the two. Equation (7) reveals it.

$$F1\ Score = \frac{2\,(Precision \times Recall)}{Precision \times Recall} \quad (7)$$

Loss Function: Determining whether a class is fraudulent or not is the goal of the loss function, which calculates the discrepancy between the two sets of labels.

AUC-ROC: One may observe the model's ability to differentiate between positive and negative instances at different levels using ROC-AUC. An increase in the ROC-AUC within the context of fraud detection indicates a more robust ability to distinguish between valid and fraudulent transactions. This data should be taken into account while attempting to detect online transaction fraud with a minimum of false positives.

By using these metrics, the system's performance can be objectively evaluated and adjusted for optimal fraud detection results.

IV. Result Analysis and Discussion

The proposed solution is to identify fraud in UPI transactions. In order to test the effectiveness of the BiLSTM model, an online fraud payment detection dataset was used in

experimentation. The modeling was done on a Lenovo Ideapad 500 workstation with Windows 10 Pro (64-bit). The technical specification was 8 GB RAM and the processor based on Intel(R) Core (TM) i5-6200U with a base frequency 2.30 GHz, and maximum frequency 2.40 GHz. All models are scripted in Python with the help of the corresponding libraries. Table II shows the performance of the BiLSTM model in identification of fraudulent cases in UPI transactions. The accuracy of the model was extremely high at 99.90%, which is a sign of its general credibility in the predictions it makes about the classification of transactions. Precision rate of 99.99% indicates that the model has a high potential to reduce false alarms, and actual transactions are hardly flagged as fraud-those. Equally, the overall recall of 99.81% illustrates how well the model would capture practically all of the fraudulent transactions and reduce the risk of false negatives. Its F1-score of 99.91% shows that the BiLSTM performs well in precision and recall, proving it to be robust yet acceptable to real-life fraud detection purposes in UPI-based systems.

TABLE II. PERFORMANCE OF BILSTM FOR DETECTING FRAUDS IN UPI TRANSACTIONS

Matrix	BiLSTM
Accuracy	99.90
Precision	99.99
Recall	99.81
F1 Score	99.91

	Precision	Recall	F1-Score	Support
0 (Not Fraud)	0.99	0.96	0.98	834
1 (Fraud)	0.96	0.99	0.98	816
Accuracy			0.98	1650
Macro avg	0.98	0.98	0.98	1650
Weighted avg	0.98	0.98	0.98	1650

Fig. 5. Classification report of Bi-LSTM model

Figure 5 shows the classification report of the Bi-LSTM model routinely used to train a binary classification model having classes: 0 (Not Fraud), 1 (Fraud). An overall accuracy of 0.98 is reached by the model. In the case of class 0, precision, recall and F1-score are 0.99, 0.96, and 0.98 respectively with 834 instances. Class 1 shows the precision, recall and F1-score as resources availed are 0.96, 0.99 and 0.98, respectively, faculties by 816 instances. Both macro and weighted averages of precision, recall and F1-score are 0.98 that is, there is a balanced performance between the two classes.

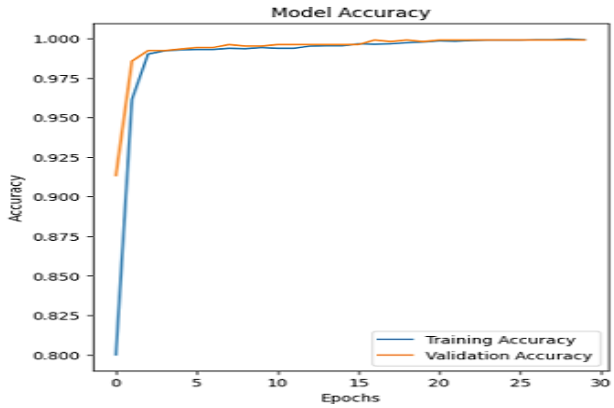

Fig. 6. Accuracy and Validation Accuracy of the BiLSTM Model

Figure 6 shows the training and validation accuracy of BiLSTM model on 30 epochs. The findings indicate that the training and cross-validation accuracy have increased rapidly on initial epochs with accuracy rate greater than 97%. As the epochs increase, the curves tend towards equilibrium around 99.90% showing good learning ability and learning stability of the model. The significance of the consistency between the training and the validation accuracy is indicating that the BiLSTM does not experience overfitting, and that it can provide strong generalization in relation to predicting fraudulent UPI transactions.

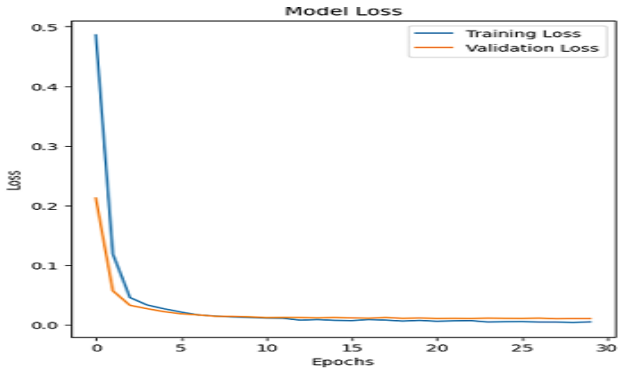

Fig. 7. Loss and Validation Loss of the BiLSTM Model

Figure 7 shows the training and the validation loss of the BiLSTM model during 30 episodes. The initial loss in training is quite high with a value of about 0.5 whereas the validation loss is somewhere around 0.25. As one continues training, both of the losses reduce dramatically during the early few epochs and keep on falling till they approach zero at the end. The near overlap of the loss of training and validation curves denotes that the model has precisely minimized the errors as well as provided good generalization in absence of overfitting. This trend shows that the BiLSTM-based model is also efficient and stable with regard to distinguishing between suspected and genuine UPI transactions.

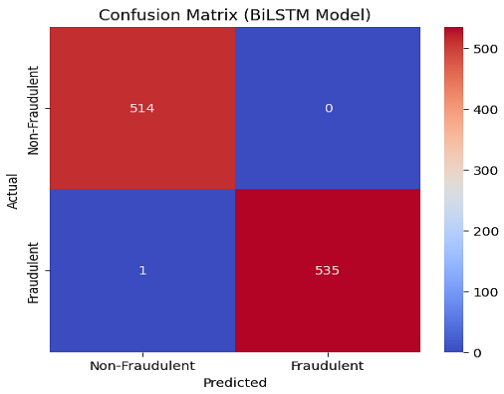

Fig. 8. Confusion Matrix of BiLSTM Model

The confusion matrix in Figure 8 lays more emphasis on the usefulness of the BiLSTM model in detecting fraud. The model made 514 non-fraudulent transactions and 535 fraudulent transactions the correct classification as true negatives and true positives respectively. These outcomes indicate the excellent level of the model capability in accurately identifying a genuine and fraudulent UPI transaction, hence establishing its integrity in implementing the model in practical usages.

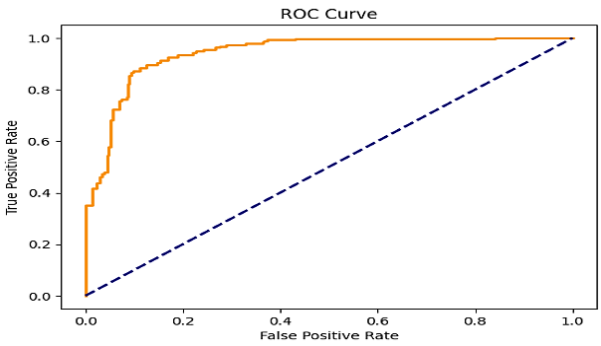

Fig. 9. ROC Characteristics of BiLSTM

Figure 9 shows the ROC curve of BiLSTM model to detect UPI fraud. The curve shows its robust nature under the fact that the curve increases rapidly steeply in the top left corner revealing high true positive rate with low false positive rate. This indicates that the model works well to identify fraudulent and non-fraudulent speeches. The area under the curve (AUC) which is nearly equal to one again confirms the strength and dependability of the BiLSTM model in perfect identification of fraud in UPI transaction.

A. Comparison and Discussion

Table III carries a comparative study of the proposed BiLSTM model and the other existing benchmarking models, which are namely Logistic Regression (LR), Random Forest (RF), and Decision Tree (DT), in detecting in fraudulent UPI transactions. Baseline RF, DT, and LR had the accuracy of 93.0%, 94.67 and 89.8%, respectively. The proposed BiLSTM model compared to the rest showed considerably great results with an accuracy of 99.90%, the precision was measured to be 99.99%, the recall was 99.81%, and the F1-score was 99.91%. These findings provide clear evidence of the potential efficacy of BiLSTM model in accurately detecting/preventing fraudulent activities, and have high reliability and robustness than manipulated determinant-based machine learning methods.

TABLE III. PERFORMANCE COMPARISON OF PROPOSED MODEL WITH BENCHMARKING MODELS FOR DETECTING FRAUDS IN UPI TRANSACTIONS

Matrix	Accuracy	Precision	Recall	F1 Score
LR [34]	89.8	86.18	89	90
RF [35]	93.0	93.0	93.0	93.0
DT [36]	94.67	89.75	86.44	88.07
BiLSTM	99.90	99.99	99.81	99.91

The constructed BiLSTM model would have great benefits to uncover fraud in UPI transactions over the normal machine learning mechanisms. The possibility to capture long-term dependencies and sequential patterns in transaction data makes it also more reliable in drawing differences between the simulation of real and fraudulent behavior. The BiLSTM model exploits deep learning to automatically learn and infer complex features in addition to adjusting to new and evolving fraud patterns. This makes it more stable and to manage the dynamic and imbalanced financial data. In addition, the model has a great generalization ability, which decreases chances of overfitting hence it performs consistently in various transaction situations. Generally, the enhanced learning algorithm and versatility enable the BiLSTM to outsmart the modelling standards, and it is a strong candidate solution to real-time fraud detection in the UPI environment.

B. Novelty and Justification of the Study

The innovation of this work is in the interpolation of Bidirectional Long Short-Term Memory (BiLSTM) and transformer-based feature encoding framework in fraudulent transaction detection in Unified Payments Interface (UPI) systems, which still lacks in the current literature where there is an over-reliance on conventional machine learning models like Logistic Regression, Decision Tree, and Random Forest. Compared to traditional models, which suffer serial dependency and a dynamic of fraud patterns, the proposed framework takes advantage of the ability of BiLSTM to perceive the past and the future in transaction sequences, as well as feature transformer encoders to capture the complexity of temporal relations. This integration provides a strong selection of minute and dynamic fraudulent operations in the very sparse fiscal datasets. The rationale behind this practice is the necessity of a scalable, flexible, and responsible model of fraud detection that can maintain a large number of digital payment transactions, the reduction of false-positive feedback, and the proposal of high detection of accuracy, precision, recall and F1- score with preference over baseline models, thus enhancing overall system security and trustworthiness of financial systems based on UPI.

V. CONCLUSION AND FUTURE SCOPE

The UPI Fraud Detection System is designed as an efficient method to identify and counter fraudulent activities in digital payment systems using advanced machine learning techniques. By leveraging diverse data types such as transaction records, sound, text, and images, the system can detect multiple fraud categories, including vishing, impersonation, false payments, and QR code fraud. This study focused on fraud detection in UPI transactions through a Bidirectional Long Short-Term Memory (BiLSTM) network. Using the Online Payments Fraud Detection dataset, which captures sequential relationships in transactional data, the BiLSTM model successfully identified complex fraud patterns. Experimental analysis showed that BiLSTM outperformed traditional models like Logistic Regression, Random Forest, and Decision Tree, achieving a remarkable accuracy of 99.90%. These results highlight the model's reliability and superiority over approaches that rely on static patterns and hand-crafted features. The study confirms the feasibility of BiLSTM in real-world early-warning fraud detection systems, where precision and recall are crucial to reducing financial losses and safeguarding customers. Looking ahead, improvements may include integrating attention mechanisms, graph-based learning, and hybrid deep learning models to enhance performance. Additionally, applying BiLSTM to real-time streaming data and incorporating explainable AI (XAI) will strengthen interpretability and adaptability in future payment systems.

REFERENCES

[1] M. Tayebi and S. El Kafhali, "Generative Modeling for Imbalanced Credit Card Fraud Transaction Detection," *J. Cybersecurity Priv.*, vol. 5, no. 1, 2025, doi: 10.3390/jcp5010009.

[2] M. Hassan, L. A.-R. Aziz, and Y. Andriansyah, "The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance," *Rev. Contemp. Bus. Anal.*, vol. 6, no. 1, pp. 110–132, 2023.

[3] V. Verma, "Security Compliance and Risk Management in AI-Driven Financial Transactions," *Int. J. Eng. Sci. Math.*, vol. 12, no. 7, pp. 1–15, 2023.

[4] B. Chaudhari, S. C. G. Verma, and S. R. Somu, "Next-Generation

Authentication and Authorization Models for Secure Financial Microservices APIs: Challenges, Innovations, and Best Practices," *Int. J. Curr. Sci.*, vol. 14, no. 1, 2024, doi: 10.56975/ijcsp.v14i1.303089.

[5] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[6] R. Kumar, S. Kishore, H. Lu, and A. Prakash, "Security analysis of unified payments interface and payment apps in India," in *Proceedings of the 29th USENIX Security Symposium*, 2020.

[7] J. Mishra, B. B. Biswal, and N. Padhy, "Machine Learning for Fraud Detection in Banking Cyber security Performance Evaluation of Classifiers and Their Real-Time Scalability," in *2025 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, IEEE, Feb. 2025, pp. 431–436. doi: 10.1109/ESIC64052.2025.10962752.

[8] P. Ambadkar, S. Ambure, H. Bhoir, S. Indalkar, and P. V. Bhosale, "EZPAY - ENHANCING UPI USABILITY AND SECURITY," no. 04, pp. 8998–9002, 2024.

[9] S. Gajula, "Cloud Transformation in Financial Services: A Strategic Framework for Hybrid Adoption and Business Continuity," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 1244–1254, Mar. 2025, doi: 10.32628/CSEIT25112464.

[10] D. Patel, "Enhancing Banking Security: A Blockchain and Machine Learning- Based Fraud Prevention Model," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, Dec. 2023, doi: 10.14741/ijcet/v.13.6.10.

[11] D. S. S. Jagtap, "Evaluating User Perceptions and Security Concerns in Unified Payments Interface (UPI) Services," *Int. J. Res. Publ. Rev.*, vol. 5, no. 8, pp. 2219–2223, 2024, doi: 10.55248/gengpi.5.0824.2136.

[12] V. Verma, "Deep Learning-Based Fraud Detection in Financial Transactions: A Case Study Using Real-Time Data Streams," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 149–157, 2023, doi: 10.56472/25832646/JETA-V3I8P117.

[13] B. Chaudhari, S. C. G. Verma, and S. R. Somu, "A Review of Secure API Gateways with Java Spring for Financial Lending Platforms," *Int. J. Curr. Sci.*, vol. 14, no. 4, pp. 315–326, 2024, doi: 10.56975/ijcsp.v14i4.303090.

[14] S. J. Wawge, "A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[15] M. Jabeen, S. Ramzan, A. Raza, N. L. Fitriyani, M. Syafrudin, and S. W. Lee, "Enhanced Credit Card Fraud Detection Using Deep Hybrid CLST Model," *Mathematics*, vol. 13, no. 12, p. 1950, Jun. 2025, doi: 10.3390/math13121950.

[16] A. Sharma and S. Kabade, "Optimization Algorithms for Pension Asset Allocation Under Market Volatility," *TIJER – Int. Res. J.*, vol. 11, no. 9, 2024.

[17] R. Q. Majumder, "Machine Learning for Predictive Analytics: Trends and Future Directions," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3557–3564, May 2025, doi: 10.38124/ijisrt/25apr1899.

[18] R. U, M. P. Raj, J. N. Mithra, S. B. S, A. N. L, and J. M. Dass Y, "A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles," in *2025 International Conference on Electronics and Renewable Systems (ICEARS)*, 2025, pp. 1551–1558. doi: 10.1109/ICEARS64219.2025.10941576.

[19] R. R, S. C. H, and G. R, "Leveraging Machine Learning Techniques of Real Time Detection of UPI Fraud," in *2025 7th International Conference on Intelligent Sustainable Systems (ICISS)*, 2025, pp. 1506–1510. doi: 10.1109/ICISS63372.2025.11076419.

[20] K. S. A, P. M, and S. J, "Enhancing UPI Fraud Detection Accuracy Using Isolation Forest: A Novel Machine Learning Approach," in *2025 International Conference on Emerging Technologies in Engineering Applications (ICETEA)*, IEEE, Jun. 2025, pp. 1–5. doi: 10.1109/ICETEA64585.2025.11099839.

[21] R. Rani, A. Alam, and A. Javed, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, 2024, pp. 924–928. doi: 10.1109/ICDT61202.2024.10489682.

[22] M. Tamilselvi, R. Begum, K. K, J. Giri, D. Sheela, and M. O. Sabri, "Experimental Evaluation Unified Payment Interface (UPI) Fraud Detection System Using Elevated Deep Learning Methodology," in *2024 2nd International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)*, 2024, pp. 40–45. doi: 10.1109/ICETEMS64039.2024.10965083.

[23] V. Gupta, S. Sharma, S. Nimkar, and S. Pathak, "UPI Based Financial Fraud Detection Using Deep Learning Approach," in *2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET)*, 2024, pp. 1–6. doi: 10.1109/ACROSET62108.2024.10743663.

[24] H. M. R. Al Lawati *et al.*, "An Integrated Preprocessing and Drift Detection Approach With Adaptive Windowing for Fraud Detection in Payment Systems," *IEEE Access*, vol. 13, pp. 92036–92056, 2025, doi: 10.1109/ACCESS.2025.3569609.

[25] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[26] M. M. Ismail and M. A. Haq, "Enhancing Enterprise Financial Fraud Detection Using Machine Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 4, pp. 14854–14861, Aug. 2024, doi: 10.48084/etasr.7437.

[27] A. Alourani, F. Ashfaq, N. Jhanjhi, and N. Khan, "BiLSTM- and GNN-Based Spatiotemporal Traffic Flow Forecasting with Correlated Weather Data," *J. Adv. Transp.*, vol. 2023, pp. 1–17, 2023, doi: 10.1155/2023/8962283.

[28] K. Sudharson, S. Varsha, S. Rajalakshmi, D. Rajalakshmi, and R. Santhiya, "Financial Transactional Fraud Detection using a Hybrid BiLSTM with Attention-Based Autoencoder," *Int. Res. J. Multidiscip. Technovation*, vol. 7, no. 2, pp. 135–147, 2025, doi: 10.54392/irjmt25211.

[29] P. Feng, "Hybrid BiLSTM-Transformer Model for Identifying Fraudulent Transactions in Financial Systems," *J. Comput. Sci. Softw. Appl.*, vol. 5, no. 3, 2025.

[30] N. Malali, "Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance," in *2025 International Conference on Advanced Computing Technologies (ICoACT)*, IEEE, Mar. 2025, pp. 1–6. doi: 10.1109/ICoACT63339.2025.11005357.

[31] H. Kali, "Optimizing Credit Card Fraud Transactions Identification and Classification in Banking Industry Using Machine Learning Algorithms," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 11, pp. 85–96, 2024.

[32] J. Singh and P. Kaur, "Fraud Detection in Online Transactions Using Machine Learning." 2023. doi: 10.13140/RG.2.2.29971.66088.

[33] G. Mantha, "Transforming the Insurance Industry with Salesforce: Enhancing Customer Engagement and Operational Efficiency," *North Am. J. Eng. Res.*, vol. 5, no. 3, 2024.

[34] P. J. Basilio, "Online Payment Fraud Detection using Machine Learning Techniques Taranjyot Singh Chawla National College of Ireland Supervisor :," pp. 1–21, 2022.

[35] A. R and R. M, "Fraud Detection in Online Payment Using Machine Learning Techniques," *ijariie*, vol. 10, no. 2, pp. 1640–1646, 2024.

[36] K. Singh, R. Tiwari, and N. Agarwal, "Online Payment Fraud Detection Using Machine Learning," *YMER- An Int. Peer-Reviewed J.*, vol. 24, no. 04, pp. 1699–1709, 2025.

