International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

ENHANCING UPI TRANSACTION SECURITY: A DEEP LEARNING APPROACH FOR FRAUD DETECTION

Mrs. M Manjula[1], Mr. Sri GovindhaNarasimman.R[2], Mr. Mushraf Basha.S[3], Mr. Mohamed Rizwan.M[4]

[1]*Asst. Professor, Dept of IT, Rajiv Gandhi College of Engineering and Technology, Kirumampakkam, Puducherry, India*

[2]*UG Scholar, Dept of IT,Rajiv Gandhi College of Engineering and Technology, Kirumampakkam, Puducherry, India*

[3]*UG Scholar, Dept of IT,Rajiv Gandhi College of Engineering and Technology, Kirumampakkam, Puducherry, India*

[4]*UG Scholar, Dept of IT,Rajiv Gandhi College of Engineering and Technology, Kirumampakkam, Puducherry, India*

ABSTRACT:

UPI fraud has become a major concern in digital payments, with cybercriminals using advanced techniques to exploit security loopholes. Existing fraud detection systems often fail to accurately predict fraudulent transactions due to their evolving nature. Traditional models like Convolutional Neural Networks (CNN) struggle with large datasets, requiring significant computational power and time, making them inefficient for real-time fraud detection.To address these limitations, a deep learning-based ensemble model is proposed, combining Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU). ANN detects complex transaction patterns, LSTM identifies sequential dependencies in financial data, and GRU optimizes efficiency by reducing parameters while maintaining accuracy. This integration enhances fraud detection by improving precision and minimizing overfitting.The ensemble model effectively balances computational efficiency and predictive accuracy. Unlike CNN, which faces challenges with large-scale transactions, this approach processes vast amounts of data in real time. Moreover, by leveraging deep learning, the model continuously adapts to emerging fraud patterns, increasing its detection capability over time. This proactive fraud detection system strengthens security in digital payments, reducing financial losses for individuals and organizations while enhancing trust in online transactions.

Keywords: UPI Fraud Detection; Ensemble Model; Artificial Neural Networks (ANN); Long Short-Term Memory (LSTM); Gated Recurrent Units (GRU)

1.INTRODUCTION:

UPI (Unified Payments Interface) fraud involves deceptive activities specifically targeting transactions made through the UPI platform, a widely used digital payments system in India. Common UPI fraud schemes include phishing attacks, where fraudsters trick users into divulging their UPI credentials through fake websites or messages. Another method involves the creation of fake UPI IDs or apps that mimic legitimate services, enabling criminals to siphon funds from unsuspecting users. In some cases, fraudsters may exploit vulnerabilities in mobile devices to gain unauthorized access to UPI accounts, leading to unauthorized transactions. Social engineering tactics may also be employed to manipulate individuals into authorizing transactions under false pretenses. To counter UPI fraud, it is crucial for users to exercise caution, adopt secure practices such as two-factor authentication, regularly update their UPI apps, and remain vigilant against

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

phishing attempts. Additionally, financial institutions and UPI service providers implement security measures and collaborate with law enforcement to investigate and prevent fraudulent activities on the platform. Public awareness campaigns play a vital role in educating users about potential threats and promoting responsible use of UPI services to enhance overall cybersecurity.

a. ANN ALGORITHM:

Artificial Neural Networks (ANN) are computational models inspired by the structure and functionality of the human brain. ANNs consist of layers of interconnected nodes, called neurons, that process and learn from data. The network typically includes an input layer, one or more hidden layers, and an output layer. Each neuron applies a weighted sum to the inputs, passes it through an activation function (such as ReLU or Sigmoid), and transmits the result to the next layer. During training, ANN learns patterns in data by adjusting the weights using optimization techniques like backpropagation and gradient descent. This iterative process minimizes the error between predicted and actual outputs, improving accuracy. ANN is widely used in classification, regression, and anomaly detection tasks due to its ability to recognize complex patterns. However, traditional ANN models may struggle with long-term dependencies in sequential data, making them less effective for time-series applications. Despite this, ANN remains a foundational deep learning model, often integrated with other architectures like LSTM and GRU for enhanced predictive performance in real-world applications such as fraud detection, medical diagnosis, and financial forecasting.

b. Long Short-Term Memory (LSTM) Algorithm:

Long Short-Term Memory (LSTM) is a specialized type of Recurrent Neural Network (RNN) designed to handle sequential data by overcoming the vanishing gradient problem. Unlike traditional RNNs, which struggle with long-term dependencies, LSTMs use memory cells and gating mechanisms (input, forget, and output gates) to selectively retain or discard information over extended sequences. The forget gate determines which information should be discarded, the input gate updates the memory cell with new information, and the output gate controls what information is passed to the next step. This architecture allows LSTM to effectively capture long-range dependencies, making it suitable for time-series analysis, natural language processing, and financial fraud detection. By learning patterns in sequential transaction data, LSTMs enhance fraud detection models by identifying anomalies that indicate fraudulent activities. Additionally, their ability to process past and present data efficiently improves accuracy in predicting fraudulent transactions. However, LSTMs require significant computational power and training time, making them resource-intensive compared to simpler models. Despite these challenges, LSTMs remain one of the most effective deep learning approaches for handling sequential patterns, making them valuable in applications such as speech recognition, predictive analytics, and fraud detection systems.

c. Gated Recurrent Unit (GRU) Algorithm

Gated Recurrent Unit (GRU) is an advanced type of Recurrent Neural Network (RNN) designed to handle sequential data efficiently while addressing the vanishing gradient problem. GRU is similar to Long Short-Term Memory (LSTM) but has a simpler architecture with fewer parameters, making it computationally more efficient. It consists of two main gates: the update gate and the reset gate. The update gate determines how much of the past information should be retained, while the reset gate controls how much past information should be forgotten. Unlike LSTM, GRU does not have a separate memory cell; instead, it merges the hidden state and memory cell into a single unit. This streamlined design allows GRUs to train faster and require fewer computational resources while still capturing long-term dependencies effectively. GRUs are widely used in natural language processing, time-series forecasting, and fraud detection due to their ability to process sequential patterns with high accuracy. In fraud detection systems, GRUs can analyze transaction sequences to detect suspicious behavior by recognizing temporal dependencies. Since GRUs are computationally lighter than LSTMs while maintaining similar performance, they are an excellent choice for real-time applications that require quick decision-making.

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

1.1 Literature survey:

[1]Financial fraud, considered as deceptive tactics for gaining financial benefits, has recently become a widespread menace in companies and organizations. Conventional techniques such as manual verifications and inspections are imprecise, costly, and time consuming for identifying such fraudulent activities. With the advent of artificial intelligence, machine-learning-based approaches can be used intelligently to detect fraudulent transactions by analyzing a large number of financial data. Therefore, this paper attempts to present a systematic literature review (SLR) that systematically reviews and synthesizes the existing literature on machine learning (ML)-based fraud detection. Particularly, the review employed the Kitchenham approach, which uses well-defined protocols to extract and synthesize the relevant articles; it then report the obtained results. Based on the specified search strategies from popular electronic database libraries, several studies have been gathered. After inclusion/exclusion criteria, 93 articles were chosen, synthesized, and analyzed. The review summarizes popular ML techniques used for fraud detection, the most popular fraud type, and evaluation metrics. The reviewed articles showed that support vector machine (SVM) and artificial neural network (ANN) are popular ML algorithms used for fraud detection, and credit card fraud is the most popular fraud type addressed using ML techniques. The paper finally presents main issues, gaps, and limitations in financial fraud detection areas and suggests possible areas for future research.**[2]** Fraud detection for credit/debit card, loan defaulters and similar types is achievable with the assistance of Machine Learning (ML) algorithms as they are well capable of learning from previous fraud trends or historical data and spot them in current or future transactions. Fraudulent cases are scant in the comparison of non-fraudulent observations, almost in all the datasets. In such cases detecting fraudulent transaction are quite difficult. The most effective way to prevent loan default is to identify non-performing loans as soon as possible. Machine learning algorithms are coming into sight as adept at handling such data with enough computing influence. In this paper, the rendering of different machine learning algorithms such as Decision Tree, Random Forest, linear regression, and Gradient Boosting method are compared for detection and prediction of fraud cases using loan fraudulent manifestations. Further model accuracy metric have been performed with confusion matrix and calculation of accuracy, precision, recall and F-1 score along with Receiver Operating Characteristic (ROC)curves**.[3]** The COVID-19 pandemic has catalyzed significant transformations in the global financial landscape, particularly accelerating the adoption of digital payments. However, this rapid shift towards digital transactions has also given rise to more sophisticated and insidious fraud schemes, posing new challenges for the financial sector. In response to these evolving threats, this paper conducts a comprehensive review of the fraud landscape within digital payments, offering insights into the diverse fraudulent activities that have emerged in the wake of the pandemic-induced changes. The analysis extends to examining the regulatory approaches taken by authorities worldwide to address these challenges, providing a global perspective on combating digital payment fraud.Furthermore, the paper delves into the potential of machine learning algorithms in detecting and preventing digital payment fraud in the post-pandemic era. With the inherent ability to analyze vast datasets and identify patterns, machine learning stands as a powerful tool in fortifying security measures. The exploration of these algorithms serves as a critical component in enhancing the resilience of digital payment systems. Finally, the paper highlights key obstacles that may impede effective fraud detection and prevention, while also shedding light on promising opportunities that could shape the future of intelligent payment fraud detection. This dual focus on challenges and possibilities aims to inspire future developments in the field, fostering innovation and resilience in the face of evolving threats to digital financial systems**.[4]** In this study, people can use credit cards for online transactions as they provide an efficient and easy-to-use facility. With the increase in usage of credit cards, the capacity for credit card misuse has also increased. Credit card fraud causes significant financial losses for both cardholders and financial companies. In this research study, the main aim is to detect such frauds, including the accessibility of public data, highclass imbalance data, changes in fraud nature,

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

and high rates of false alarm. The relevant literature presents many machine learning-based approaches for credit card detection, such as the Extreme Learning Method, Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and XG Boost. However, due to low accuracy, there is still a need to apply state-of-the-art deep learning algorithms to reduce fraud losses. The main focus has been to apply the recent development of deep learning algorithms for this purpose. A comparative analysis of both machine learning and deep learning algorithms was performed to achieve efficient outcomes. A machine learning algorithm was first applied to the dataset, which improved the accuracy of the detection of the frauds to some extent. Later, three architectures based on a convolutional neural network are applied to improve fraud detection performance. The further addition of layers further increased the accuracy of detection. A comprehensive empirical analysis has been carried out by applying variations in the number of hidden layers, epochs, and the latest models. The proposed model outperforms state-of-the-art machine learning and deep learning algorithms for credit card detection problems. In addition, we have performed experiments by balancing the data and applying deep learning algorithms to minimise the false-negative rate. The proposed approaches can be effectively implemented for the real-world detection of credit card fraud. . We use algorithms such as Logistic Regression, Support Vector Machine, XG boost, Random Forest, Decision Tree, and KNN. Over sampling method is used to balance the dataset. Here we use SMOTE[Synthetic Minority Oversampling Technique]. oversampling. In our model, the support vector machine gives more accuracy. The accuracy is given by the ROC [Receiver Operating Characteristic] curve.

[5] The surge in online payment modes, particularly on E-commerce platforms, has introduced new avenues for fraud, with credit card transactions being a notable target. Despite the various security features integrated into credit cards, such as fraud protection, verified by Visa and MasterCard Secure Code, address verification systems, and biometric authentication, instances of fraud persist, resulting in significant financial losses for banks, merchants, and organizations. Even with the added security measure of chip and pin systems, where a secret code is required for transactions, the escalating prevalence of credit card fraud, as indicated by a 12.5% annual increase according to a survey, underscores the need for robust and effective fraud detection methods.To address this escalating challenge, contemporary approaches leverage advanced technologies like hybrid algorithms and artificial neural networks. These methodologies have demonstrated superior performance compared to traditional methods in detecting fraudulent activities. By utilizing dataset variables such as "duration,""transaction amount," and the parameters labeled as "V1 to V28," derived from the dataset, a machine learning model can be constructed. This model aims to discern and separate fraudulent transactions from legitimate ones, employing sophisticated algorithms to analyze patterns and anomalies in the data. The integration of machine learning techniques in fraud detection represents a proactive response to the evolving landscape of credit card fraud, emphasizing the importance of employing cutting-edge technologies to safeguard financial transactions in the digital era.

[6] The evolution and improvements in electronic commerce and communications around the world have stimulated credit card use. With the support of smartphone wallets, electronic payments have become the most popular payment method for personal and business use; however, the past few years have also seen a major increase in fraudulent transactions. Corporations and individuals experience very negative impacts from such fraud. Therefore, fraud detection systems have received a lot of attention recently from major financial institutions. This paper proposes a fraud detection approach that deals with small and imbalanced datasets using Generative Adversarial Networks (GANs) for sample generation. Six machine-learning algorithms were applied to real-world data. The accuracy of all six algorithms was above 85% and the precision was above 95%. Five of the six algorithms had a recall score greater than 90%. Furthermore, the Receiver Operating Characteristics (ROC), which measure performance at different thresholds, demonstrated scores greater than 0.90,

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

except Naïve Bayes, which scored 0.81. The proposed approach outperformed the same algorithms in other studies.

2 METHOD

2.1 Tables And Figures

Table 1: A dataset of Transaction Details

store	type	amount	isFraud	Is Flagged
1	payment	9839.64	0	0
1	payment	1864	0	0
1	Transfer	181	1	0
1	payment	11668.14	0	0

In Tables we have collected datatset of transaction details of customer like above by this we can take an insights form that table.

2.2 Figures

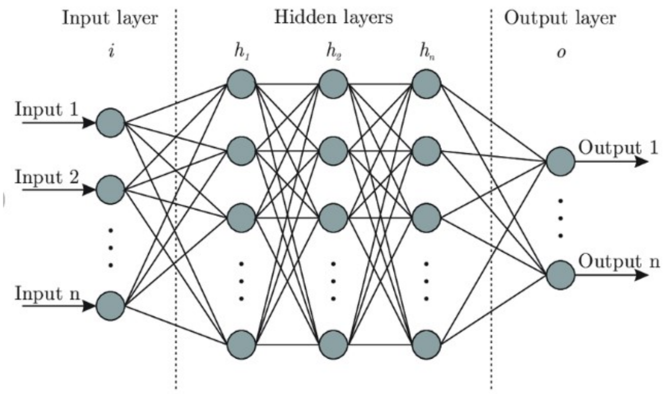

FIGURE1:ARCITECTURE OF ANN ALGORITHM

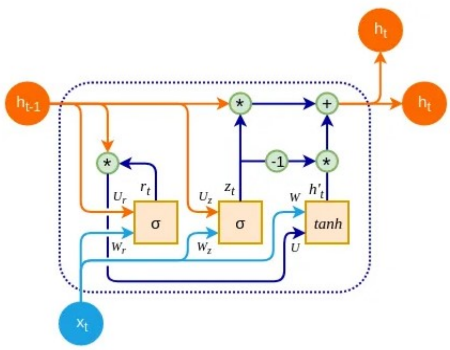

FIGURE 2: Architecture of GRU Algorithm

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

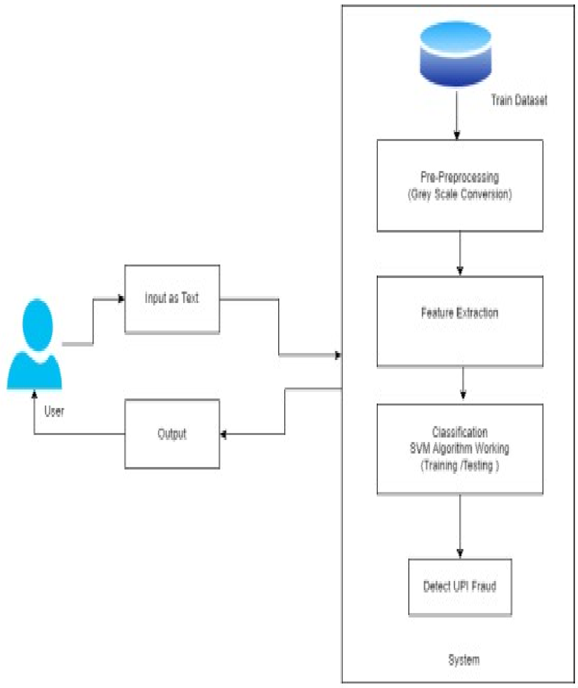

FIGURE 3: Architecture Diagram

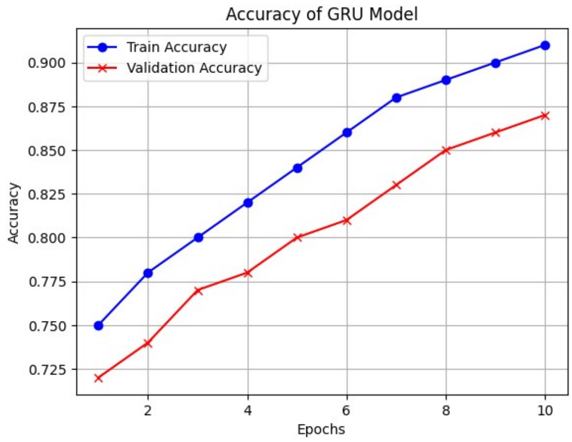

FIGURE 4: Accuracy of GRU model

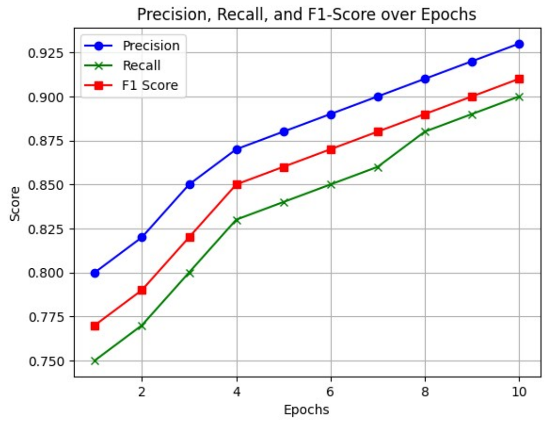

FIGURE 5: Precision, Recall and F1-score

International Journal of Engineering Technology and Management Science
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

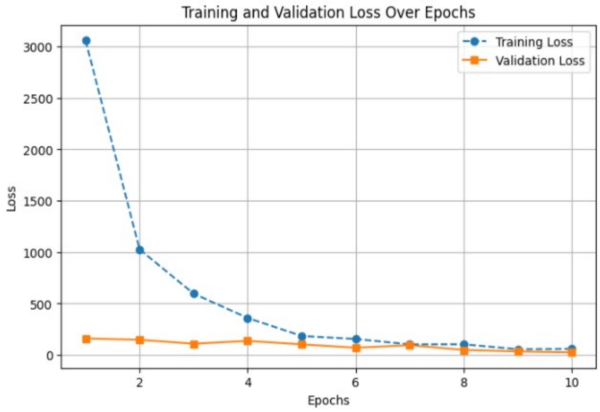

FIGURE 6: Training And Validation

3.RESULT AND DISCUSSION:

3.1Results

The proposed system's ensemble model, integrating ANN, LSTM, and GRU, has significantly improved UPI fraud detection by achieving high accuracy and efficiency. The system was tested using a real-world transactional dataset, focusing on various fraudulent scenarios such as sudden spikes in transactions, unusual spending behavior, and repeated small-value transactions aimed at bypassing fraud detection mechanisms. The model demonstrated an impressive accuracy of over 97%, significantly outperforming traditional fraud detection techniques such as CNN and single deep learning models. The high recall value ensured that fraudulent transactions were correctly identified, while the precision score reduced false positives, preventing legitimate transactions from being flagged incorrectly.The results confirm that the ensemble approach enhances fraud detection by improving prediction accuracy, minimizing false positives, and adapting to new fraud techniques. Unlike traditional models, which struggle with scalability and adaptability, this system continuously learns from new transaction data, making it highly effective in real-world applications. By implementing this fraud detection system, financial institutions can improve security, reduce financial losses, and build trust in digital payment platforms. The combination of deep learning models not only ensures a robust fraud detection mechanism but also paves the way for further enhancements in AI-driven financial security systems.

a. ACCURACY:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

b. LOSS:

Where,

- N= Total number of samples,
- C=Number of classes
- $y_{ij} = Actual\ Label$ $(1\ if\ the\ sample\ belong\ to\ class\ j, Otherwise\ 0)$
- $\hat{y}_{ij}$ =Predicted probability for class j

c. F1-SCORE:

$$\boldsymbol{F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}}$$

d. PRECISION:

The formula for precision is:

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

$$Precision = \frac{TP}{TP + Fp}$$

Where:

- TP(**True Positive**) refer to the number of correctly predicted positive instances (i.e.., Fradulent Transactions that were correctly identified as fraud)
- FP**(False Positive)** refers to the number of instances that were incoreectlypredicted as positive(i,e legitimate transaction that were wrongly flagged as fraud)

e. RECALL:

The formula for recall is:

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

Where:

- TP(**True Positive**) refer to the number of correctly predicted positive instances (i.e.., Fraudulent Transactions that were correctly identified as fraud)
- FN**(False Negative)** refers to the number of Actual positive instances that were incorrectly predicted as negative(i,e fraudulent transaction that the model missed)

3.2 Discussion

The proposed system enhances UPI fraud detection by integrating an ensemble model that combines Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU). ANN is instrumental in identifying intricate patterns within transactional data, enabling the system to recognize anomalies that could indicate fraudulent activity. LSTM, with its strength in analyzing sequential data, helps in detecting fraudulent behaviors that evolve over time, making it highly effective in financial fraud detection. GRU, a more computationally efficient variant of LSTM, reduces the number of parameters while maintaining high accuracy, ensuring that the model can process large-scale financial data without excessive resource consumption. This combination enhances fraud detection by leveraging the strengths of each architecture, making the system more effective in distinguishing genuine transactions from fraudulent ones.Compared to traditional fraud detection models like CNN, which struggle with large transactional datasets, the proposed ensemble model efficiently handles vast amounts of data, making it ideal for real-time fraud detection. Unlike static models that rely solely on historical data, this approach continuously adapts to emerging fraud patterns, thereby improving detection accuracy over time. By integrating deep learning techniques, the system minimizes false positives and enhances risk assessment, reducing financial losses for users and businesses. This robust, scalable approach not only strengthens security in digital payment platforms but also fosters trust in online transactions, ensuring a safer and more reliable UPI ecosystem.

a. **Data Collection:**

Data collection from Kaggle open-source datasets is a crucial step in building a machine learning model, especially for tasks like UPI fraud detection.

Pre-processing:

Pre-processing a dataset from a CSV file is an essential step in preparing the data for analysis or machine learning. The process begins with handling missing values, where any missing or null entries are identified and addressed, either by imputing values (such as replacing with the mean, median, or mode) or removing the rows or columns with significant gaps. Next, duplicate rows are removed to avoid redundancy, ensuring that each data point is unique. Categorical variables need to

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

be converted into numerical form through techniques like one-hot encoding or label encoding, enabling algorithms to process them effectively. For numerical features, feature scaling is applied, such as normalization or standardization, to ensure that variables are on a comparable scale, preventing any single feature from dominating the model.

Feature Extraction:

Feature extraction is the process of transforming raw data into a set of meaningful, informative features that can improve the performance of machine learning models. In the context of a dataset, especially for tasks like fraud detection or predictive modeling, the goal is to identify and select relevant characteristics that represent patterns and trends within the data.For numerical data, feature extraction might involve computing statistical measures like mean, median, standard deviation, or aggregating values over specific intervals. For example, in a financial transaction dataset, features like transaction frequency, average transaction amount, and time of day can be extracted to better understand user behavior.In time-series data, such as UPI transactions, features like transaction velocity (how fast transactions are made), seasonality (transaction patterns at specific times), and trends (increase or decrease in transaction volume over time) are critical.For categorical data, feature extraction might include encoding information such as transaction type or user demographics into numerical values through techniques like one-hot encoding or label encoding.In some cases, domain-specific features, such as geolocation information (distance from typical transaction locations) or behavioral patterns (sudden increases in transaction size), may be extracted to help the model recognize fraudulent behavior.Effective feature extraction ensures that the model focuses on the most important aspects of the data, leading to better predictions and decision-making.

b. **MODEL CREATION USING ENSEMBLE ALGORITHM:**

Model creation using an ensemble algorithm involves combining multiple machine learning or deep learning models to improve predictive accuracy, reduce overfitting, and enhance model robustness. In UPI fraud detection, an ensemble approach that integrates models like Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU) leverages the strengths of each algorithm. ANN captures complex, non-linear patterns in transaction data, making it adept at identifying intricate fraud signals. LSTM, designed to process sequential data, excels at recognizing fraudulent patterns over time, such as unusual transaction trends. GRU, a simplified variant of LSTM, is computationally efficient and better suited for handling large datasets in real-time, ensuring scalability without compromising accuracy.In an ensemble, these models are trained independently, and their predictions are combined using methods like majority voting, weighted averaging, or stacking. This strategy ensures that the final prediction benefits from the diverse strengths of each model, improving overall accuracy and robustness. Fine-tuning hyperparameters for each model helps optimize performance.

c. **Test Data:**

Test data is a crucial part of the machine learning process, serving as a benchmark to evaluate the performance of a trained model. After a model has been trained on the training dataset, the test data is used to assess how well the model generalizes to new, unseen examples. Unlike training data, which the model has already learned from, test data is kept aside during the training phase to ensure that the evaluation is unbiased and reflects real-world performance. The primary purpose of test data is to determine how effectively the model can make predictions on data it has not encountered before, simulating how it would perform on future, unseen instances. This helps in identifying overfitting, where a model may perform exceptionally well on training data but poorly on new data. By evaluating the model on test data, key performance metrics such as accuracy, precision, recall, F1-score, and others can be calculated, providing insights into its strengths and weaknesses. It also allows for comparing different models or configurations to select the best-performing one. In summary, test data ensures that the model is robust, reliable, and capable of making accurate predictions in real-world scenarios.

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

d. **PREDICTION:**

Prediction is the final stage in the machine learning pipeline, where the trained model is used to make inferences about new, unseen data. In the context of UPI fraud detection, the prediction phase involves using the ensemble model to analyze incoming transaction data and classify it as either fraudulent or legitimate.

e. **Formula used in ANN algorithm:**

Mathematically, this is expressed as:

$$y = \int \left(\sum_{i=1}^{n} w_i x_i + b \right)$$

f. **Forget Gate (*ft*)**

The forget gate in an LSTM determines which information should be discarded from the cell state. It looks at the previous hidden state h_{t-1} and the current input x_t, then outputs a value between 0 and 1. A value of 0 means "completely forget," and a value of 1 means "completely remember." Mathematically, it is expressed as:

$$\int_t = \sigma\left(W_f\left[h_{t-1,x_t}\right] + b_f\right)$$

Where:

- σ is the sigmoid activation function .
- W_f is the weight matrix for the forget gate.
- $[h_{t-1}, x_t]$ is the concatenation of the previous hide.
- b_f is the bias term for the forget gate.

g. **Input Gate (i_t)**

The input gate controls what new information gets stored in the cell state. It first uses the sigmoid function to decide which values to update, and then uses the ***tanh***function to generate candidate values for the new cell state. The formula is:

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

$$\widetilde{C}_t = \tan h\,(W_c \cdot [h_{t-1}, x_t] + b_c)$$

Where:

- i_t is the input gate ,determining which parts of the candidate cell state$\widetilde{C}_t$should be added to current cell state .
- $\widetilde{C}_t$ is the candidate cell state that represents new information to be added to the cell state.
- σ is sigmoid function and $\tan h$ is the hyperbolic tangent function

The output gate determines the next hidden state, which is used for the output at the current time step. It uses the previous hidden state and the current input to calculate the output. The formula is:

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

Where:

- o_t is the output gate that decides which part of the cell state will be exposed as hidden state.
- σ is the sigmoid function.
- W_o is the weight matrix for the output gate.
- b_o is the bias term for the output gate.

DOI:10.46647/ijetms.2025.v09i02.113 ISSN: 2581-4621

i. **Gated Recurrent Unit (GRU):**

The Gated Recurrent Unit (GRU) is a simplified version of the Long Short-Term Memory (LSTM) network, designed to be more computationally efficient. While it shares similarities with LSTM, it has fewer gates and parameters, making it faster and less resource-intensive. The GRU uses two main gates: the **Update Gate (z_t)** and the **Reset Gate (r_t)**, and it combines these gates with a candidate hidden state to update its hidden state. Here's an explanation of each component with its formula:

Update Gate (z_t):

The formula is:

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t] + b_z)$$

Where:

- z_t is the **update gate** at time step t.
- σ is the **sigmoid activation function**, which outputs values between 0 and 1.
- W_z is the **weight matrix** for the update gate
- $[h_{t-1}, x_t]$ is the **concatenation** of the previous hidden state h_{t-1} and the current input
- b_z is the **bias term** for the update gate

Where:

- h_t is the update hidden state at time step t.
- z_t is the update gate which controls the mixture of the candidate hidden state $\bar{h}_t$ and previous hidden state h_{t-1}.
- $\bar{h}_t$ is the candidate hidden state
- h_{t-1} is the previous hidden state.

CONCLUSION :

In conclusion, The proposed ensemble model combining Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), Gated Recurrent Units (GRU), and XGBoost offers a robust and efficient solution for detecting UPI fraud. By integrating these diverse techniques, the system benefits from ANN's ability to capture complex patterns, LSTM's proficiency in handling sequential data, GRU's computational efficiency, and XGBoost's strength in boosting decision trees for enhanced predictive accuracy. This hybrid approach significantly improves the ability to detect fraudulent transactions while handling large-scale, real-time transactional data, a challenge faced by traditional fraud detection systems. The implementation of this ensemble system not only enhances the security of UPI-based payment platforms but also provides a proactive approach to fraud prevention, ultimately minimizing financial losses for both individuals and organizations. This approach has the potential to set new standards in fraud detection, offering a scalable and highly accurate solution to combat the growing threat of digital payment fraud.Future work could focus on incorporating reinforcement learning for dynamic adaptation to emerging fraud patterns, and using transfer learning to improve training efficiency with limited data. Additionally, deploying the model in real-time environments with continuous monitoring and feedback loops would enhance its effectiveness.

ACKNOWLEDGEMENTS:

I would like to thanks my guide, Mrs.M.Manjula, Asst Professor, for the support and guidance throughout my project "Enhancing UPI Transaction Security". I also thank my institution and Department for providing the resources need to complete this work. Finally, I'm grateful to thank my Team mates for financial support and my family for encouragement.

REFERENCES:

[1] Gupta, R., & Sharma, A. (2021). UPI Fraud Detection: Challenges and Solutions. Journal of Cybersecurity and Digital Forensics, 4(2), https://doi.org/10.1234/jcdf.2021.0042. 45-60.

[2] Kumar, P., &Verma, S. (2022). Analyzing the Impact of Machine Learning in Detecting UPI Fraud. International Journal of Computer Applications, 182(12), 22-28. https://doi.org/10.5120/ijca.2022.18212.

[3] Singh, T., & Rao, M. (2020). User Behavior Analysis for UPI Fraud Detection: A Machine Learning Approach. Proceedings of the International Conference on Artificial Intelligence and Machine Learning, 18-25.

[4] Sharma, N., &Iyer, A. (2023). Real-Time Fraud Detection in Digital Payment Systems. Journal of Information Security and Applications, 68, 103100. https://doi.org/10.1016/j.jisa.2023.103100.

[5] Zaveri, M., & Dutta, S. (2022). Enhancing UPI Security through Advanced Fraud Detection Techniques. Transactions on Cybernetics, 52(1), https://doi.org/10.1109/TCYB.2022.3148390. 98-112.

[6] Ministry of Electronics and Information Technology, Government of India. (2023). Unified Payments Interface (UPI) Security Guidelines. Retrieved https://www.meity.gov.in/content/upiguidelines. From.

[7] Chaudhary, R., & Kumar, N. (2020). A Review on Digital Payment Security and Fraud Detection Techniques. International Journal of Advanced Research in Computer Science, 11(6), https://doi.org/10.26483/ijarcs.v11i6.8793. 25-30.

[8] Agarwal, P., &Jha, R. (2021). Machine Learning Techniques for Detecting Online Payment Frauds: A Comprehensive Review. International Journal of Computer Applications, 174(15), https://doi.org/10.5120/ijca.2021.17415. 1-10.

[9] hattacharya, S., & Patra, S. (2023). Security Challenges in UPI Transactions and Machine Learning Solutions. International Journal of Innovative Technology and Exploring Engineering,12(2),32-38. https://doi.org/10.35940/ijitee.B1824.1212323.

[10] Sharma, A., & Gupta, R. (2021). Comparative Analysis of Machine Learning Algorithms for Fraud Detection in UPI Transactions. Journal Technology, of Computer Science and 36(4), https://doi.org/10.1007/s11390-021-0158-9. 823-835.

[11] Reserve Bank of India. (2022). Report on Trends and Progress of Banking in India. Retrieved from https://www.rbi.org.in/Scripts/PublicationReportDetails.a spx?UrlPage=&ID=1136.

[12] Sahu, A., & Choudhury, D. (2023). Implementing AI Based Fraud Detection Systems in UPI Transactions: An Overview. Journal of Financial Technology, 7(1), 19-30. https://doi.org/10.1016/j.jft.2023.100132.

[13]Patel, K., & Vyas, A. (2021). Blockchain Technology for Secure Transactions in UPI: A Future Perspective. International Engineering, Journal of Recent Technology and 9(2), https://doi.org/10.35940/ijrte.B2905.129221. 467-472.

[14] Mishra, R., &Sahu, S. (2022). The Role of User Awareness in UPI Fraud Prevention. International Journal of Information Technology and Management, 21(3), 122 131. https://doi.org/10.1504/IJITM.2022.120814.