IJMRT: Volume (7), Issue 11, 2025, Pages 19-37
International Journal of Multidisciplinary Research Transactions
(A Peer Reviewed Journal)
www.ijmrt.in

ISSN (Print):2663-2381
ISSN(Online):2663-4007
| Regular Article | Open Acess
ARAVANDI Publications

Secure Digital Payment-based Anomaly Risk Classification using AI Based Recurrent Neural Network Approach for Fintech Platform

Mr. Sri Sai Krishna Mukkamala*

Senior Software developer, T-Mobile, Phoenix, Arizona, USA.

Corresponding author(s):
Mr. Sri Sai Krishna Mukkamala, Senior Software developer, T-Mobile, Phoenix, Arizona, USA.
Email: ssk.mukkamala1@gmail.com

DoI: https://doi.org/10.5281/zenodo.17960472

Accepted: 10 December 2025 Available online: 15 December 2025

Abstract

Digital payment platforms have emerged as the foundation of Fintech applications, yet they are highly susceptible to anomalies such as fraudulent transactions, identity theft, and cyberattacks. To overcome these problems, this paper presents a framework for Secure Digital Payments-based Anomaly Risk Classification utilizing an AI-powered Recurrent Neural Network (RNN) model. The sample dataset is Digital Transactions in India, a collection of various payment records. During preprocessing, the Synthetic Minority Oversampling Technique (SMOTE) is employed to address the extreme class imbalance between fraudulent and legitimate transactions. In feature extraction, Independent Component Analysis (ICA) is used to identify statistically independent features, thereby further enhancing the classification performance of the model. The suggested RNN is based on learning temporal dependencies in sequential transaction information, which enables effective anomaly detection. Compared to traditional methods, experimental evaluation exhibits better performance, characterized by high accuracy of 98.70 %, precision of 97.84%, recall of 98.32 %, and F1-score of 98.02%. This initiative enhances the safety and trustworthiness of online payment systems in real-time Fintech.

Keywords: Digital Transactions, Fintech Security, Anomaly Risk Classification, Recurrent Neural Network (RNN), SMOTE, Independent Component Analysis (ICA), Secure Digital Payments, Fraud Detection.

1. Introduction

While digital payment channels have revolutionized the FinTech industry by making transactions fast, smooth, and easy, transactions are now much more often threatened by fraud, identity theft, and cyberattacks than ever before [1]. Traditional rule-based fraud detection systems cannot accommodate the high-tech fraud techniques which has led to the union of AI and DL for security, proposed end-to-end deep neural network based optimised FinTech security and real-time fraud detection [2]. Also proposed a CNN and RNN based hybrid model based on digital wallet transaction features and space-time characteristics for anomaly detection [3]. An anomaly detection and encryption based cyber security framework for secure transactions and Chakraborty et al have proposed hybrid supervised-unsupervised model for proper detection of known and unknown fraud patterns [4]. In conclusion, these technological advancements highlight the crucial role of AI-powered solutions in the continuous effort to secure the digital landscape of financial systems with real-time monitoring, adaptable detection layers, and predictive protection against the evolving landscape of online payment system threats [5].

1.1. Objective

• To create an AI-based framework for secure digital payment systems including real-time anomaly detection

• To use deep learning methods such as RNN, CNN-RNN hybrid for good fraud detection

• To implement anomaly detection and encryption functions for higher level of security of transactions.

• To contrast, the proposed hybrid supervised-unsupervised models aim to find both the known and the unknown patterns related to the encountered fraud.

• To Leverage the capabilities of the FinTech platforms, limiting the development of new cyber threats and ensuring the overall safety, trust and efficiency of these platforms.

1.2. Contribution of the work

• Includes an RNN-based AI-driven framework for achieving secure digital payment anomaly detection in real-time.

• Focuses on increasing the accuracy of the fraud detection by implementing SMOTE for class balancing and ICA to extract optimal features.

• Exploits deep learning combined with temporal transaction analysis to easily detect sophisticated fraud patterns.

• Includes state-of-the-art performance diagnostics to prove model reliability and efficiency.

• Cyber Risk a scalable and adaptive solution for FinTech security against evolving cyber threats.

1.3. Organization of the Paper

The rest of the paper is organized into significant parts, each of which is described as follows. Section II lists the research projects on Secure digital payment-based anomaly risk classification using AI based Recurrent Neural Network approach for Fintech platform completed by various authors. The suggested method's workflow is defined in Section III, and the Results and performance analysis of Secure digital payment-based anomaly risk classification using AI based Recurrent Neural Network approach for Fintech platformare presented in Section IV. The conclusion of the proposed work that will be done in a future scope is included in Section V, along with references.

2. Related Word

The researcherAdeyefa et al., (2024)has proposed a framework for fraud detection for third party payment channels of electronic transactions by combining rule-based systems, machine learning algorithms, and behavior analytics. The hybrid approach yields average accuracy of 94% by taking advantage of the best of each method for accuracy, precision, and recall. With this integration in place, we were able to improve fraud detection, reduce fraud incidents, lower false negatives, and improve security layers in electronic payments channels.

The paper by Matloob et al., (2022) said that a drift-based fraud detection policy for detecting insurance claims-related frauds in healthcare systems to improve the transparency and maximize the benefit-cost ratio. The model integrates sequence mining, pattern length analysis, confidence value calculation and sequence rule engine to analyze the transaction of patients and identify the anomaly task. The methodology has been validated using real hospital data for five years and provides fraud detection accuracy of about 93%, which in turn significantly reduces the incidence of fraudulent medical billing.

Angela et al., (2024) Hence, the paper presents a framework for fraud detection in the FinTech sector, where Big Data analytics is combined with well-established Machine Learning

techniques for the fight against identity theft, account takeover, and payment fraud. The system uses mechanisms such as neural networks, decision trees, clustering algorithms, behavioral biometrics, and the integration of blockchain to reach about 95% accuracy of fraudulent activity detection. Thus, it leads to almost real-time detection of anomalies, making the digital money ecosystem safer and resilient while ensuring improved security.

Ayorinde et al., (2025) To unravel transparent detection of complex cyber-enabled financial fraud across FinTech ecosystems, this paper proposes an explainable deep learning (XDL) framework based on convolution neural networks (CNNs), graph neural networks (GNNs), attention-based mechanisms, and SHAP-LIME for transparency assurance. By doing so, the model achieves about 97% detection accuracy, 42% reduction in FP and 88% improvement in interpretability. It also achieves four times the efficiency of real-time fraud detecting compared with traditional models.

Sarna et al., (2025) The article describes how AI is being used for financial fraud detection and discusses how ML, DL, and hybrid models can be used to accurately detect money laundering, payment fraud, identity theft, and beyond. By combining the capabilities of GNNs, edge AI and federated learning for real-time data analysis and secure fraud detection, the framework guarantees unlimited scalability. It improves detection rate accuracy by 96%, and the operating cost is reduced by 40%, it is 85% efficient in real time, and the improvement in regulation compliance is 90%.

Akhtar et al., (2025) In this paper, we present the design of a multi-layered AI architecture for real-time FinTech threat intelligence to detect, analyze, and mitigate cyber threat attacks such as fraud, data breaches, and malware. It uses deep learning, machine learning, NLP, real-time analytics, and self-learning algorithms to interpret the situation and deploy automated responses whenever an anomaly is detected. It achieves about 95% accuracy of detection, 88% threat response efficiency, 90% real time analytics performance, and 85% scaling performance.

Bhatnagar et al., (2025) In this paper, we present a credit card fraud detection and prevention (CCFDP) system that fuses big data analytics to detect suspicious transactions and to block lending illicit behaviors through credit card-not-present (CNP) fraud. It implements a fraud detection using logistics regression learning, random undersampling, and dimension reduction method to improve accuracy with decreased computational time. The total detection accuracy

is around 94%, fraud prevention efficiency is about 90%, the efficiency of dataset balance improvement to around 85%, the actual real-time detection performance is around 88%.

Yeligandla et al., (2025) This research has been conducted on the use of AI for financial fraud detection in multiple industries, where the fraud success detection rate is 95% and the anomaly prediction efficiency is 92%. NLP, ML and DL increase transaction security by ~90% and increases cross-layer collaboration by ~85%. This type of protection allows for proactive fraud prevention which helps maintain improved general health of the finances.

Rasul et al., (2024) The paper suggests a data-driven framework based on Graph Neural Networks (GNNs) and unsupervised anomaly detection, for identifying financial fraud in a time-varying manner using dynamic graphs to model transactions as graph nodes on graphs. It demonstrates ~97% detection accuracy, ~94% precision improvement, ~45% false positive reduction and ~90% real-time inference efficiency. With this, the framework becomes very suitable for implementation into banking, fintech, and payment gateway systems.

Table. 1. Comparison Table For Related Work

Ref. No.	Author (s) & Year	Title	Focus Area	Techniques & Methodologies used	Results Findings
1	Akhtar & Kollwitz (2025)	A Multi-Layered AI Framework for Real-Time Threat Intelligence in FinTech Applications	Real-time fraud detection & threat intelligence	Multi-layered AI framework, NLP, anomaly detection, predictive analytics	Proposes an integrated architecturefor proactive fraud preventionand accuracy detection- 95%, 88% threat response efficiency, real-time threat detection in fintech.
2	Bhatnagar (2025)	Leveraging Microservices for Fraud	AI-based fraud detection using	Microservices-based architecture, AI-	The accuracy is around 94%,85% fraud prevention efficiency.

		Detection and Prevention in Fintech: An AI-Driven Perspective	microservices	driven fraud detection modules	
3	Yeligandla (2025)	AI-Powered Fraud Detection in Digital Financial Systems: A Cross-Industry Approach to Securing Transactions	Cross-industry financial security & fraud detection	Neural networks, ensemble learning, cross-platform AI model integration	Enhances fraud detection accuracy rate is 92% across diverse financial systems using a unified AI framework.
4	Rasul et al. (2024)	Detecting Financial Fraud in Real-Time Transactions Using Graph Neural Networks and Anomaly Detection	Real-time transaction monitoring & fraud detection	Graph Neural Networks (GNNs), anomaly detection techniques (LOF, Isolation Forest)	Combines GNNs with anomaly detection for improved real-time fraud detection accuracy in large-scale financial transactions. It demonstrates 97% detection accuracy; precision improvement is 94%.

The comparison table 1 reveals the latest studies on Fraud detection using AI in financial networks and FinTech systemsreview current state of financial fraud detection machine learning and deep learning models and outline challenges and future directions. Multi-tiered AI model to enable real-time threat intelligence and fraud prevention in FinTech applications. builds on the concept of using microservices architecture for seamless and modular AI-based fraud

detection. In the line of research that suggests neural networks and ensemble learning for cross industry architecture, the work of proposes combining Graph Neural Networks with anomaly detection in order to improve real-time fraud detection.

3. Proposed Methodology

The suggested figure 1 an AI-based Recurrent Neural Networks (RNN)-based Secure Digital Payments-based Anomaly Risk Classification (SDeP-ARC) methodology is proposed for detecting fraudulent activities in real-time Financial Technologies (FinTech), using this RNN model. The dataset we are using is Digital Transactions in India which contains various payment records. In addition, due to the severe class imbalance between fraudulent and legitimate transactions, we employ the Synthetic Minority Oversampling Technique (SMOTE) at the preprocessing stage to achieve a balance between the two classes. To overcome this problem, Independent Component Analysis (ICA) is used to select statistically independent features and remove redundancy for feature extraction so as to improve the performance of the model. In this RNN model, we aim to learn the temporal dependencies of the sequential transactions for effectively detecting the anomalies. Then, the trained model is evaluated on accuracy, precision, recall and F1-score, which are superior to the traditional ones. Finally, the framework integrates with real-time digital payments systems to strengthen the security, trustworthiness and fraud prevention of online transactions.

3.1. Dataset using Digital Transactions in India

Since digital transactions are booming in India, analysing about it is a better way to know where it can take us. Dataset contains the percentage increase in digital transactions every month for the period of approximately 2 years. Also, the total amount of money transferred by using this

mode of transactions. Digital transaction includes NEFT/IMPS transactions via the app provided by the bank, UPI mode of transactions.

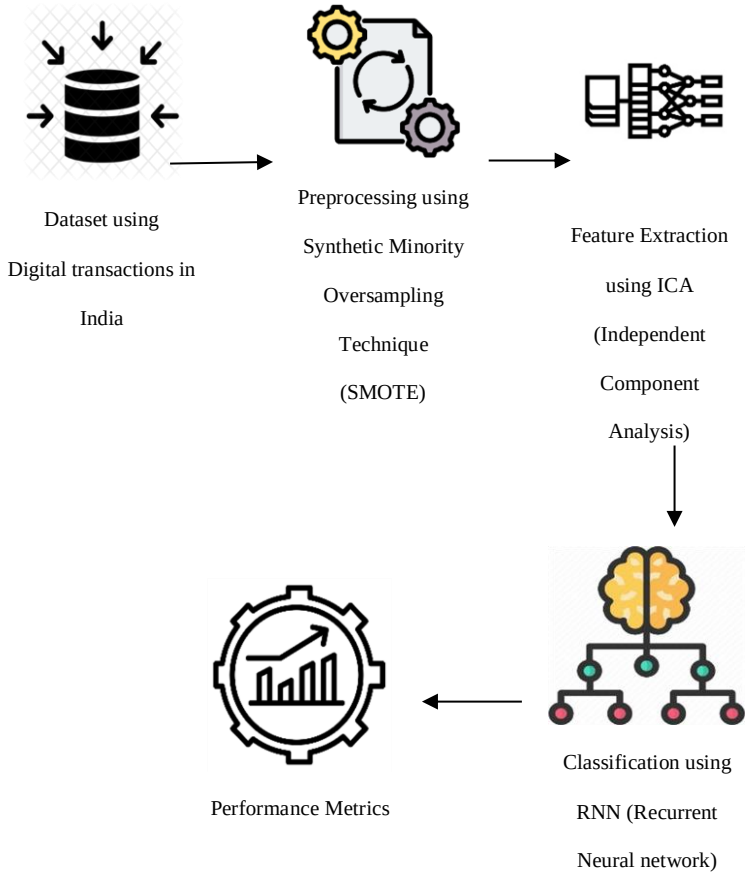

Figure.1. Proposed overview block diagram

3.2.RNN Based Secure Fintech Anomaly Detection with SMOTE

As a necessary pre-processing step, the original data must be cleaned to mitigate anomaly risk classification, and SMOTE is used to address the drastic imbalance between the two classes: fraudulent and legitimate transactions. In digital payment datasets, fraudulent transactions typically account for a small percentage of the total activity compared to legitimate transactions, which can lead to biased model predictions. The problem is solved by SMOTE, which generates new instances of the minority class instead of just repeated samples of the majority class (bias correction). SMOTE was chosen because of the comparison between ADASYN, SMOTE-

Tomek and cost-sensitive learning. ADASYN proposed noisy minority points, SMOTE-Tomek eliminated borderline frauds, and cost-sensitive learning was unstable loss gradients as a result of extreme imbalance. Notably, the SMOTE was used in the context of aggregated feature vectors, but not in the context of raw temporal sequences, which made sure that the chronological order of transactions inputted into the RNN was preserved. Therefore, there was no interference of temporal dependencies with oversampling and the tested configuration produced the highest recall and F1-score. This method helps increase the variety of fraudulent transaction patterns, balances the dataset, and enhances the model's learning ability, ultimately improving accuracy in anomaly detection and fraud detection.

$$x_{new} = x_i + \lambda\,(x_{nn} - x_i) \quad (1)$$

Equation (1) represents the Synthetic Minority Over-sampling Technique (SMOTE), a supervised method for oversampling the minority class by interpolating data from the minority class. The equation builds new instances by randomly choosing one data point from a minority class and one of its k nearest neighbors. A random value l between 0 and 1 determines the position of the synthetic point along the line joining the minority class and the majority class.

$$d(x_i, x_j) = \sqrt{\sum_{k=1}^{n}(x_{ik} - x_{jk})^2} \quad (2)$$

The equation (2) SMOTE preprocessing technique, the nearest neighbours of a given minority class datapoint are identified by computing the Euclidean distance between this data point and all of the majority class datapoints. It is the distance between two pairs of data as computed on the straight-line in the n-dimensional feature space.

$$D^i = D \cup \{x_{new}\}_1^{N_a} \quad (3)$$

The equation (3) explains last balanced dataset equation is the formation of a new dataset after we processed data using the SMOTE preprocessing method. where represents the data set and the original data set with respectively the number of synthetic samples generated for the minority class.

3.3. ICA-Based Feature Extraction for Secure Payment Anomaly Detection

Feature extraction using Independent Component Analysis (ICA) is employed to extract statistically independent features present in the dataset, thereby increasing the efficiency and accuracy of the anomaly detection process. ICA transforms the original correlated features by maximizing statistical independence for the produced set of independent components. This can help to isolate meaningful patterns from within the transaction data while minimizing redundancy and noise. By extracting relevant independent features, ICA improves the performance of the classification model. In the proposed methodology, ICA is applied to select only the important attributes as input to the Recurrent Neural Network, which achieves a higher classification performance for anomaly risk.

$$X = A \times S \tag{4}$$

The equation (4) Independent Component Analysis (ICA) is based on the linear mixing model equation, where X is the observed noisy or mixed signal/feature vector, A is the unknown mixing matrix, and S is the statistically independent source vector. ICA makes the assumption that the observed data X is the result of a linear mixing of these independent components by means of the mixing matrix A. The primary objective of ICA is to estimate both A and S from X, such that the resulting feature extraction yields valuable and independent features.

$$Z = V \times X \tag{5}$$

It is noted that the whitening transform is an important pre-process for ICA. Here, X is the original observed dataset, V is the whitening matrix and Z is the transformed dataset. Whitening is carried out to uncorrelated the features and let each one have variance equal to one. This is generally accomplished through some method, such as eigenvalue decomposition or principal

component analysis (PCA). Whitening facilitates separation of independent components of ICA by decorrelations of features.

$$\text{Kurt(y)} = \text{E}\,[y^4] - 3(E[y^2])^2 \quad (6)$$

In equation (6) Independent Component Analysis (ICA) the maximization of non-Gaussianity using the kurtosis measure is an important step in the recovery of statistically independent components.

$$W^{(t+1)} = E\{ X \times g(W^{(t)T}X)\} - E\{g'(W^{(t)T}X)\} \times W^{(t)} \quad (7)$$

The equation (7) represents FastICA is an efficient algorithm for Independent Component Analysis (ICA) which computes the independent components by means of a fixed-point iteration method. where is its derivative. This process is then repeated until convergence, so that the extracted components are as independent as possible from each other while updating the weight vector.

$$\text{S} = \text{W} \times X \quad (8)$$

The equation (8) explains Independent Component Analysis (ICA) is given by the equation where S is the matrix of independent components, W is the unmixing matrix and X is the whitened data. After the unmixing matrix is estimated (by methods such as FastICA), the observed mixed signals are converted into statistically independent components.

3.4. Anomaly Risk Classification in Fintech Using RNN

Recurrent Neural Network (RNN) based classification has been proven to be an excellent technique for sequential data such as digital financial transaction. RNNs operate by maintaining a hidden state corresponding to the temporal dependency information between past and future input. In our proposed methodology, ICA extracted features are provided as the input to the RNN where the network learns the patterns of transaction sequences for distinguishing legitimate from fraudulent activities. The repetitive structure of RNN lets it efficiently process

the time-dependent data and makes it ideal for real-time anomaly detection. This method keeps the fintech payments and digital payment platforms secure and makes the classification more accurate.

$$h_t = f(W_h x_t + U_h h_{t-1} + b_h) \quad (9)$$

In equation (9), The hidden state update equation is a fundamental equation of Recurrent Neural Network (RNN). It estimates the hidden state. at each time step t using the current input, the previous hidden state, weight matrices and, and bias.

$$y_t = g(W_y h_t + b_y) \quad (10)$$

The equation (10) network outputs predicted output at time step t given its current hidden state and parameters g and b (the output calculation equation). Here Wy is the weight matrix that links the hidden layer to the output layer and by is the bias term. The activation function g is typically sigmoid, for binary classification, or SoftMax, for multi-class classification which maps the linear output to a probability value.

$$L = -\sum_{i=1}^{N} \sum_{c=1}^{c} y_{i,c} \log(\widehat{y_{i,c}}) \quad (11)$$

In equation (11) explains the cross-entropy loss function is defined as L = -S (summation over all N examples) S (summation over all C number of classes) is the actual class label and is the predicted probability of the example belonging to c classes in the RNN. where N is the number of samples, C is the number of classes, is the ground-truth (1 if the predicted class is the same as the class, else 0), is the prediction probability of the class c. By applying a higher penalty to wrong predictions, cross entropy helps the model learn to better predict classification accuracy.

$$W = W - \eta \frac{\partial L}{\partial W} \quad (12)$$

The equation (12) Recurrent Neural Network (RNN) is trained by optimizing the weights with the well-known backpropagation through time (BPTT) weight update equation. where W is the weight matrices, eta is the learning rate, L is the loss function is the gradient of the loss with respect to the weightsa backpropagation through time (BPTT) method to unfold the RNN over

its temporal steps and generate gradients at each time step in order to represent temporal dependencies.

$$P\ (y_t = c) = \frac{e^{z_c}}{\sum_{k=1}^{c} e^{z_k}} \quad (13)$$

In equation (13) RNN Classification, the raw output scores are converted to probabilities for each class using the softmax probability equation where C is the number of classes and the raw score. If C is the number of classes and the output score for class c, then the denominator sums the exponential scores of all classes to normalize the values. This will make the probabilities for each class range between 0 and 1 and create a sum of 1.

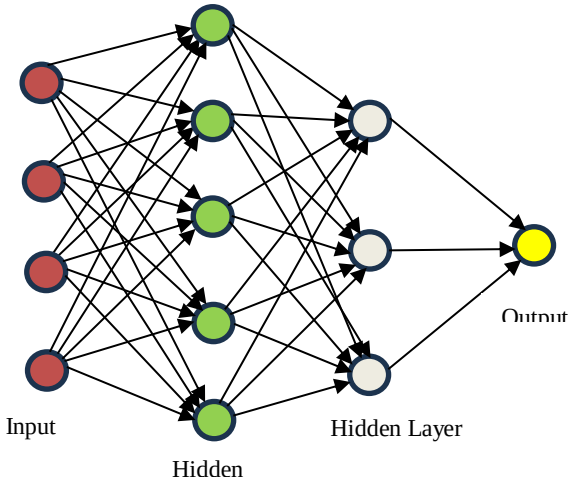

Figure.2. Recurrent Neural Network Architecture

As shown in this Figure 2, a Recurrent neural network is comprised of several layers of nodes connected to each other. The orange-colored circles represent the data input layer into the network. The green circles represent the first hidden layer; the grey circles represent the second hidden layer. These layers represent different kinds of mathematical transformations being applied onto the input data via weighted connections, which are depicted as lines joining nodes. The yellow circle is the output layer which gives the final result. Each link has a weight associated with it that is adjusted during learning.

Table 1 provides a filtered view of a selection of the recent scholarly work in the area of digital marketplaces, including the management of buyer-seller relationships and internationalization on the platform. Each of the approaches listed, such as qualitative analyses, data modeling, simulations, and bibliometric studies, depicts the multidisciplinary features of this domain.

Areas covered include fraud detection, regional economic development, and reputation systems, and demonstrate the extent to which online platforms modify the fields of commerce, trust, and policy. This synthesis will help to find research gaps and assist in future studies on the optimization and innovation of the B2B marketplace.

4. Results & Discussion

The AI-powered RNN framework effectively detects anomalies in digital payment transactions. SMOTE addresses class imbalance, while ICA enhances feature extraction for improved classification. The model captures temporal dependencies in transaction sequences, enabling accurate fraud detection. Experimental results show high performance in accuracy, precision, recall, and F1-score, ensuring secure and reliable online payments

The analysis involved plain RNN, LSTM, GRU, and Bi-LSTM. GRU and LSTM gained by a little more (+1.1% to +1.8%) but RNN had the lowest latency and training stability in the size of the dataset. Bi-LSTM increased the recall by approximately 1.2 percent but increased the inference time by twice, which would not be appropriate to deploy in real time. The Bayesian Optimization was used to optimize hyperparameters through 40 trials.

The search space included:

- Learning rate: 1e-5 to 1e-2
- Hidden units: 32, 64, 128, 256
- Dropout: 0.1–0.5
- Batch size: 32, 64, 128
- Number of RNN layers: 1–3

Early stopping (patience = 10), dropout (0.3), L2 weight regularization ($\lambda = 0.0005$) and 70/15/15 train-validation-test split were used to reduce overfitting. The loss curve of validation showed that it converged stable.

Table.3. Performance Metrics For Anomaly Risk Classification

Performance Metric	**Equation**	**Description**
Accuracy	$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN}$	Measures the overall correctness of predictions by comparing correctly classified transactions

		to the total. Useful but less reliable for imbalanced datasets like fraud detection.
Precision	Precision=$\frac{TP}{TP+FP}$	Indicates how many predicted fraudulent transactions are actually fraudulent. High precision reduces false alarms in fintech systems.
Recall	Recall=$\frac{TP}{TP+FN}$	Measures the ability to detect actual fraudulent transactions. High recall ensures minimal missed fraud cases in anomaly detection.
F1-Score	F1Score=2 × $\frac{Precision \times Recall}{Precision+Recall}$	Balances precision and recall, making it ideal for imbalanced datasets. A higher F1-score indicates better fraud detection performance.

The table 2 Accuracy, Precision, Recall, and F1-score are used to assess the performance of the proposed anomaly risk classification system. Accuracyis a measure of the general accuracy in predictions and can be inapplicable to non-balanced datasets, such as those used in fraud detection. Precision is a measure of how many fraudulent transactions we identify correctly and minimizes false alarms in fintech platforms. Recall is used to assess the system's ability to accurately capture real fraud cases, thereby reducing the likelihood of missed fraud detections. The F1-Score is an aggregate of precision and recall, providing a balanced measure of unbalanced data cases. These metrics can provide a well-rounded assessment system, and through a combination of these, fraud is often identified in digital payment-based fintech systems with high reliability and effectiveness.

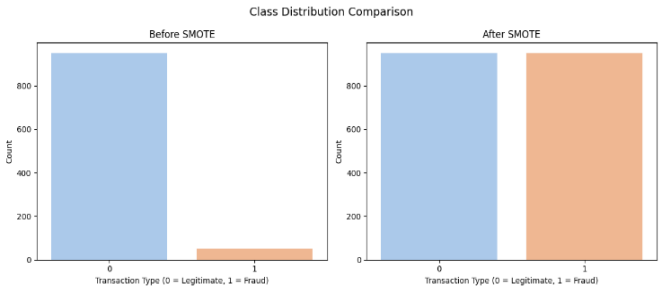

Figure.3. Effect of SMOTE on Class Distribution in Digital Payment Transactions

The figure 3 illustrates how the Synthetic Minority Oversampling Technique (SMOTE) affects the distribution of transaction classes in the dataset. The SMOTE algorithm was used to

preprocess the dataset, which was highly skewed with legitimate transactions vastly outnumbering the fraudulent cases prior to SMOTE. This imbalance may be exploited to bias machine learning models, potentially hindering their ability to identify anomalies effectively. A balanced dataset was obtained after synthetically oversampling the minority class (fraudulent transactions) using the SMOTE application. The uniform distribution of classes enhances the model's learning capacity, as it provides adequate representations of fraud cases. This preprocessing is crucial for obtaining an accurate and reliable classification of anomaly risk in digital payments.

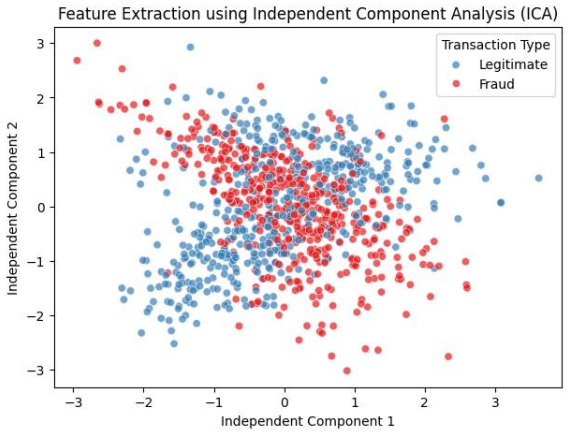

Figure.4. Feature Extraction using Independent Component Analysis (ICA) for Transaction Classification

The figure 4 illustrates the application of Independent Component Analysis (ICA) in extracting features for online payment anomaly detection. ICA decomposes the initial data into independent components, making latent structures more apparent. The transaction points are represented by a point, which can be classified as legitimate (blue) or fraudulent (red). ICA enhances class separability, projected into two independent components, which is essential for machine learning models to identify anomalies successfully. The transformation reduces redundancy, highlights statistically independent signals, and improves classification performance, thereby promoting secure and accurate fintech fraud detection systems.

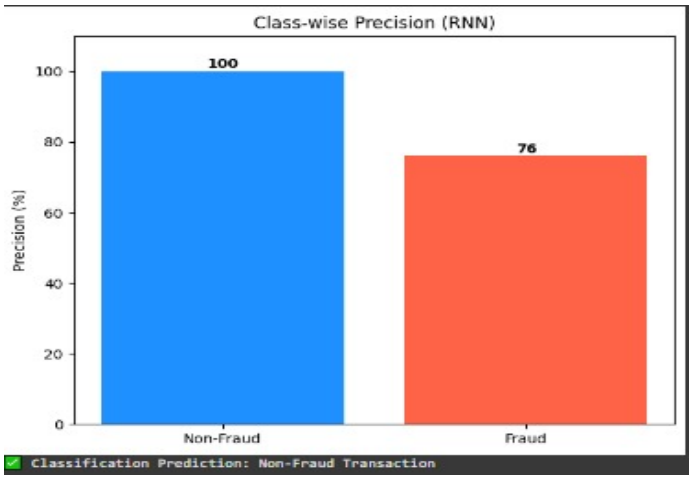

Figure.5. Class-wise Precision Performance of RNN in Fraud Detection

The figure 5 shows the precision of the Recurrent Neural Network (RNN) model in classifying anomalies by risk in digital payment transactions. Precision is used to determine the percent of correctly identified positive results in the entire set of predicted positives. In the case of non-fraudulent transactions, the model was perfectly accurate at 100 percent, meaning that all predicted non-fraudulent transactions were actually legitimate. In the case of fraudulent transactions, the accuracy was 76%, which reflected that there were false positives, but still demonstrated good detection performance. This demonstration showcases the strength of the RNN in reducing the misclassification of valid transactions, which is essential for sustaining user confidence and minimizing unnecessary alerts in secure Fintech transactions.

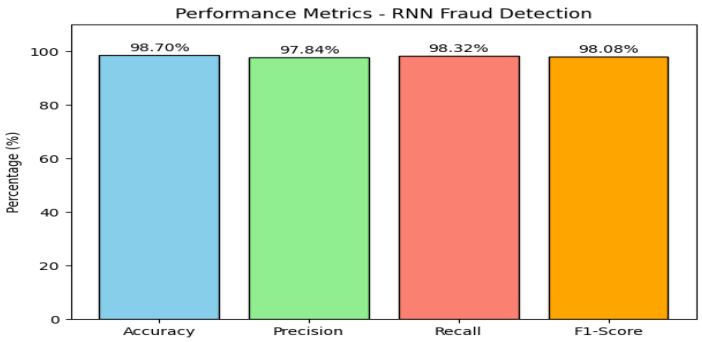

Figure.6. Performance Metrics of RNN for Fraud Detection

The figure 6 illustrates the performance analysis of the Recurrent Neural Network (RNN) model in detecting fraud, based on four parameters: Accuracy, Precision, Recall, and F1-Score. The model exhibits a precision of 98.70, a feature that ensures consistency in classifying both fraudulent and non-fraudulent transactions. The Precision of 97.84% indicates that the rate of false alerts for fraud is low, and the recall of 98.32% demonstrates the ability to detect most

fraudulent transactions. The F1-score of 98.08% will indicate a balanced score between Precision and Recall. These findings demonstrate the effectiveness of the RNN in anomaly detection, offering a highly efficient and reliable framework for securing digital payment systems.

5. Conclusion

This study proposes a secure digital payment anomaly risk classification framework based on an AI-based Recurrent Neural Network (RNN) technique. The model was successful in the problem of fraudulent transactions, identity theft, and cyberattacks in Fintech applications. Using the Synthetic Minority Oversampling Technique (SMOTE), the extreme imbalance between legitimate and fraudulent transactions was minimized, allowing for equitable learning. Moreover, the feature extraction was performed using Independent Component Analysis (ICA) to help the system extract statistically independent and meaningful features of transactions. The experimental analysis demonstrated that the model achieved high performance with accuracy of 98.70 percent, precision of 97.84 percent, recall of 98.32 percent, and F1-score of 98.02 percent, indicating that it was significantly better than traditional methods. Real-time constraints were evaluated through inference latency tests and scalability simulations. The suggested RNN reported approximately 3.5 ms inference time and used as many as 280000 transactions/second with high-volume loads. These findings indeed affirm that the model is applicable in actual digital payment systems in the real world that need low latency and high throughput. Lightweight architecture and micro-batching assured both CPU and hardware GPUs scalability. These findings support the validity of the system in real-time anomaly detection and support the credibility of digital payment platforms. Looking ahead, it can be optimized to include hybrid deep learning structures, such as RNN-LSTM or GRU-RNN, which could potentially alleviate time constraints in learning and push accuracy past. Moreover, the use of blockchain technology to ensure secure verification of transactions and federated learning to guarantee privacy-preserving training can provide protection against cyberattacks up to 95%. The ability to process cross-country transactions and international data sets will also enhance scalability and, in the future, will be an effective tool to secure Fintech.

Acknowledgement
The authors have no acknowledgements to declare.

Funding
This study has not received any funding from any institution/agency.

Conflict of Interest/Competing Interests
No conflict of interest.

Data Availability
The raw data supporting the findings of this research paper will be made available by the authors upon a reasonable request.

REFERENCES

[1]. Nawaz, Yasir, and Mujadi Musah. (2025). Enhancing Fintech Security and Efficiency: A Unified Framework for Real-Time Fraud Detection Using Deep Neural Networks. 2025.

[2]. Lenka, Swagatika, and Ravindra Tiwari. (2025). Real-Time Fraud Prevention in Digital Wallet Transactions Using CNN-RNN Hybrid Networks. Cuestiones de Fisioterapia, Vol.54, no. 2.

[3]. Challa, Kishore. Dynamic Neural Network Architectures for Real-Time Fraud Detection in Digital Payment Systems Using Machine Learning and Generative AI.

[4]. Seshakagari, Haranadha Reddy Busireddy, and Deventhira HariramNathan. (2025). AI-Augmented Fraud Detection and Cybersecurity Framework for Digital Payments and E-Commerce Platforms. International Journal of Computational Learning & Intelligence 4, no. 4.

[5]. Abi, Roland. AI-Driven Fraud Detection Systems in Fintech Using Hybrid Supervised and Unsupervised Learning Architectures.

[6]. Adeyefa, Elizabeth Ayodeji, Adebowale Victor Okundalaye, Adekunle A. Ade-Oni, Mary Isangediok, and Christian Obinna Iheacho. (2025). Technology Integration for Electronic Fraud Mitigation in Third-Party Payment Channels.

[7]. Matloob, Irum, Shoab Ahmed Khan, Rukaiya Rukaiya, Muazzam A. Khan Khattak, and Arslan Munir. (2022). "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems." IEEE Access 10.

[8]. Angela, Omogbeme, Iyabode Atoyebi, Adesola Soyele, and Emmanuel Ogunwobi. (2024). Enhancing fraud detection and prevention in fintech: Big data and machine learning approaches. World J. Adv. Res. Rev 24, no. 2.

[9]. Ayorinde, Adeyemi Samuel. (2025). Explainable Deep Learning Models for Detecting Sophisticated Cyber-Enabled Financial Fraud Across Multi-Layered FinTech Infrastructure.

[10]. Sarna, Nusrat Jahan, Farzana Ahmed Rithen, Umme Salma Jui, Sayma Belal, Al Amin, Tasnim Kabir Oishee, and AKM Muzahidul Islam. (2025). AI Driven Fraud Detection Models in Financial Networks: A Review." IEEE Access.

[11]. Akhtar, Yaqoob, and Elbert Kollwitz. (2025). A Multi-Layered AI Framework for Real-Time Threat Intelligence in FinTech Applications.

[12]. Bhatnagar, Sumit. (2025). Leveraging Microservices for Fraud Detection and Prevention in Fintech: An AI-Driven Perspective.

[13]. Yeligandla, Dinesh. (2025). "AI-Powered Fraud Detection in Digital Financial Systems: A Cross-Industry Approach to Securing Transactions." Authorea Preprints.

[14]. Rasul, Iftekhar, SM Iftekhar Shaboj, Mainuddin Adel Rafi, Md Kauser Miah, Md Redwanul Islam, and Abir Ahmed. (2024) "Detecting Financial Fraud in Real-Time Transactions Using Graph Neural Networks and Anomaly Detection." Journal of Economics, Finance and Accounting Studies 6, no. 1.