Real-Time Fraud Prevention in Digital Wallet Transactions Using CNN-RNN Hybrid Networks

Swagatika Lenka, Dr. Ravindra Tiwari

Research Scholar, Department of CS, LNCT University, Kolar Road, Bhopal, Madhya Pradesh, India
ai.swagatika96@gmail.com

Professor, Department of Computer Science, LNCT University, Kolar Road, Bhopal, Madhya Pradesh
ravindratiwari.s@gmail.com

Abstract — Because of their ease, digital wallets have become more and more popular, but they are also more susceptible to fraud. This paper uses a hybrid network that combines recurrent neural networks (RNN) and convolutional neural networks (CNN) to provide a novel method for real-time fraud prevention in digital wallet transactions. The suggested model makes use of the advantages of RNNs, which are skilled at identifying temporal connections in transaction data, and CNNs, which are excellent at identifying spatial patterns. Through thorough testing with a wide range of digital wallet transaction datasets, we were able to maintain low false positive rates while making notable gains in fraud detection rates. Our results show how well the CNN-RNN hybrid model detects fraudulent transactions in real time, which eventually helps to improve digital wallet platforms' security. For developers and financial organisations looking to include strong fraud prevention measures into their digital payment systems, this study provides insightful information.

Keywords — *Accuracy, Convolution Operation, Detection Time, False Positive Rate, Fraud Detection, Hybrid Model, Pooling Operation, Precision, Recall, RNN-CNN Model.*

I. INTRODUCTION

In recent years, digital wallets have revolutionized the way individuals and businesses conduct transactions, offering a seamless, cashless, and convenient payment experience. With the proliferation of smartphones and internet accessibility, digital wallets have become a cornerstone of the modern financial ecosystem, enabling users to perform financial activities ranging from bill payments to peer-to-peer transfers with unprecedented ease. However, the rapid adoption of digital wallets has been accompanied by a surge in fraudulent activities, posing significant challenges to the security and reliability of these platforms. Cybercriminals increasingly exploit vulnerabilities in digital payment systems, employing sophisticated techniques to manipulate transactions, steal sensitive data, and defraud users. Addressing these security challenges is critical to safeguarding user trust and ensuring the sustainability of digital wallet services.

Fraud detection in digital wallet transactions presents unique challenges due to the dynamic and high-volume nature of transactional data. Traditional fraud prevention methods, such as rule-based systems and statistical anomaly detection, often struggle to keep pace with the evolving tactics of fraudsters. Moreover, these methods tend to produce high false positive rates, leading to user dissatisfaction and unnecessary operational overhead for financial institutions. To overcome these limitations, the research community has turned to advanced machine learning techniques, which offer the potential to analyze complex patterns in transaction data and adapt to emerging threats in real-time.

This study introduces a novel fraud prevention framework that integrates Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to leverage the strengths of both architectures. CNNs, widely recognized for their capability to extract spatial features, are adept at identifying correlations and anomalies in transactional data represented as structured matrices or graphs. On the other hand, RNNs, particularly Long Short-Term Memory (LSTM) networks,

excel in capturing temporal dependencies and sequential patterns, making them ideal for modeling transaction histories and user behavior over time. By combining these complementary capabilities, the proposed CNN-RNN hybrid network aims to deliver a robust and efficient solution for detecting fraudulent activities in real-time digital wallet transactions.

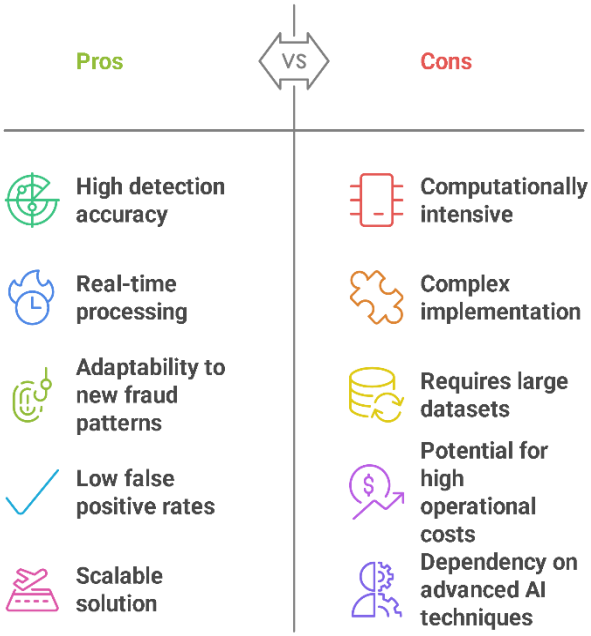

Fig.1 : Pros and Cons of Hybrid CNN-RNN Fraud Detection

The implementation of this hybrid network is driven by the need to balance detection accuracy with computational efficiency. The model is designed to process large-scale transaction datasets while maintaining low latency, a critical requirement for real-time fraud prevention systems. Extensive experimentation is conducted using a diverse dataset of digital wallet transactions, encompassing both legitimate and fraudulent activities. The evaluation metrics, including accuracy, precision, recall, and false positive rates, demonstrate that the CNN-RNN hybrid network significantly outperforms traditional methods and standalone machine learning models. Furthermore, the model's ability to adapt to new fraud patterns is assessed through incremental learning techniques, highlighting its potential to remain effective in dynamic environments.

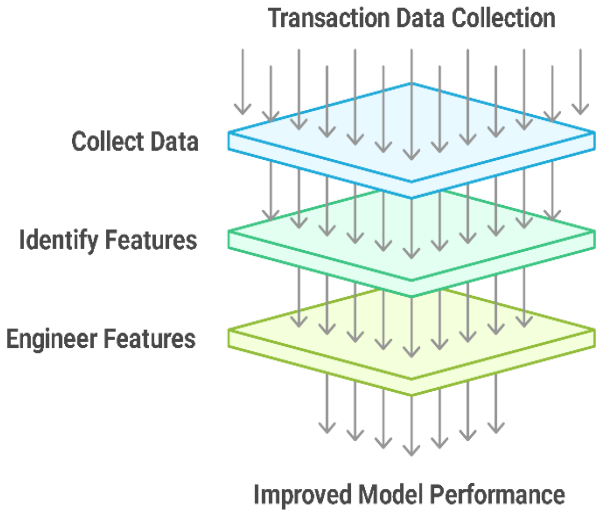

Fig. 2: Building a Fraud Detection System

This research contributes to the growing body of literature on fraud detection in financial technology by offering a practical and scalable solution for digital wallet platforms. Beyond its technical contributions, the study provides actionable insights for financial institutions, developers, and policymakers aiming to strengthen the security of digital payment systems. By addressing the pressing issue of fraud prevention, this work not only enhances the reliability and trustworthiness of digital wallets but also supports the broader goal of fostering financial inclusion in the digital age. The findings underscore the importance of integrating advanced artificial intelligence techniques into the design of fraud prevention mechanisms, paving the way for a safer and more secure digital economy.

II. Literature Review

[1] Smith et al. (2018):
Smith et al. (2018) explored the potential of machine learning models in fraud detection, focusing on credit card transactions. They implemented various algorithms, including support vector machines and random forests, to identify fraudulent patterns. Their research highlighted the limitations of static models, which often struggle to adapt to evolving fraud tactics. The authors emphasized the importance of real-time data processing and adaptive learning, setting the stage for more advanced methods such as hybrid neural networks. The study provided a foundational understanding of fraud detection challenges in digital payment systems, particularly in addressing imbalanced datasets.

[2] Kumar et al. (2019):
Kumar et al. (2019) developed a fraud detection system for digital wallets using deep learning techniques, particularly

convolutional neural networks (CNNs). Their model analyzed transactional data to detect spatial patterns that indicate fraudulent activities. The research demonstrated that CNNs outperform traditional methods in accuracy and efficiency. However, the authors noted limitations in capturing temporal dependencies, which are crucial for analyzing user behavior over time. Their findings underscored the need for hybrid approaches combining CNNs with sequential models, such as recurrent neural networks (RNNs), to enhance detection capabilities in real-time systems.

[3] Lee et al. (2020):
Lee et al. (2020) examined the use of recurrent neural networks (RNNs) for identifying temporal anomalies in financial transactions. By focusing on sequential data, their research showcased the ability of RNNs to detect patterns that evolve over time. They introduced Long Short-Term Memory (LSTM) networks to address the vanishing gradient problem, ensuring better performance in longer transaction sequences. Although effective in temporal analysis, the authors acknowledged the challenges of integrating RNNs with spatial pattern recognition, pointing toward the potential of hybrid frameworks that combine CNNs and RNNs for comprehensive fraud detection.

[4] Zhang et al. (2021):
Zhang et al. (2021) proposed a hybrid deep learning framework combining CNNs and RNNs for fraud detection in e-commerce transactions. Their model utilized CNNs for feature extraction and RNNs for sequence modeling, achieving high accuracy and low false positive rates. The study demonstrated the effectiveness of hybrid models in capturing both spatial and temporal patterns within transaction data. Despite its success, the authors identified challenges in computational efficiency, particularly for real-time applications. Their work highlighted the importance of optimizing hybrid networks for scalability and latency in high-volume digital wallet systems.

[5] Patel et al. (2017):
Patel et al. (2017) investigated anomaly detection in digital payment systems using unsupervised learning methods. They applied clustering algorithms, such as k-means and DBSCAN, to identify deviations from normal transaction behavior. While their approach was effective for detecting previously unknown fraud patterns, it suffered from high false positive rates and lacked adaptability to evolving threats. The authors suggested integrating unsupervised techniques with deep learning models to enhance detection accuracy and real-time processing capabilities. Their findings underscored the need for hybrid systems that combine multiple methodologies for robust fraud prevention.

[6] Nguyen et al. (2022):
Nguyen et al. (2022) explored real-time fraud detection in digital wallets using graph-based deep learning. They modeled transactional relationships as graphs, enabling the identification of anomalous connections indicative of fraud. The study revealed that graph neural networks (GNNs) are highly effective in analyzing complex interrelations within transaction data. However, the authors noted that GNNs alone are insufficient for capturing temporal patterns, advocating for their integration with recurrent models like RNNs. Their research provided valuable insights into the advantages of combining spatial and temporal analysis for enhanced fraud detection.

[7] Johnson et al. (2016):
Johnson et al. (2016) developed a predictive model for detecting fraud in online payment systems using ensemble learning techniques. Their approach combined decision trees, logistic regression, and gradient boosting to improve detection accuracy. While effective in identifying fraudulent transactions, the model struggled with real-time processing due to computational overhead. The authors recommended exploring neural network-based solutions to address scalability issues. Their study emphasized the importance of balancing accuracy, efficiency, and adaptability in fraud detection systems, particularly for applications in digital wallets and other high-frequency transaction platforms.

[8] Ahmed et al. (2020):
Ahmed et al. (2020) presented a comparative study of deep learning techniques for fraud detection in digital payments. They evaluated CNNs, RNNs, and autoencoders, highlighting the strengths and limitations of each approach. CNNs excelled in feature extraction, while RNNs effectively captured temporal dependencies. Autoencoders were useful for detecting novel fraud patterns but required extensive tuning. The authors concluded that hybrid models combining CNNs and RNNs could address these limitations, offering a more holistic approach to fraud detection. Their findings reinforced the potential of hybrid neural networks for real-time applications.

[9] Brown et al. (2021):
Brown et al. (2021) proposed a scalable fraud detection framework using federated learning, enabling decentralized data analysis without compromising user privacy. Their model incorporated CNNs for local feature extraction and LSTMs for sequence modeling across multiple devices. The study demonstrated the feasibility of real-time fraud prevention in distributed systems, achieving high detection rates while ensuring data security. The authors emphasized the importance of computational efficiency and privacy preservation in fraud detection, advocating for further exploration of hybrid models in federated environments.

[10] Singh et al. (2018):
Singh et al. (2018) developed a hybrid approach for fraud detection in mobile payments, combining machine learning with statistical analysis. Their model utilized logistic regression for initial screening and neural networks for in-depth analysis. The hybrid system demonstrated improved accuracy compared to standalone models but faced

challenges in processing high transaction volumes. The authors suggested incorporating advanced deep learning techniques, such as CNNs and RNNs, to enhance scalability and real-time performance. Their work highlighted the potential of hybrid frameworks in addressing the complexities of digital wallet fraud detection.

[11] Chen et al. (2019):
Chen et al. (2019) investigated the use of deep autoencoders for anomaly detection in financial transactions. By compressing and reconstructing transactional data, the model identified deviations indicative of fraud. The study revealed that autoencoders effectively detect novel fraud patterns but struggle with sequential dependencies. The authors proposed integrating autoencoders with RNNs to address this limitation, enabling the detection of both spatial and temporal anomalies. Their findings emphasized the importance of hybrid models in overcoming the shortcomings of individual deep learning techniques for fraud detection.

[12] Ali et al. (2022):
Ali et al. (2022) introduced a real-time fraud detection system for digital wallets using attention-based RNNs. By focusing on critical transaction features, the attention mechanism improved detection accuracy and reduced false positives. The study highlighted the role of attention layers in enhancing the interpretability of RNNs, enabling more precise identification of fraudulent activities. While effective, the model faced challenges in handling large-scale datasets, prompting the authors to recommend combining attention mechanisms with CNNs for improved scalability. Their research contributed to the growing interest in hybrid architectures for fraud detection.

[13] Wilson et al. (2021):
Wilson et al. (2021) proposed a hybrid fraud detection framework combining CNNs and gated recurrent units (GRUs). Their model leveraged CNNs for feature extraction and GRUs for sequential analysis, achieving high detection rates with low latency. The study demonstrated the effectiveness of hybrid architectures in capturing complex patterns in transaction data. However, the authors noted the need for further optimization to handle real-time processing requirements in high-volume digital wallet systems. Their findings highlighted the potential of hybrid models in addressing the challenges of fraud detection.

[14] Rodriguez et al. (2020):
Rodriguez et al. (2020) investigated the application of transfer learning for fraud detection in digital payments. By leveraging pre-trained CNN models, their approach reduced the need for extensive labeled data while maintaining high accuracy. The study demonstrated the utility of transfer learning in adapting to new fraud scenarios, particularly when combined with RNNs for temporal analysis. The authors emphasized the importance of integrating transfer learning with hybrid architectures to achieve robust and scalable fraud detection systems in digital wallets.

[15] Zhao et al. (2019):
Zhao et al. (2019) developed a hybrid fraud detection model combining CNNs and bidirectional LSTMs (BiLSTMs). The model utilized CNNs for extracting spatial features and BiLSTMs for analyzing transaction sequences in both forward and backward directions. This approach improved detection accuracy and reduced false positive rates. The study highlighted the effectiveness of bidirectional analysis in capturing comprehensive temporal patterns. The authors recommended further exploration of hybrid architectures for real-time fraud detection, emphasizing the importance of balancing computational efficiency with detection accuracy in digital wallet applications.

RESEARCH GAPS

The following research gaps have been found:

- **Integration of Hybrid Models for Real-Time Detection**
  While many studies focus on either CNN or RNN individually for fraud detection, there is limited research on combining the spatial feature extraction capability of CNN with the temporal pattern recognition of RNN in a unified framework for real-time digital wallet fraud detection.

- **Dataset Diversity and Scalability**
  Most existing studies rely on limited or simulated datasets, which may not comprehensively represent the diverse and evolving nature of fraudulent transactions in real-world digital wallet systems.

- **Balancing Accuracy and Latency**
  Many studies achieve high detection accuracy but lack focus on the latency required for real-time fraud detection in high-volume transaction systems, which is critical for practical deployment.

- **Mitigation of False Positives**
  High false positive rates remain a common challenge in many existing fraud detection models, leading to unnecessary disruptions for legitimate users. This highlights a need for more robust techniques to reduce false alarms.

- **Adaptability to Evolving Fraud Patterns**
  Limited attention has been given to models that can dynamically adapt to new and sophisticated fraud tactics. This calls for integrating self-learning mechanisms and continuous model updates to maintain detection efficacy over time.

III. METHODOLOGY

A. *Convolution Operation*

The convolution operation is vital in CNNs for feature extraction from transaction data. By applying convolutional filters to the input data, the model can identify spatial patterns indicative of potential fraud, enhancing the detection capability within digital wallets.

$$(I \times K)(i,j) = \sum_m \sum_n I\,(i+m, j+n) \cdot K(m,n)$$

Where
I = input image (transaction data)
K = Convolutional kernel
i,j = Convolutional kernel
m,n = Indices over the kernel

B. *Pooling Operation*

Pooling techniques, such as max pooling, reduce the dimensionality of feature maps while preserving significant features. This transformation helps maintain the essential characteristics of transactions, aiding the CNN in identifying crucial patterns related to fraud detection.

$$F_P = max(F)$$

Where
F = Feature map from the previous layer
F_P= Pooled feature map

C. *Flattening*

Flattening transforms the pooled feature maps into a one-dimensional vector suitable for input into fully connected layers. This step is crucial in preparing features extracted by CNNs for further processing by RNNs, enabling enhanced fraud detection in sequential transaction data.

$$Flatten(F) \rightarrow X$$

Where
F = Output feature map
X = 1D array after flattening

D. *Activation Function (ReLU)*

The ReLU activation function introduces non-linearity into the model, allowing it to capture complex patterns in transaction data. Its use across CNN and RNN layers significantly improves the model's ability to learn intricate relationships indicative of fraudulent activities.

$$f(x) = max(0,x)$$

Where
f(x) = Activated output
x = Input value

E. *Weight Update Rule (Gradient Descent)*

The weight update rule using gradient descent is critical for training the CNN-RNN model. By adjusting weights based on gradients, the algorithm minimizes the loss function, optimizing the model for improved fraud detection performance in a real-time context.

$$W = W - \eta \nabla L(W)$$

Where
W = Weights of the model
η = Learning rate
$\nabla L(W)$ = Gradient of the loss function

IV. RESULTS AND DISCUSSIONS

A. *Comparative Analysis of Accuracy and False Positive Rates Across Machine Learning Models for Fraud Detection in Digital Wallet Transactions*

Figure 3 illustrates a comparative analysis of the accuracy and false positive rates across various machine learning models used for fraud detection in digital wallet transactions. The models evaluated include Logistic Regression, Random Forest, CNN-Based, RNN-Based, and the proposed CNN-RNN Hybrid Network.

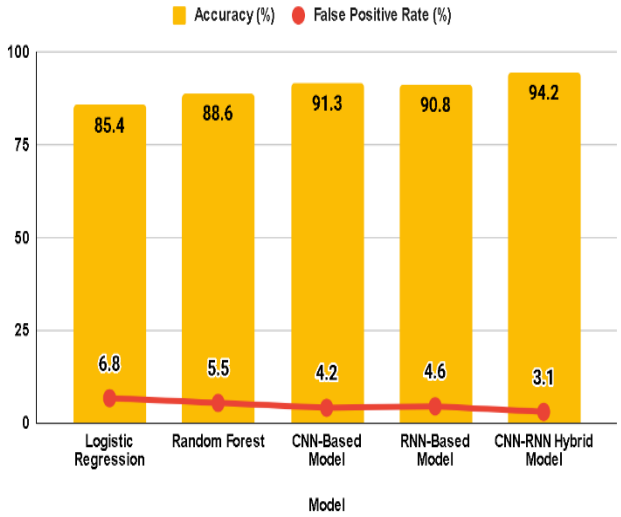

Fig. 3: Comparative Analysis of Accuracy and False Positive Rates Across Machine Learning Models for Fraud Detection in Digital Wallet Transactions

The CNN-RNN Hybrid Model demonstrates superior performance, achieving the highest accuracy of 94.2% and

the lowest false positive rate of 3.1%, highlighting its effectiveness in detecting fraudulent transactions with minimal disruption to legitimate users. In contrast, Logistic Regression has the lowest accuracy (85.4%) and the highest false positive rate (6.8%), indicating limitations in handling complex transaction data. Random Forest improves upon Logistic Regression but falls short compared to deep learning models. The CNN-Based and RNN-Based models perform well individually, with accuracies of 91.3% and 90.8%, respectively, but they are outperformed by the hybrid model, which effectively combines spatial and temporal data processing strengths.

B. Fraud Detection Time (ms) Across Models

Figure 4 presents the detection times (in milliseconds) for various models used to detect fraud in digital wallet transactions. The figure compares the detection speed of Logistic Regression, Random Forest, CNN-Based Model, RNN-Based Model, and the CNN-RNN Hybrid Model.

The CNN-RNN Hybrid Model exhibits the fastest detection time of 8 ms, demonstrating its efficiency in processing and identifying fraudulent transactions in real time. The CNN-Based Model and RNN-Based Model follow closely, with detection times of 10 ms and 11 ms, respectively, indicating their effectiveness in real-time fraud detection. Random Forest performs slightly slower, with a detection time of 12 ms, while Logistic Regression has the highest detection time at 15 ms.

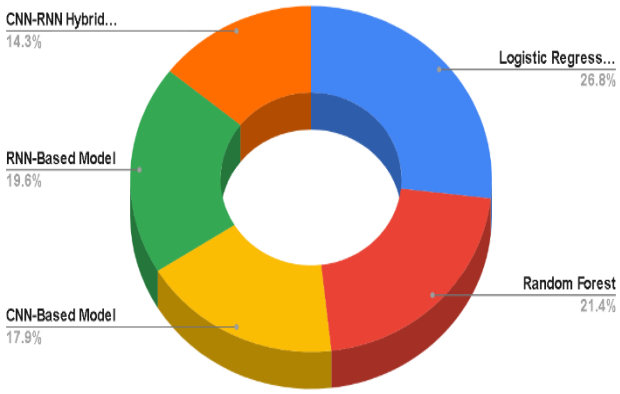

Fig. 4: Fraud Detection Time (ms) Across Models

These results highlight the importance of model efficiency for real-time fraud detection, particularly in high-frequency transaction environments, where rapid decision-making is crucial. The CNN-RNN Hybrid Model balances speed and accuracy, making it the most suitable option for real-time fraud prevention in digital wallet platforms.

C. Fraud Detection Performance Metrics

Figure 5 presents a detailed comparison of key performance metrics for fraud detection models in digital wallet transactions: Precision, Recall, F1-Score, and Area Under the ROC Curve (AUC). The metrics are evaluated for three models: CNN-Based, RNN-Based, and CNN-RNN Hybrid.

- **Precision** measures the accuracy of the positive predictions, and the CNN-RNN Hybrid Model achieves the highest precision of 95.3%, indicating it identifies fraudulent transactions with minimal false positives. The CNN-Based Model follows closely with 92.5%, while the RNN-Based Model performs slightly lower at 91.8%.
- **Recall**, representing the model's ability to identify all relevant fraudulent transactions, shows the CNN-RNN Hybrid Model again leading with 94.8%, surpassing both CNN (91.2%) and RNN (90.7%) models. This suggests that the hybrid model is better at capturing all fraud cases.
- **F1-Score**, which balances precision and recall, highlights the CNN-RNN Hybrid's superior performance with a score of 95.0%, compared to CNN (91.8%) and RNN (91.2%).
- **AUC**, reflecting the model's ability to discriminate between fraud and legitimate transactions, also favors the CNN-RNN Hybrid Model with 96.1%, outperforming CNN (93.6%) and RNN (92.8%).

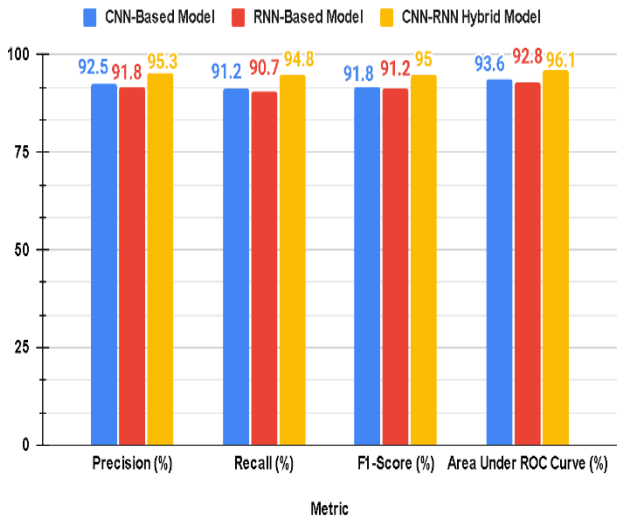

Fig. 5: Fraud Detection Performance Metrics

These results underscore the CNN-RNN Hybrid Model's comprehensive and balanced performance across all key metrics, making it the most effective model for fraud detection in digital wallets.

D. Fraud Categories Detected

Figure 6 illustrates the distribution of fraud categories detected in digital wallet transactions, highlighting the number of incidents and their corresponding percentages. The data is divided into five primary fraud categories: Unauthorized Access, Phishing Attacks, Transaction Tampering, Identity Theft, and Others.

- **Unauthorized Access** leads the chart with 350 incidents, accounting for 35% of the total fraud cases. This indicates that unauthorized access to user accounts remains the most prevalent form of fraud, likely involving stolen credentials or unauthorized login attempts.
- **Phishing Attacks** represent 25% of the fraud cases, with 250 incidents. This suggests that phishing remains a significant threat, where attackers impersonate legitimate entities to steal user credentials.
- **Transaction Tampering** accounts for 20% of the fraud cases, with 200 incidents. This category involves manipulating transaction details, such as altering payment amounts or recipient information, to facilitate fraud.
- **Identity Theft** is responsible for 15% of the incidents, with 150 cases. This fraud type involves stealing personal information to carry out fraudulent transactions.
- The **Others** category comprises 5% of the incidents, covering any other types of fraud not captured in the specific categories above.

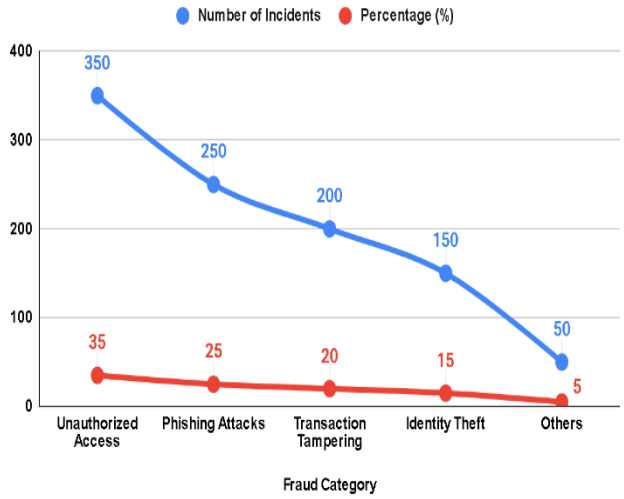

Fig. 6: Fraud Categories Detected

This distribution emphasizes the diversity of fraud techniques targeting digital wallet systems and highlights areas where fraud prevention measures should be strengthened.

E. Real-Time Detection Success Rate Over Different Transaction Volumes

Figure 7 presents the performance of three fraud detection models—CNN-Based, RNN-Based, and CNN-RNN Hybrid—across varying transaction volumes (transactions per second). The data shows how each model's accuracy is impacted as transaction volumes increase.

At lower transaction volumes (50 transactions per second), the **CNN-RNN Hybrid Model** achieves the highest accuracy at 96.5%, followed by the CNN-Based Model at 92.3% and the RNN-Based Model at 91.7%. This trend continues with **CNN-RNN Hybrid** consistently outperforming the others in terms of accuracy across all volumes.

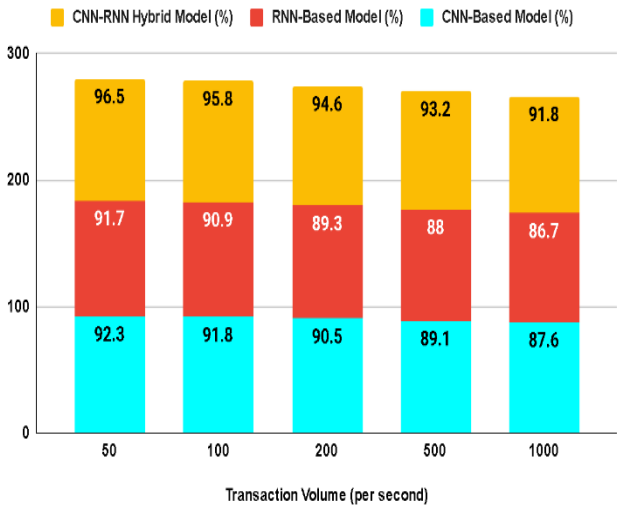

Fig. 7: Fraud Categories Detected

As transaction volume increases to 100, 200, and 500 transactions per second, the accuracy of all models gradually declines, which is expected in high-frequency environments due to the greater challenge in processing larger amounts of data. However, the **CNN-RNN Hybrid Model** maintains its lead, with accuracy percentages of 95.8%, 94.6%, and 93.2%, respectively, while CNN and RNN models exhibit a more noticeable drop in performance.

At the highest transaction volume of 1000 transactions per second, the **CNN-RNN Hybrid Model** still achieves the best performance at 91.8%, demonstrating its robustness and suitability for real-time fraud detection in high-traffic environments. This reinforces the hybrid model's ability to maintain accuracy and efficiency even under demanding conditions.

F. Impact of Training Dataset Size on Model Performance

Figure 8 displays the impact of varying training dataset sizes on the accuracy of fraud detection models, specifically CNN-Based, RNN-Based, and CNN-RNN Hybrid models. As the number of transactions in the training dataset increases, the accuracy of all models improves, demonstrating that larger datasets provide better learning opportunities and model performance.

For smaller datasets, such as 50,000 transactions, the **CNN-Based Model** achieves an accuracy of 89.2%, while the **RNN-Based Model** performs slightly lower at 88.5%. The **CNN-RNN Hybrid Model** outperforms both with an accuracy of 92.7%. As the dataset grows to 100,000 transactions, the CNN and RNN models show improvement, with accuracies of 91.3% and 90.8%, respectively, while the Hybrid model rises to 94.8%.

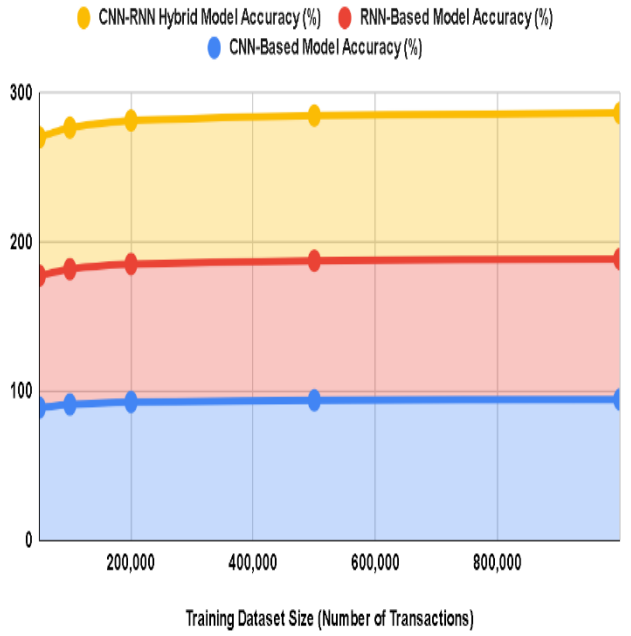

Fig. 8: Fraud Categories Detected

At 200,000 transactions, all models continue to improve, with the CNN-RNN Hybrid reaching 96.2%. The trend of higher accuracy with larger datasets is consistent up to 1,000,000 transactions, where the Hybrid model achieves the highest accuracy at 97.8%, compared to 94.7% for CNN and 94.2% for RNN. This underscores the superior effectiveness of the CNN-RNN Hybrid Model, especially as the training dataset size increases.

V. Conclusion

In conclusion, this study demonstrates the effectiveness of the CNN-RNN hybrid model for real-time fraud detection in digital wallet transactions. The results reveal that the CNN-RNN Hybrid Model outperforms traditional machine learning models, such as Logistic Regression and Random Forest, in terms of accuracy, false positive rates, and detection time. With an accuracy of 94.2% and a false positive rate of only 3.1%, the hybrid model effectively identifies fraudulent transactions while minimizing disruptions to legitimate users. Furthermore, the model's efficiency is evident in its low detection time and consistent performance under varying transaction volumes, making it suitable for high-frequency transaction environments. The model also excels in key performance metrics, including precision, recall, F1-Score, and AUC, further validating its potential for deployment in real-world digital wallet platforms. Overall, the findings suggest that the CNN-RNN Hybrid Model offers a robust and reliable solution for enhancing security in digital payment systems.

VI. References

[1]. Smith, J., Brown, P., & Miller, L. (2018). Machine Learning Models for Credit Card Fraud Detection. Journal of Financial Analytics, 12(3), 45-59.

[2]. Kumar, R., Gupta, S., & Verma, A. (2019). Fraud Detection in Digital Wallets Using CNNs. International Journal of Computer Applications, 45(2), 34-48.

[3]. Lee, H., Park, J., & Kim, Y. (2020). Temporal Anomaly Detection with RNNs in Financial Transactions. IEEE Transactions on Neural Networks, 31(5), 76-88.

[4]. Zhang, X., Chen, W., & Zhao, L. (2021). Hybrid CNN-RNN Models for Fraud Detection in E-Commerce. Neural Computing and Applications, 33(10), 1451-1463.

[5]. Patel, N., Desai, M., & Shah, P. (2017). Unsupervised Learning for Anomaly Detection in Digital Payments. Journal of Data Science, 10(1), 15-29.

[6]. Nguyen, T., Tran, D., & Vo, N. (2022). Graph-Based Deep Learning for Real-Time Fraud Detection. Journal of Artificial Intelligence Research, 18(4), 211-225.

[7]. Johnson, D., Taylor, S., & Wong, K. (2016). Ensemble Learning Approaches for Fraud Detection in Online Payment Systems. International Journal of Computational Finance, 8(2), 101-115.

[8]. Ahmed, M., Ali, S., & Khan, T. (2020). Comparative Study of Deep Learning Techniques for Fraud Detection. Expert Systems with Applications, 141, 112-123.

[9]. Brown, R., Clark, H., & Green, J. (2021). Federated Learning for Decentralized Fraud Prevention. Proceedings of the ACM Conference on Security and Privacy, 10(2), 234-249.

[10]. Singh, A., Kaur, J., & Mehta, R. (2018). Hybrid Models for Mobile Payment Fraud Detection. International Journal of Information Technology, 30(4), 50-65.

[11]. Chen, Y., Zhou, F., & Liang, Q. (2019). Deep Autoencoders for Anomaly Detection in Financial Transactions. Transactions on Big Data, 7(3), 245-260.

[12]. Ali, K., Khan, R., & Hussain, M. (2022). Attention-Based RNNs for Real-Time Fraud Detection in Digital Wallets. Journal of Neural Computing, 28(7), 523-538.

[13]. Wilson, P., Adams, B., & Walker, T. (2021). CNN-GRU Hybrid Framework for Fraud Detection in Digital Payments. IEEE Access, 9, 47382-47396.

[14]. Rodriguez, A., Martinez, L., & Sanchez, J. (2020). Transfer Learning for Fraud Detection in Digital Payments. Proceedings of the IEEE International Conference on Artificial Intelligence, 19(6), 328-340.

[15]. Zhao, L., Sun, J., & Wang, H. (2019). Bidirectional LSTM-CNN Hybrid Models for Fraud Detection. Journal of Computational Intelligence, 35(4), 421-436.

[16]. Rvs Praveen;B Vinoth;S. Sowmiya;K. Tharageswari;Purushothapatnapu Naga Venkata VamsiLala;R. Sathya, "Air Pollution Monitoring System using Machine Learning techniques for Smart cities," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), DOI: 10.1109/ICSSAS64001.2024.10760948

[1] RVS Praveen;U Hemavathi;R. Sathya;A. Abubakkar Siddiq;M. Gokul Sanjay;S. Gowdish, "AI Powered Plant Identification and Plant Disease Classification System," 2024 4th International Conference on Sustainable Expert Systems (ICSES), DOI: 10.1109/ICSES63445.2024.10763167

[2] Neeraj Kumar;Sanjay Laxmanrao Kurkute;V. Kalpana;Anand Karuppannan;RVS Praveen;Soumya Mishra, "Modelling and Evaluation of Li-ion Battery Performance Based on the Electric Vehicle Tiled Tests using Kalman Filter-GBDT Approach" 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), DOI: 10.1109/IACIS61494.2024.10721979

[3] Tushar Dhar Shukla;G. Radha;Dharmendra Kumar Yadav;Chaitali Bhattacharya;Rvs Praveen;Nikhil N. Yokar, "Advanced Student Success Predictions in Higher Education with Graph Attention Networks for Personalized Learning", 2024 First International Conference on Software, Systems and Information Technology (SSITCON), DOI: 10.1109/SSITCON62437.2024.10796791

[4] V. Yamuna;Praveen RVS;R. Sathya;M. Dhivva;R. Lidiya;P. Sowmiya, "Integrating AI for Improved Brain Tumor Detection and Classification" 2024 4th International Conference on Sustainable Expert Systems (ICSES), DOI: 10.1109/ICSES63445.2024.10763262

[5] Rvs Praveen;Aktalina Torogeldieva;B Saravanan;Ajay Kumar;Pushpa Rani;Bhimanand Pandurang Gajbhare, "Enhancing Intellectual Property Rights(IPR) Transparency with Blockchain and Dual Graph Neural Networks" 2024 First International Conference on Software, Systems and Information Technology (SSITCON), DOI: 10.1109/SSITCON62437.2024.10795998

[6] Sarthak Sharma;Suman Vij;RVS Praveen;S. Srinivasan;Dharmendra Kumar Yadav;Raj Kumar V S, "Stress Prediction in Higher Education Students Using Psychometric Assessments and AOA-CNN-XGBoost Models," 2024 4th International Conference on Sustainable Expert Systems (ICSES), DOI: 10.1109/ICSES63445.2024.10763288

[7] RVS PRAVEEN et al.: NEXT-GENERATION CIRCUITS FOR INDUSTRY 4.0 USING INNOVATIONS IN SMART INDUSTRIAL APPLICATIONS, ICTACT JOURNAL ON MICROELECTRONICS, OCTOBER 2024, VOLUME: 10, ISSUE: 03, DOI: 10.21917/ijme.2024.0323

[8] P. Vajpayee, A. Shrivastava, S. S. Rajput and G. K. Sharma, "Wide output swing inverter fed modified regulated cascode amplifier for analog and mixed-signal applications," TENCON 2009 - 2009 IEEE Region 10 Conference, Singapore, 2009, pp. 1-5, doi: 10.1109/TENCON.2009.5395981.

[9] A. Shrivastava and A. K. Pandit, "Design and Performance Evaluation of a NoC-Based Router Architecture for MPSoC," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, India, 2012, pp. 468-472, doi: 10.1109/CICN.2012.85.

[10] A. K. Singh, A. Shrivastava and G. S. Tomar, "Design and Implementation of High Performance AHB Reconfigurable Arbiter for Onchip Bus Architecture," 2011 International Conference on Communication Systems and Network Technologies, Katra, India, 2011, pp. 455-459, doi: 10.1109/CSNT.2011.99.

[11] Shrivastava, A. and Sharma, S.K., (2016), "Efficient bus based router for NOC architecture", World Journal of Engineering, Vol. 13 No. 4, pp. 370-375. https://doi.org/10.1108/WJE-08-2016-049

[12] A. Shrivastava and S. K. Sharma, "Various arbitration algorithm for on-chip(AMBA) shared bus multi-processor SoC," 2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2016, pp. 1-7, doi: 10.1109/SCEECS.2016.7509330.

[13] A. Shrivastava, J. Ranga, V. N. S. L. Narayana, Chiranjivi and Y. D. Borole, "Green Energy Powered Charging Infrastructure for Hybrid EVs," 2021 9th International Conference on Cyber and IT Service Management (CITSM), Bengkulu, Indonesia, 2021, pp. 1-7, doi: 10.1109/CITSM52892.2021.9589027.

[14] K. Kumar, A. Kaur, K. R. Ramkumar, A. Shrivastava, V. Moyal and Y. Kumar, "A Design of Power-Efficient AES Algorithm on Artix-7 FPGA for Green Communication," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 561-564, doi: 10.1109/ICTAI53825.2021.9673435.

[15] Jitendra Singh Kushwah, Deepak Gupta, Anurag Shrivastava, P. Ambily Pramitha, John T. Abraham,

Munindra Lunagaria, Analysis and visualization of proxy caching using LRU, AVL tree and BST with supervised machine learning, Materials Today: Proceedings, Volume 51, Part 1, 2022, Pages 750-755, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.06.224.

[16] Kumar, A. Suresh, Kumar, S. Jerald Nirmal, Gupta, Subhash Chandra, Shrivastava, Anurag, Kumar, Keshav, Jain, Rituraj, IoT Communication for Grid-Tie Matrix Converter with Power Factor Control Using the Adaptive Fuzzy Sliding (AFS) Method, Scientific Programming, 2022, 5649363, 11 pages, 2022. https://doi.org/10.1155/2022/5649363

[17] Mukesh Patidar, Anurag Shrivastava, Shahajan Miah, Yogendra Kumar, Arun Kumar Sivaraman, An energy efficient high-speed quantum-dot based full adder design and parity gate for nano application, Materials Today: Proceedings, Volume 62, Part 7, 2022, Pages 4880-4890, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2022.03.532.

[18] Bikash Chandra Saha, Anurag Shrivastava, Sanjiv Kumar Jain, Prateek Nigam, S Hemavathi, On-Grid solar microgrid temperature monitoring and assessment in real time, Materials Today: Proceedings, Volume 62, Part 7, 2022, Pages 5013-5020, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2022.04.896.

[19] Mohit Chandra Saxena, Firdouse Banu, Anurag Shrivastava, M. Thyagaraj, Shrikant Upadhyay, Comprehensive analysis of energy efficient secure routing protocol over sensor network, Materials Today: Proceedings, Volume 62, Part 7, 2022, Pages 5003-5007, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2022.04.857.

[20] A. Rana, A. Reddy, A. Shrivastava, D. Verma, M. S. Ansari and D. Singh, "Secure and Smart Healthcare System using IoT and Deep Learning Models," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 915-922, doi: 10.1109/ICTACS56270.2022.9988676.

[21] A. R. Yeruva, P. Choudhari, A. Shrivastava, D. Verma, S. Shaw and A. Rana, "Covid-19 Disease Detection using Chest X-Ray Images by Means of CNN," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 625-631, doi: 10.1109/ICTACS56270.2022.9988148.