© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716911

Deep Learning Fraud Detection in Mobile Payment Transactions

NAVEEN KAMBLE[1], PRAFUL S[2], ROHITH V[3]
[1,2,3]*Dept of Computer Science & Engineering, Dayananda Sagar University, Bengaluru, Karnataka, India*

Abstract- ***With growing digital UPI payment platforms for online payment, concurrently there is rise in digital fraudulent activities which can cause financial loss for individuals, businesses, Govt entities. So to prevent such losses and digital fraudulent activities there is requirement of Deep learning models. Deep learning is nothing but a branch of Machine learning which uses neural network to learn large set of previously stored data and analyze real-time transactions to conclude the transactions as genuine or fraud and detect the suspicious activity. It inspects thoroughly advances in models, such as Artificial Neural Network [ANN], Recurrent Neural Network [RNN], Long-short term memory [LSTM], Gated recurrent units [GRU], and Auto-encoders. As a key volunteer, this study initiates Deep Learning-Sector-Governance [DLSG] framework. By incorporating above introduced models, this review offers practical counselling for researchers, industry practitioners working to avert fraud activities.***

Keywords - Deep learning; Machine learning; ANN; RNN; LSTM; GRU; Auto-encoders; Fraud detection, UPI.

I. INTRODUCTION

Fraud in mobile payment transactions includes ambiguous activities such as otp-theft, account takeover, suspicious links, phishing attack, fake payment request-resulting in humongous economic losses and eroding trust in financial institutions. According to global calibrations, entities loose approximately 5% of their annual revenue due to fraud. The wave of digital transaction exceeding-billions in the globe has escalated new tracks and increasing the frequency of sophistication of fraud attempts.

Traditional methods for fraud detection are not enough as they are rulebased algorithms, and they require manual inspection which is increasingly insufficient. Relying on traditional methods can often cause late responses by producing false positives because of their rigidity in adapting to evolving fraud tactics. With respect to that, the above proposed models improve fraud detection accuracy and help reduce financial losses. Models such as ANN, RNN, GRU, LSTM, and Auto-encoders are proficient in real-time detecting malicious activity, entitling adaptive responses to fraud. In addition, Deep learning (DL) models are increasingly lined-up with data protection, making them appropriate for deployment in confidentiality. These models not only upgrade fraud detection proficiency but also line up with evolving legal landscape governing financial data use.

In defiance of their promise, DL applications for fraud detection face significant challenges. Key components include the need for high-quality labeled data, the difficulty of interpreting model-decisions, and ethical concerns regarding transparency and fairness. Addressing these limitations requires a comprehensive understanding of the current trends and methods in DL applications for fraud detection.

II. LITERATURE REVIEW

For this research paper I have gone through articles on SCPUS, google scholar, and GOI (Govt of India) released data. According to calibrated data provided by the Ministry of Home Affairs (MAH), India, Indians has faced a loss of over 22,845 crore rupees in the fiscal year 2024-25, which represents a 206% increase in compare with over 7,465 crore rupees in the fiscal year 2022-23. According to officials in India, in the fiscal year 2024-25, the calibrated online UPI transactions via digital UPI payment platforms was 228 billion, and the rupee count was about 30 trillion.

In recent years, deep learning (DL) has become increasingly significant in mobile payment

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716911

transactions due to its ability to handle complex, highdimensional datasets. As highlighted by Ozbayoglu et al. (2020), advanced deep learning models like gated recurrent units (GRUs), recurrent neural network (RNNs) have determined superior performance in compare with traditional method algorithms, particularly in identifying non-linear fraud patterns and intricate. Of all these perspectives, graph neural networks (GNNs) have attained noteworthy attention for their efficiency in work. A supervised review revealed that most astounding GNN-based studies depend on supervised or semi-supervised frameworks. However, there is acceptable potential for developing unsupervised GNN models that can catch previously untouched fraudulent activities.

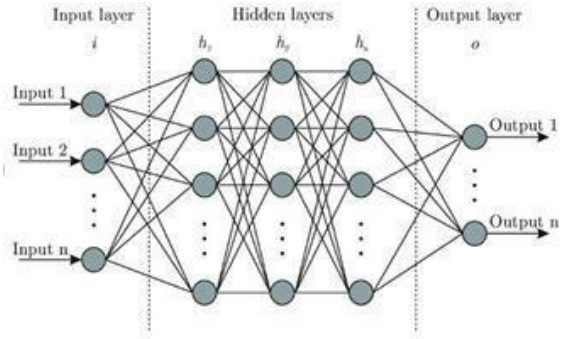

Figure 1: Architecture of ANN Algorithm (Source: Ozbayoglu et al., 2020).

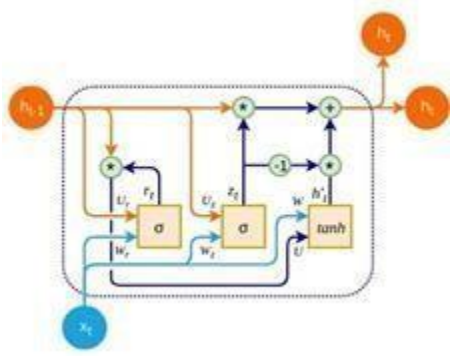

Figure 2: Architecture of GRU Algorithm (Source: Ozbayoglu et al., 2020)

III. METHODOLOGY

An overarching search technique was developed to find-out clone studies using databases like SCPUS, google-scholar, and IEEE-Xplore in aspect of having strong coverage of inter-disciplinary and technical reports. Going through all these databases thoroughly I end-up with the following conclusion-

Sl no.	Name of Model	Working	Formula
1.	Artificial Neural Network [ANN]	Each node reflects neurons, calibrating the weighted sum of inputs, and applying an activation function to demonstrate fraud probability.	$Zi = \sum_{nj=1} wijxj + bj$ $a_i = \sigma(z_i)$ Where, x_j = input features wij = weights bi = bias σ = activation function
2.	Recurrent Neural Network [RNN]	Analyze sequential transaction data (e.g., last 10 trans) by retaining context from previous inputs.	$ht = \sigma$ (Whhht-1 + Wxhxt + b_h) $yt = \sigma$ (Whyht + by) Where, h_t = hidden state t = time x_t = current inputs ht-1 = previous hidden state
3.	Gated Recurrent Units [GRU]	Use 'reset' & 'update' gates to decide how much past information to forget or update for current transactions.	Update gate (z_t): $z_t = \sigma$ (W_z.[h_t-1 , x_t]) Reset gate (r_t): $r_t = \sigma$ (W_r .[h_{t-1} , x_t]) lidate state ($\hat{h}_t$): $\hat{h}_t$ = tanh(W.[r_t * h_{t-1} , x_t])

- Good at grouping instead fails to snap the 'sequence' or timing of transactions, making them difficult to sequential models.
- Mastery to clean gradient problems, result to less attractive than LSTMs/GRUs for vast sequences.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716911

- Consistently vomits the notable accuracy (approx. 90.6% - 99.8%) for mobile fraud due to its effectiveness over LSTM in modeling temporal fraud.

IV. EXPERIMENTAL RESULT

The main aim of implementing the above proposed models was to find examples of digital payment system-fraud, with aspect of P2P (persontoperson) transactions where relational patterns and tactics constantly manifest. The above proposed DL models have been implemented across different sectors of financial fraud domains mainly integrated in mobile payment transactions and came up with the following conclusions-

Architectur e	Accuracy	Precision	Recall	Inference time(ms)	Model Size
RNN	94.6%	70%	66%	8.7	Small
LSTM	98.7%	93%	85%	23.2	Large
GRU	97.3%	89%	86%	14.4	Medium

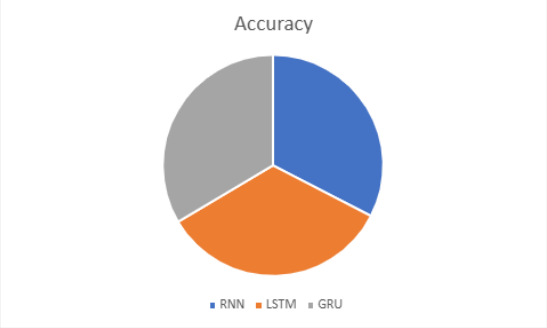

Figure 3: Accuracy (%) of DL models

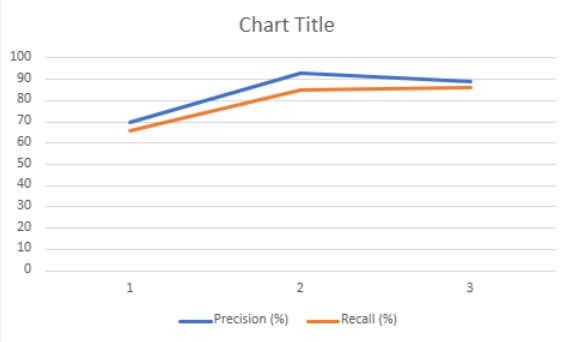

Figure 4: Comparison of Precision (%) and Recall (%)

V. DISCUSSION

The end results of this study highlight the effectiveness of DL techniques used in detecting fraudulent activities in mobile payment applications. As mobile payment transactions tend to augment globally, fiscal institutions will be in need of intelligent systems that can be able to recognize suspicious activity in a short time and avert humongous financial loss. DL models are competent in evaluating large volumes of transaction data and identifying concealed patterns which are not easy to detect using traditional rule-based algorithms. The above DL models evaluate different types of transaction components like transaction frequency, device information, location, and user behavior patterns. By calibrating all historical data models conclude the transaction as genuine or fraud with improved efficiency.

VI. STATEMENT OF LIMITATION

- Data confidentiality: Users financial sensitive data must be kept from transparency and must be handled cautiously to obey the regulations.
- Contentious attacks: Fraudsters may seek game DL models cloning normal patterns.
- Model drift: Fraud patterns evolve with respect to time, so retraining models is necessary.
- Comprehensible: Ensuring that DL models are not only effective but also explainable.

VII. CONCLUSION

This paper reflects the pivotal role of DL models in restructuring financial fraud detection within a vastly emerging digital landscape. Through a complete review of research papers published in SCPUS, google scholar, and IEEE-Xplore, it can conclude that DL models like- artificial neural networks (ANN), recurrent neural networks (RNN), gated recurrent units (GRU), and auto-encoders have constantly improved the detection patterns of complex and dynamic fraud patterns across various fiscal sectors. Continued with worldly preprocessing techniques and feature engineering tactics, these models come up with facing challenges like class imbalance and data sparsity, and the need for acceptable solutions for real-time fraud detection.

REFERENCES

[1] Chen, Y., Zhao, C., Xu, Y., Nie, C., Zhang, Y., Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications, Data Science and Management, https:// doi.org/10.1016/j.dsm.2025.08.002.

[2] Ms. Nibedita Mukhopadhyay and Prof. Dr. Mahadeb Mukhopadhyay (2024). UPI FRAUDS A STUDY ON UPI USAGE, AWARENESS AND IMPACT IN INDIA, International Journal of Research in Commerce and Management Studies (IJRCMS) 6 (6): 179-197 Article No. 312 Sub Id 594.

[3] Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems, 55, 278–288.

[4] Hajek P, Abedin MZ, Sivarajah U. Fraud Detection in Mobile Payment Systems using an XGBoost-based framework. Inf Syst Front. 2022 Oct 14: 1 – 19. Doi: 10. 1007 /s10796-022-10346-6. Epub ahead of print. PMID: 36258679; PMCID: PMC9560719.

[5] Ozbayoglu, A. M., Gudelek, M. U., & Sezer, O. B. (2020). Deep learning for financial applications: A survey. Applied Soft Computing, 93, 106384.