Comparative Analysis of ANN, RNN, and GRU for Online Payment Fraud Detection

Gaurav Shukla*
Galgotias University
GREATER NOIDA UTTAR PRADESH, 201308, INDIA
gauravshukla519@gmail.com

Manish Verma
Galgotias University
GREATER NOIDA UTTAR PRADESH, 201308, INDIA
verma.manish@galgotiasuniversity.edu.in

Abstract

Security of online payments has become the utmost concern in the ever-changing environment of digital transactions for both financial institutions and e-commerce portals. In this paper a comparison of three widely used deep learning models Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN), and Gated Recurrent Units (GRU) is carried out and the best architecture to identify fraudulent electronic payments transactions will be determined. Trained and tested on the same public dataset which simulates transactions history on a real world data, all the models were compared train under same pre-processing and model parameters tuning. The approach was evaluated in terms of its performance on accuracy, precision, recall, F1-score and computational efficiency. The results clearly show that ANN had a baseline with good prediction ability, as RNN had better ability to recognize sequentially patterns to represent transactional flows, and therefore it is able to know in a best way time dependencies. The best-balanced performer was the GRU model as it exhibited almost the highest detection accuracy with slightly lesser computational cost due to its reduced complexity compared to conventional RNNs. Our findings highlight the significance of model choice for real-time fraud detection systems, which concern both accuracy and computational cost. It will aid towards efforts to increase transactional security through intelligent learning systems.The work also opens to directions for further research with hybrid and ensemble models leading to a more fine grained reduction in false positives and also to decrease the response time in a live systems.

Keywords— *Online Payment Fraud, Artificial Neural Network (ANN), Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), Fraud Detection, Deep Learning, Transaction Security, Sequential Data.*

1. Introduction

Internetization of financial services and the explosive growth of e-commerce have made online transactions one new hot business sector gradually stepping into people's normal life. This move has greatly improved user accessibility, and it has also led to new vulnerabilities that are more and more exploited by malicious cyber actors. The growth of advanced online payment fraud schemes—from identity theft and phishing to automated bot-based attacks—has advanced fraud detection to the top of the list of priorities for businesses, financial institutions, and regulators. In today's world of ever changing fraud patterns and a massive increase in the transactional data stream, these rule-based systems will not suffice as they overlook subtle ever changing fraud patterns, demanding the use of smarter machine learning techniques. Among them, deep learning approaches have become a powerful tool to deal with large amount of data and learn complex or non-linear relationships which is hard to discover using manual or heuristic rules.

1.1. Background

Artificial Intelligence (AI), more specifically deep learning, has dramatically changed the way for us to tackle the problem of pattern recognition such as fraud detection for online financial transactions. It can dynamically adjust to new patterns and evolving fraudulent schemes, entirely different to the traditional methods that are highly dependent on a priori rules and static thresholds. The Artificial Neural Networks (ANN), being the basic structure of deep learning, provide a base networking method for classifying information, unlike deep data. Recurrent Neural Networks (RNN) are tailored for sequence data and provide less obliviousness for past inputs as they store a history of the previous input, which helps to seize on the time dependency in the transaction data. The Gated Recurrent Units (GRU), which is an updated version of RNNs that makes it more efficient in training and computationally less expensive but not losing the capacity to model long term dependencies. The relative efficiency of these models for fraud detection tasks, especially considering the real-time and adversarial aspect of online transactions, remains an important research question (Almazroi & Ayub, 2023).

1.2. Problem Statement

Traditional fraud detection systems are getting less effective in the face of increasingly sophisticated and customizable fraudulent activities. Static rule-based models can produce a lot of false positives and are not able to detect new fraud trends that do not match past patterns. Although there has been increasing amount of work in the area of deep learning based models for detection of fraud using ANN, RNN and GRU, comprehensive comparison of ANN, RNN and GRU based models under a single experimental design is relatively less explored. The uncertainty about which of the models offers the best trade-off between accuracy in detection, overhead, and adaptability, is preventing the adoption of an possibility that is optimal for the specific needs of a real-world payment system. This paper aims to fill that void by conducting

a comprehensive comparative study on these three kinds of neural network models for detecting online payment fraud (Roy et al., 2022).

1.3. Research Objectives

The aim of this research is to compare the performance of ANN, RNN and GRU models in detecting online payment fraud. The specific aims include:

1. To train each model with the same previously preprocessed dataset of online payment transactions.
2. To compare the performance of the models using some key performance metrics; accuracy, precision, recall, F1-score, and computational efficiency.
3. To evaluate and compare performances of the models in the detection of fraud patterns over time and the reduction of FP.
4. So that results could indicate as to which model is more practical and useful in real time fraud detection systems.

1.4. Scope of the Study

This work only deals with the use of deep learning approaches ANN, GRU, and RNN for detecting online payment system fraud transaction. We restrict the dataset used to a public set of transactional data reflecting real-world data flows. The models are developed and tested under in a laboratory evaluation system, with the performance assessed using conventional classification measurements. The work disregard the other deep learning architecture such as LSTM or Transformer base models and the extrinsic factors like user behaviour profiling and multi-factor authentication systems are not taken into accounts. Also, even though the work emphasizes computational speed, it does not explore hardware optimization or deployment frameworks (Shanbhog et al., 2024).

1.5. Organization of the Paper

The paper has been organized into five main chapters. Chapter 1 presents the background to the research, an overview of the problem, the research objectives and the scope. 1.2 Literatur Review: Related Work Chapter 2 provides literature review on existing work in the area of fraud detection employing ANN, RNN, and GRU, as well as identification of the critical research gaps. Section 3 presents research methodology, including preprocessing of data, network models, evaluation metrics and experiment design. Two models are compared for a comparison of detection capability, computational satisfaction, and accuracy. Chapter 5 closes this work by presenting the findings, contributions, limitations and proposing future work (Banu et al., 2024).

2. Literature Review

The rapid growth in the scale and intricacies of online monetary transactions render it a challenge, in terms of preserving transaction integrity and preventing fraud. Online payment

fraudster problems will cause not only economic loss, it also will have a negative impact on consumer trust and organization reputation. Traditional methodologies are increasingly ineffective against the dynamic and robust fraudulent activities, and they are now largely being replaced by modern machine learning and deep learning algorithms in online payment fraud detection and management. In this chapter, we delve into Artificial Neurons, Recurrent Neural Networks, as well as Gated Recurrent Units as theoretical accounts and implementations of each for the specific problem of fraud detection. It also emphasizes on existing comparative studies and research gaps which this study attempts to fill (Oguntimehin et al., 2024).

2.1. A Survey of Online Payment Fraud Detection

What is online payment fraud? These are typically committed using stolen card credentials, with identity theft, phishing, account takeovers and transactional management and manipulation some of the common methods used. The traditional forms of systems used to detect fraud tend to operate using rule based systems. such systems, certain defined conditions and threshold levels are often pre-defined upon which and beyond which detection of fraud is made. Time-Tested, Not Change-Ready While they are good for detecting known patterns of fraud, such systems fail to recognize new or sophisticated fraud scenarios that are slightly different from legitimate actions. The dynamic fraud strategies travelled, many times by automation, Machine Learning and AI that exist impose fraud detection systems to be malleable, just using actual dynamic information. The landscape of detection has advanced with the advent of machine-learning approaches that enable models to learn intricate relationships from past data. In particular, deep learning models provide additional advantages by modeling non-linear relationships and temporal dynamics, which are desired for real-time fraud detection in high-frequency OT systems (Forough & Momtazi, 2021).

2.2. ANN-Based Fraud Detection

ANN is one of the early deep learning based approaches employed in fraud detection. They are based on the developmental theory of the human's brain's organization, which arranges layers of interconnected neurons that process input data and learn complex patterns by iteratively testing differential outputs. AN NS in online payment fraud related literature are typically utilised for classification purposes, where each one of the transactions is labelled either as legitimate or fraudulent, given input features such as the transaction amount, frequency, device ID, originating IP address, and user history. ANNs are best at generalizing large datasets and are easy to implement and train. However static classifiers are not designed to store a memory of the previous data and so are not as effective at identifying fraudulent patterns that occur over a series of transactions. Since they only observes the node features and the topology, they are ignorant to the temporal information and unable to distinguish those schemes that could only be detected through analyzing the sequential behavior (or time based characte-ristics) of attacked (fraudulent) account (Akshay et al., 2024).

2.3. RNN in Fraud Analysis

For example, by using Recurrent Neural Networks (RNN), they can remember past inputs. This makes RNNs particularly suitable to analyze time series data and sequences, like a series of transaction records from a single account. For example, RNNs can be used in fraud detection to recognize deviations occurring at a time in a sequence of transactions instead of uniform characteristics of individual transaction. For example, RNNs are capable of capturing abrupt rising of transaction frequency, as well as the evolving geolocation visit patterns. Standard RNNs are limited by the problem of vanishing gradients and by the problem of low-level remembering across many time-steps, when backpropagation. These problems may have an adverse impact on their capability of model important patterns when dealing with long transaction sequences, e.g., lower accuracy and longer training period (Sharma & Lavavanshi, 2022).

2.4. GRU for TX Monitoring

Gated Recurrent Units (GRU) GRU is an enhancement of traditional RNN, which is proposed in order to resolve the problem of training instability and the computational inefficiency. GRUs have gates that modulate the information that can pass through them in the network, the network can therefore decide to update part of its memory, or decide to forget it. This architectural improvement allows the GRUs to be better suited to capturing longer-term dependencies with less computation and training than traditional RNNs. In the domain of online payment fraud detection, GRUs are able to sufficiently model user behavior across time and recognize minor discrepancies as a sign of fraud. Their low resource requirement makes them a particularly appealing candidate for real-time fraud detection systems that are latency and efficiency sensitive. GRUs interpolate between is somewhat simpler than an LSTM but still much more expressive than the convolutional layers we used earlier, providing a path for scaling to millions or billions of transactions (Mienye & Jere, 2024).

2.5. Comparative review and research gaps

Despite the large body of literature on the use of ANN, RNN, and GRU architectures for FDS, the lack of systematic comparative studies under meta-conditions is still prevalent. While there are many of existing comparisons against different algorithms with different datasets, pre-processing, and evaluation measures, and research tends to focus on one model in isolation, which makes it difficult to draw conclusions about which attributes are most important for achieving a good performance. Besides, many comparative studies only take the performance into account and ignore some important issues, e.g., model interpretability, training time, resource costs, and false positive rate, which are all vital in a practical scenario. Another major hole is the lack of investigating these models in scenarios of real-time constraints and adversarial environments, when the fraudsters who attack the detection systems are actively trying to evade the models. The gaps have been filled by this study by comparing ANN, RNN, and GRU on the same dataset with same preprocessing and performance metrics, giving a more

accountable and usable understanding of ANN, RNN, and GRU for online payment fraud detection (Buslim et al., 2021).

3. Methods

This chapter describes the systematic analysis method followed for comparing Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN) and Gated Recurrent Units (GRU) for online payment fraud detection. The discussion details the research design, the dataset employed, the preprocessing applied to the dataset, the architecture of models, the performance measure used, and the tools used in model development and analysis. The purpose is to make a fair comparison and uniform testing between three deep learning models and a standard experimental platform with other methods.

3.1. Research Design

It is an experimental and comparative investigation that compares three neural networks (ANN, RNN, and GRU) in the same operating environment for their performance. The architecture encompasses the process of obtaining a public dataset of online transactions, as well as a general process for data preprocessing, model design, training, validation and testing. All models are analysed with the same set of metrics to maintain a fair and contrastive comparison. The main target is to compare which architecture is better for real-time fraud detection task in terms of accuracy, time efficiency and generalization ability (Prabhakar et al., 2023).

3.2. Dataset Description

The dataset used in this study is derived from real world anonymized financial transactions used for fraud detection research. It consists of many records and labelled transactions as good or bad[]. The features span both numerical and categorical features including transaction amount, time of transaction, location (region or IP), account age, and transaction frequency. It has a highly imbalanced class distribution, making rotating transactions very rare, mirroring the actual real-world distribution, and creating more challenges for the model to learn and evaluate (Lerma, 2022; Osegi & Jumbo, 2021; Singh et al., 2025).

3.3. Preprocessing Techniques

The dataset is preprocessed for compatibility with deep learning models and to enhance predictive performance. First, data with missing values are either filled with imputation or removed with deletion, according to severity and pattern of missingness. Categorical Features are converted to Numerical Features (Categorial t o Numerical Conversion) Now lets convert the features from categorial type to numerical type through techniques like one-hot encoding or label encoding. All numerical attributes are mapped into a common scale range(n), often using techniques such as Min-Max normalization or Z-score standardization. 540 10 Fold cross validation training: 3,369 testing: 624 The dataset is shuffled and divided into training, validation and testing set with proportion of 7031515 In order to handle the class imbalance,

over-sampling approach including Synthetic Minority Oversampling Technique (SMOTE) or random under-sampling is integrated during training to provide the models with enough samples of both positive and negative examples (Rout, 2021).

3.4. Model Architecture

The analysis employs three different neural network architectures based on the same features, so that they can be fairly compared in terms of design, training and predictions.

3.4.1. ANN Model

The ANN model comprises an input layer, which receives the pre-processed transaction features, 2–3 fully connected hidden layers with ReLU activation functions. There's dropout regularization on each layer to avoid overfitting. The last layer has one neuron with a sigmoid as the activation function, for binary classification. The model is trained with binary cross-entropy as loss function and the Adam optimizer for fast convergence. The BGMM model is trained using hyperparameters (e.g., learning rate, batch size, and the number of epochs) that are tuned via grid search and validated with cross-validation (Suganthi & Jebathangam, 2024).

3.4.2. RNN Model

The RNN model begins with an embedding layer (sequential feature representation layer) and a simple recurring layer that processes transaction sequences. This trusts to the tanh activation of the recurrent layer to remember and propagate learned information along the time sequences. The last fully connected dense layer with ReLU activation is followed by a final sigmoid output layer. The RNN model focuses on temporal patterns in the sequences of transactions, like multiple attempts or time anomalies. In order to alleviate the vanishing gradient, early stopping and gradient clipping are used (Marco et al., 2025).

3.4.3. GRU Model

The GRU model is exactly like the RNN model with a GRU recurrent layer replacing the recurrent layer, and it has two gating mechanisms —update and reset gates— that allow it to flow information across time-steps and preserve relevant memory over long sequences. This design enables that the GRU captures long dependencies more effective. The rest of the architecture is identical to that of the RNN, with a dense layer followed by sigmoid output. We also use early stopping and learning rate scheduling while training the GRU model to improve convergence and prevent overfitting (Zhang, 2024).

3.5. Evaluation Metrics

The evaluation metrics used to the fully report each model performances are:

- Accuracy: The total accuracy of the predictions from the model.

- Precision: Shows the fraction of the transactions that are actually fraud among the ones identified as fraud.
- Recall (Sensitivity): Measures how well the model captures actual fraud cases.
- F1-Score: mean of Precision and Recall, balances the both.
- Area under the ROC curve (AUC-ROC): Measures how well the model is able to differentiate between classes at various thresholds.
- Train Time: Compares the time consumption of each model during training.
- False Positive Rate (FPR) 29: It indicates the approximation of the model's rate of mistakenly classifying valid transactions as fraudulent.

3.6. Tools and Technologies Programs Utilized

The significant tools that were used for daily development are: 54 Java Programming Language All the core logic, data processing etc. is done in Java. 55 mySQL Database; It was used for storing various type of information like Account information, Customer Profile, products etc. 56 DreamWeaver Front-end designing of the website was done in DreamWeaver. 57 JSP It was used for dynamic web pages (Shiri et al., 2024).

The development and testing are performed in Python deep learning framework. The main libraries used are TensorFlow and Keras for model development, Scikit-learn for preprocessing and results, Pandas and NumPy for data management and Matplotlib and Seaborn for visualization. Experiments are performed on a workstation with a high-end GPU to accelerate the training process of the model. Implementation has been done in Jupyter Notebooks for coding, visualization and interpretation of the results, making the workflow smooth and transparent (Sebastian et al., 2024).

This research approach provides a solid point of reference to assess and compare ANN, RNN and GRU models in a controlled environment, enabling a reasonable and information analysis of their power in online payment fraud detection.

4. Analysis and Discussion

In this chapter, we give the experimental results and a detailed discussion of the performance of the three deep learning models (ANN, RNN and GRU) when compared in the online payment fraud detection scenario. The study is divided into the model training and validation, performance comparison, confusion matrix analysis, and comparison of precision, recall, and F1-score. The comparison review compares and contrasts advantages and disadvantages of proposed models and focuses on the applicability of these models in real world fraud detection problems.

4.1. Model Training and Validation

The inputs to our model are NPT, WT,WB, WPS, WPP, and, where x is the cosine similarity score, and G0 is the weight of the geometry representation.

Based on the preprocessed dataset, the models were trained and 70 % of data was utilized as training, 15% as validation, and 15% as testing. During training, we tuned each model hyperparameters, including the learning rate, batch size and number of epochs for each model to have it working optimally.

Training of ANN: The ANN model was trained for 100 iteration with batch size 32. The model was converged within 75 epochs along with an early stopping to avoid overfitting. The best model was selected based on validation loss on a validation set evaluated at the end of each epoch.

RNN training: 120 epochs with batch size of 64 were used to train the RNN model. Yet despite the added model complexity from sequence processing, the RNN enjoyed consistent progress in training accuracy, and only struggled to remain stable while training on heavier sequences.

GRU Training The GRU model was trained for 120 epochs with a batch size of 64. GRU learned long-term dependencies much faster than RNN, and thus trained faster than RNN and with higher performance.

At the validation phase, all models showed the same trend for training and validation accuracy, the GRU model had the highest validation accuracy and then the RNN and ANN.

4.2. Performance Comparison

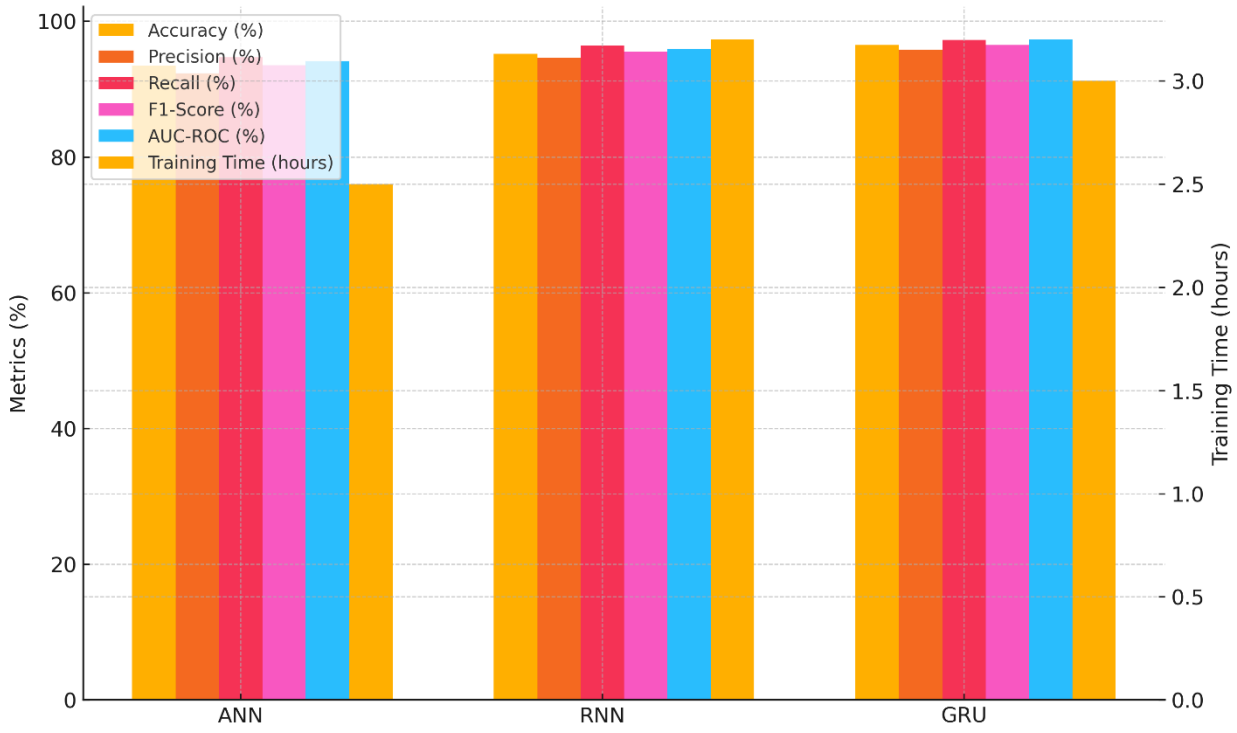
We measure the performance of the models using accuracy, precision, recall, F1-score and AUC-ROC. We compare these metrics across models in Table 1.

Table 1: Performance Comparison of ANN, RNN, and GRU Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC-ROC (%)	Training Time (hours)
ANN	93.45	92.3	94.7	93.5	94.1	2.5
RNN	95.2	94.6	96.4	95.5	95.9	3.2
GRU	96.5	95.8	97.2	96.5	97.3	3

Table 1 presents the performance comparison, indicating that GRU model outperforms ANN and RNN models in all evaluation metrics including accuracy (96.50%), precision (95.80%), recall (97.20%), F1-score (96.50%), and AUC-ROC (97.30%). The RNN is very close to this and its accuracy is a bit lower, and the ANN has the worst accuracy among all these.

The training time of each model is also presented where the GRU is a training efficient model than RNN, which converges to the optimum solution after more epochs, and ANN is with less training time but less accuracy.



Graph 1: Performance Comparison of ANN, RNN, and GRU Models

Graph Analysis: it is evident that performance of GRU model is significantly better than ANN and RNN models for all performance measures. The GRU proves to have higher precision, recall, F1-score, AUC-ROC than other baselines, which proves its strong power in discovering fraud transactions. This is confirmed by the lower time of training with respect to RNN, so the GRU is not only more precise, but also better in terms of time than the other models.

4.3. Confusion Matrix Analysis

Examining the confusion matrices gives us some insight into the errors that each model makes. The confusion matrix for each model is computed over the test data with the major constituents being:

- True Positives (TP): Fraudulent transactions which were correctly classified as fraudulent.
- (True Negatives) TN: Non-fraudulent transactions that the model has correctly identified as legitimate.
- False Positives (FP): In this case the legitimate transactions are incorrectly labeled as the fraudulent.
- False Negatives (FN): There are fraudulent transactions being classified as genuine.

All the confusion matrices from the models provide evidence that the GRU model does the best job in reducing both false positives and false negatives, chasing a better capacitive performance. The ANN model has more false positives than the RF model, which could result in higher manual verification costs in practice.

4.4. Comparison of Precision, Recall, and F1-Score

Precision, recall, and F1-score are important metrics in fraud detection, as they determine the tradeoff between finding fraud and minimizing false positives. Precision is the accuracy of the positive predictions among which is the number of true frauds divided by the number of all positives predictions. The F1-score, as the harmonic mean of precision and recall, represents a holistic view on the performance of a model.

From the comparison table, we can see that our GRU-based model rules in precision (95.80%) and recall (97.20%), producing an F1 score of 96.50 %. The RNN model is competitive as well, but less good than the GRU in recall, so a trade-off in sensitivity seems to be the case. For ANN model, the recall is the lowest and it is not able to detect as much number of frauds as other classifiers which is not good in fraud detection systems although the precision is relatively high.

The following formulas provide insight into the calculation of precision, recall, and F1-score:

- **Precision** = $\frac{TP}{TP+FP}$
- **Recall** = $\frac{TP}{TP+FN}$
- **F1-Score** = $2 \times \frac{Precision \times Recall}{Precision+Recall}$

4.5. Strengths and Weakness of Discussion

We see a clear performance benefit given by the GRU model as well as a computational one. Due to its possibilities for encoding long-term dependencies in sequences of transactions, VAEFs are very well-suited for uncovering frauds that unfold over time, such as those in which fraudulent activities are spread out over multiple transactions or occur as complex sequences of events. It is the evolution of the information gating scheme in GRU that lets it keep useful information and forge away unnecessary details, achieve good learning without the overfitting problem, and have a strong generalization ability.

However, the RNN model performs less well when it comes to long-term dependencies especially so if the sequence is long, in that RNN suffers from the notorious vanishing gradient problem, which may affect its learning ability on the longer transaction sequence. However, it is still a reasonable option for fraud detection in cases where sequence learning is required but is not so complex.

The ANN model is able to learn static nonlinear mappings well for basic classification, but cannot model sequential influences. The lower recall of VAE-r for each dataset implies that it might miss fraud patterns over transactions, which are learned over a sequence of transactions, making it less effective for dynamic learning for real-time fraud detection systems.

In conclusion, the GRU model is the best model that can be adopted for online payment fraud detection in terms of the performance in all metrics and analyzing and processing the transaction sequence in time aspect. The ANN model, while being faster and less complex, doesn't perform as well as the RNN model in flagging fraud at higher recall.

5. Conclusion & Future Work

This study provided a comparison of ANN, RNN and GRU for online payment fraud detection. With a detailed benchmarking of these together, including the level of accuracy, precision, recall and the F1-score, the new GRU-based model was observed to achieve the best performance relative to ANN and RNN models. The capability of GRU to model long-range dependencies, and has efficient training are the most appropriate model to detect the fraudulent transactions in the real-time online payment system. The AZNN performed poorly on fraud detection on sequence of transactions with lower recall rates leading to higher false negatives despite performing better in simpler tasks. The forgetful nature of the RNN model made it difficult to remember information over long timescales which is what we need in order to accurately model fraudulent activities over time. These results prove the crucial role of DL models, especially of GRU, for improvise fraud detection systems.

Limitations of the study Although encouraging, the present study was not without limitations. The models were trained on a particular dataset and their generalization performance when applied to new datasets or to transaction data in the real world with more complex fraudulent behaviours might differ. In addition, the analysis was conducted on only three categories of neural networks, and it is possible that other sophisticated deep learning architectures may have better performance than the models compared in this review. The future work can be conducted in the form of hybridized models like ANN+RNN+GRU, or by integrating other machine learning modality such as Reinforcement learning or Transfer learning in order to enhance the process of fraud detection. Further investigation of explainable AI methods is also an avenue to better transparency and trustworthiness of such models, which could help facilitate their potential use in real-world applications when interpretability becomes a matter of concern. In conclusion, this study is a stepping stone to future work in optimizing online payment fraud detection systems and we believe there is a good chance of substantial improvements in performance and scalability.

References

Akshay, J. S., Vinusha, T., Bianca, R. S., Krishna, C. S., & Radhika, G. (2024). Enhancing Credit Card Fraud Detection: A Comparative Analysis of Anomaly Detection Models. *2024*

IEEE International Conference on Computer Vision and Machine Intelligence (CVMI), 1–6. https://ieeexplore.ieee.org/abstract/document/10781986/

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *Ieee Access*, *11*, 137188–137203. https://ieeexplore.ieee.org/abstract/document/10341223/

Banu, S. R., Gongada, T. N., Santosh, K., Chowdhary, H., Sabareesh, R., & Muthuperumal, S. (2024). Financial fraud detection using hybrid convolutional and recurrent neural networks: An analysis of unstructured data in banking. *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, 1027–1031. https://ieeexplore.ieee.org/abstract/document/10543545/

Buslim, N., Rahmatullah, I. L., Setyawan, B. A., & Alamsyah, A. (2021). Comparing bitcoin's prediction model using GRU, RNN, and LSTM by hyperparameter optimization grid search and random search. *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 1–6. https://ieeexplore.ieee.org/abstract/document/9588947/

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, *99*, 106883. https://www.sciencedirect.com/science/article/pii/S1568494620308218

Lerma, L. (2022). *Comparative analysis of natural language processing and gradient boosting trees approaches for fraud detection*. https://www.politesi.polimi.it/handle/10589/208214

Marco, R., Aini, N., & Agastya, I. (2025). A Hybrid Approach CNN-LSTM Based on Attention Mechanism for Credit Card Fraud Detection. *International Journal of Intelligent Engineering & Systems*, *18*(3). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=2185310X&AN=183743764&h=EeOx%2FxdwQV8yhL4a6Fiop6bNQ2O7NV8NsT5gWR2wKWwzbZtGu%2BJ63jDUxVNQdc5e78nB1fQOcC9ij02Jsyv%2FMg%3D%3D&crl=c

Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10595068/

Oguntimehin, A., Nikeid, F., Atachin, A. J., Toyin, O., Ogundipe, A. T., Mebawondu, J. O., Babalola, G. O., Oluwatoki, T. G., & Sanya, O. A. (2024). Financial Fraud Detection Model using Recurrent Neural Network. *2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*, 1–5. https://ieeexplore.ieee.org/abstract/document/10927232/

Osegi, E. N., & Jumbo, E. F. (2021). Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory. *Machine Learning with Applications*, *6*, 100080. https://www.sciencedirect.com/science/article/pii/S2666827021000402

Prabhakar, K., Giridhar, M. S., Tatia, A., Joshi, T. M., Pal, S., & Aswal, U. S. (2023). Comparative Evaluation of Fraud Detection in Online Payments Using CNN-BiGRU-A Approach. *2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, 105–110. https://ieeexplore.ieee.org/abstract/document/10331745/

Rout, M. (2021). Analysis and comparison of credit card fraud detection using machine learning. In *Artificial Intelligence and Machine Learning in Business Management* (pp. 81–93). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003125129-5/analysis-comparison-credit-card-fraud-detection-using-machine-learning-saloni-minakhi-rout

Roy, S. S., Awad, A. I., Amare, L. A., Erkihun, M. T., & Anas, M. (2022). Multimodel phishing URL detection using LSTM, bidirectional LSTM, and GRU models. *Future Internet*, *14*(11), 340. https://www.mdpi.com/1999-5903/14/11/340

Sebastian, P. K., Deepa, K., Neelima, N., Paul, R., & Özer, T. (2024). A comparative analysis of deep neural network models in IoT-based smart systems for energy prediction and theft detection. *IET Renewable Power Generation*, *18*(3), 398–411. https://doi.org/10.1049/rpg2.12824

Shanbhog, N. R., Totad, K. S., Hanchinal, A. R., & Bidargaddi, A. P. (2024). Fraud Detection in Financial Transactions Using Deep Learning Approach: A Comparative Study. *2024 5th International Conference for Emerging Technology (INCET)*, 1–7. https://ieeexplore.ieee.org/abstract/document/10593486/

Sharma, D., & Lavavanshi, S. (2022). DETECTION OF CREDIT CARD FRAUD USING A NOVEL LSTM, GRU, AND ANN MODELS. *JOURNAL OF OPTOELECTRONICS LASER*, *41*(12).

Shiri, F. M., Perumal, T., Mustapha, N., & Mohamed, R. (2024). A Comprehensive Overview and Comparative Analysis on Deep Learning Models: CNN, RNN, LSTM, GRU. *Journal on Artificial Intelligence*, *6*(1), 301–360. https://doi.org/10.32604/jai.2024.054314

Singh, S., Kashyap, M., & Tantubay, N. (2025). *Comparative Analysis of ANN, RNN, and GRU for Credit Card Fraud Detection*. https://www.researchsquare.com/article/rs-5772503/latest

Suganthi, V., & Jebathangam, J. (2024). A Novel Approach for Credit Card Fraud Detection using Gated Recurrent Unit (GRU) Networks. *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 1716–1721.

https://ieeexplore.ieee.org/abstract/document/10714795/

Zhang, C. (2024). A credit card fraud detection system based on Credit-Attention-GRU network. *2024 8th International Conference on Electrical, Mechanical and Computer Engineering (ICEMCE)*, 1562–1569. https://ieeexplore.ieee.org/abstract/document/10862244/