Mesopotamian journal of Computer Science
Vol. 2024, **pp**. 204–213
DOI: https://doi.org/10.58496/MJCSC/2024/016; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

Credit Card Fraud Detection based on Deep Learning Models

El-Sayed M. El-Kenawy [1,2,3,*], Ahmed Mohamed Zaki [4], Wei Hong Lim [5], Abdelhameed Ibrahim [1], Marwa M. Eid [6], Ahmed M. Osman [7], Ahmed M. Elshewey [8]

[1] *School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain*

[2] *Jadara University Research Center, Jadara University, Jordan.*

[3] *Applied Science Research Center, Applied Science Private University, Amman, Jordan.*

[4] *Computer Science and Intelligent Systems Research Center, Blacksburg 24060, Virginia, USA*

[5] *Faculty of Engineering, Technology and Built Environment, UCSI University, Kuala Lumpur 56000, Malaysia.*

[6] *Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura 11152, Egypt.*

[7] *Department of Information Systems, Faculty of Computers and Information, Suez University, P.O.Box:43221, Suez, Egypt.*

[8] *Department of Computer Science, Faculty of Computers and Information, Suez University, P.O.Box:43221, Suez, Egypt.*

ARTICLE INFO

Article History

Received 14 Aug 2024
Revised: 14 Sep 2024
Accepted 13 Nov 2024
Published 05 Dec 2024

Keywords

fraud detection

Deep Learning

Recurrent Neural Network (RNN)

Credit card fraud detection.

ABSTRACT

Credit card fraud detection (FD) protects consumers and financial institutions by identifying suspicious or unauthorized transactions. To improve security and reduce false positives, fraud detection systems can analyze transaction data patterns in real time using advanced machine learning (ML) and deep learning (DL). This paper exploits DL models to detects transactional data which includes anomalies through Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU) to verify data and mitigate fraud. The models used precision, recall, F1-score, and AUC on a balanced shared 559856-record Kaggle repository dataset. The RNN model detected anomalies with 99.39% accuracy, 0.9939 F1-score, and excellent recall. RNN shows promise as a real-time anomaly detection method with high performance and low computational cost.

1. INTRODUCTION

The Internet widespread use across sectors has increased social and economic growth as science and technology advance. Network protocols' openness makes malicious software and cyberattacks easier to spread, which negatively impacts network security [1]. Threats disrupt online operations, cause significant economic losses, and threaten national security. There are a number of factors that contribute to the complexity of identifying and classifying anomaly-detection techniques. These include the types of anomalies, the systems that are being studied, and technical challenges such as processing costs. This level of complexity leads to the fragmentation of the literature, with many summaries failing to provide a comprehensive overview. A number of applications, including the detection of credit card fraud, the detection of cyber-security intrusions, and the detection of faults in safety-critical systems, can benefit from performing anomaly detection. The vulnerabilities enable unauthorized network users to threat the security of the network which is a vital concern as Internet and transactions increase. Threats compromise data integrity and disrupt services, causing financial and operational harm. Advanced detection and prevention systems are needed as attacks become more sophisticated. DL models are used to enhance FD accuracy and real-time responses in this study.

*Corresponding author. Email: skenawy@ieee.org

The paper develops and implements RNN, LSTM, and GRU DL models to detect credit card transaction irregularities. These models will be assessed using performance indicators to reduce false positives and enhance detection accuracy. The goal is to find the best real-time fraud detection model to improve network security and credit card fraud protection.
This paper exploits DL models to detect transactional data, which includes anomalies, through RNN, LSTM, and GRU to verify data and mitigate fraud. The models used precision, recall, F1-score, and AUC on a balanced shared 559856-record Kaggle repository dataset.
The paper has a structure as follows: Section 2 mentions related studies about anomaly detection methods. Section 3 outlines materials and methods, preprocessing, and proposed approach. Section 4 mentions the metrics used to compare RNN, LSTM, and GRU DL models. While the results and discussion in Section 5 continue, finally the conclusion highlights key findings and suggests anomaly detection methods.

2. RELATED WORK

Wawrowski et al. [2] developed a solution called the anomaly detection module, intended for network traffic safety enhancements by continuously monitoring traffic statistics as well as detecting anomalies. Public institutions essentially regarded the module as an extra element in any network security services. Whereas it aimed at identifying the optimal combination of models and also tuning those models in an even faster offline mode via a distinct selection approach.
Duan et al. [3] applied the multi-scale residual classifier (MSRC) to develop a technique intended for network traffic anomaly detection. The developed technique embraced network traffic partitioning into subsequences of different observation scales while collecting time-frequency information through wavelet transform technology and learning data distribution via a stacked automatic encoder. The results demonstrated how positively this technique impacts detection performance improvements, unlike traditional techniques and large observation and transformation scales, in addition to revealing potential diversity information in the original network traffic.
To do an analysis for network flow features as well as detecting anomalies in real-time, Liu and Wang [4] applied a convolutional neural network. For the purpose of managing network changes, they employed SDN in their analysis, supporting zero-configuration anomaly detection. The packet filter automatically managed abnormal traffic via certain mitigation techniques. The findings demonstrate the accuracy of their methodology, which helps network managers to begin setting up security measures and also improves the performance of edge clustering network security.
Yu et al. [5] applied the Gaussian mixture model to develop a statistical methodology intended for network traffic anomaly detection. This methodology applied the learned Gaussian distribution for the purpose of supporting learning normal communication process behavior as well as predicting data point attacks. It demonstrates high accuracy in certain scenarios; however, it may be inappropriate for intricate data points that are featured by various factors, and a single Gaussian mixture model can't make them accessible.
Fotiadou et al. [6] managed to detect threats and warnings in network logs obtained from pfSense, an open-source software as a firewall on FreeBSD, by developing new deep learning algorithms. Their study is intended for analyzing logs and offering an efficient solution to the traffic flow via several learned patterns. Furthermore, they applied Convolutional Neural Networks (CNNs) in addition to Long Short-Term Memory Networks (LSTMs) to come up with effective multi-class classifiers. The study examined many different quantitative experiments and drew comparisons to highly effective algorithms for the purpose of evaluating the performance of the developed scheme.
Patil et al. [7] applied principal component analysis (PCA) for the purpose of feature selection and dimensionality reduction, while also applying a bidirectional generative adversarial network (BiGAN) model for detecting network traffic anomalies. This model was assessed in comparison with current deep learning models using the KDDCUP-99 dataset. The study highlighted the crucial role of the feature reduction process in supporting the performance and speed of BiGAN and thereby enhancing its efficiency.
Song et al. [8] introduced a technique intended for network anomaly detection by formalizing normal and anomalous system behavior using the Hurst parameter. This technique employed the Three Sigma Rule along with the Hurst parameter for the purpose of detecting and avoiding a variety of network anomalies. For Hurst parameter examination, they came up with a rescaled range technique. They determined a set of necessary conditions for the practicality of their technique, including a minimum amount of time spent calculating, a short amount of time spent monitoring, self-training, and observing a variety of traffic types. They also introduced a system, Deep Packet Inspection (DPI), which integrated several algorithms intended for traffic analysis, protocol detection, and statistical load parameters. Based on a comparison between the system and SolarWinds Deep Packet Inspection, they managed to evaluate its capacity to detect and avoid network traffic anomalies. The results revealed how this system can detect non-standard factors along with dependencies, thereby upleveling intrusion detection efficacy.
Feng et al. [9] introduced an anomaly detection algorithm in their study, X-iForest, via X-means and iForest, which is intended for secondary filtering through X-means by clustering the standard Euclidean distance between the abnormal points and the normal cluster center. Their study examined a comparison between X-iForest and seven mainstream

unsupervised algorithms based on the AUC and anomaly detection rates. Many different experiments and outcomes revealed the effectiveness of X-iForest outperforming other algorithms and its significant role in supporting anomaly detection for large-scale network traffic data when applied.

Vigoya et al. [10] applied Logistic Regression, NB, RF, AdaBoost, and SVM when evaluating the DAD dataset, attempting to develop an approach for detecting traffic anomalies in IoT. Furthermore, they employed several techniques intended for data imbalance management, feature selection, and grid search optimization. The applied dataset supported effective detection rates and revealed tree-based models achieving a mean accuracy of 0.99.

Jain and Kaur [11] managed to detect concept drift in network traffic as well as network-based attacks by developing distributed ML algorithms. Random Forest, Logistic Regression, and Support Vector Machine functioned as level '0' learners in their study, in which sliding window-based K-means for concept drift were clustered and ensemble-based techniques were employed, particularly for traffic attack detection. They applied three datasets, including NSL-KDD and CIDDS-2017, along with a developed Testbed, in their experiments. In conclusion, the SVM-based blending model could achieve 93%, 98%, and 97% accuracy rates on the NSL-KDD, CIDDS-2017, and Testbed datasets, respectively.

A measurement intrusion detection system (MIDS) along with measurement data applied in a SCADA system has been developed by Mokhtari et al. [12], particularly for detecting abnormal activities even when hidden in the control layer by attackers. Furthermore, they developed an ML model that was supervised and intended for classifying normal and abnormal activities in an ICS. They managed to simulate power generation units and apply the attack dataset via a hardware-in-the-loop (HIL) testbed. They also employed a number of ML models for the dataset applied in their study, demonstrating their exceptional effectiveness in detecting anomalies, particularly stealthy attacks, and highlighting the random forest algorithm as the most effective classifier in detecting anomalies for measured data.

Ahmad et al. [13] applied mutual information (MI) to an IoT network via a deep neural network (DNN), attempting to develop an efficient anomaly detection technique. Their study examined a variety of deep-learning models, particularly DNN, Convolutional Neural Network, Recurrent Neural Network, and variants like Gated Recurrent Unit and Long Short-term Memory, via the IoT-Botnet 2020 dataset. The outcomes revealed the efficacy of the DNN-based NIDS model, outperforming other deep learning models with improved accuracy by 0.57-2.6% and a reduction of 0.23-7.98% in FAR. Applying MI along with only the most effective features could lead to lower performance while decreasing complexity. Overall, the detection accuracy achieved by DL-based models has improved by 0.99–3.45%.

Dang et al. [14] examined current advances in ML and DRL for credit card fraud detection. It corrects the CCF dataset imbalance using SMOTE and ADASYN resampling. The research evaluates ML and DRL algorithms on the balanced and unbalanced datasets using classification measures. When both resampling methods are used before the training/test split, ML models attain above 99% accuracy. Logistic regression performance reduces dramatically when resampling is confined to the training dataset. Unfortunately, the DRL model only achieves 34.8% accuracy.

A hybrid DL system by Mienye and Swart [15] uses Generative Adversarial Networks (GANs) and RNNs to identify fraud. GANs produce realistic synthetic fraudulent transactions to balance data and improve training datasets. The discriminator uses Simple RNN, LSTM, and GRUs to categorize synthetic and actual transactions as fraudulent or authentic. In experiments on the European credit card dataset, the GAN-GRU model outperformed standard approaches with great sensitivity and specificity. This study shows that GANs and deep learning can detect credit card fraud.

Table 1 shows the summary of related studies according to anomaly detection approaches.

TABLE I. THE SUMMARY OF RELATED STUDIES ACCORDING TO ANOMALY DETECTION APPROACHES.

Study	Methodology	Contributions
Wawrowski et al. [2]	Anomaly Detection Module with model selection and tuning for network traffic safety	Enhanced network traffic monitoring; provides an additional layer to existing network security, suitable for public institutions.
Duan et al. [3]	MSRC with wavelet transform and stacked autoencoder	Improved detection performance by capturing time-frequency data; reveals diversity in network traffic through multi-scale analysis.
Liu & Wang [4]	Convolutional Neural Network with SDN for zero-configuration anomaly detection	Effective real-time anomaly detection, enhances edge clustering performance and automates mitigation of abnormal traffic.
Yu et al. [5]	Gaussian Mixture Model for statistical anomaly detection	High accuracy in specific cases; limited effectiveness for complex, multifactorial data points due to single Gaussian model use.
Fotiadou et al. [6]	Deep learning using CNN and LSTM for threat detection in network logs from pfSense firewall	Effective multi-class classification with deep learning; demonstrates the capability to detect threats through log analysis.
Patil et al. [7]	PCA with BiGAN for anomaly detection, feature reduction for performance	Highlighted feature reduction's importance in enhancing BiGAN efficiency, achieving high performance on KDDCUP-99 dataset.

Song et al. [8]	Three Sigma Rule & Hurst Parameter for anomaly detection with DPI	Detects non-standard network anomalies with high efficacy, compared favorably with SolarWinds DPI.
Feng et al. [9]	X-iForest (X-means clustering + iForest) for large-scale anomaly detection	Outperformed other unsupervised methods in AUC and detection rate; suitable for large-scale traffic data.
Vigoya et al. [10]	Logistic Regression, NB, RF, AdaBoost, and SVM with techniques for imbalance and feature selection	Achieved 99% accuracy with tree-based models; effective approach for IoT traffic anomaly detection.
Jain & Kaur [11]	Distributed ML algorithms (RF, Logistic Regression, SVM) with concept drift handling using K-means clustering	SVM-based blending model achieved up to 98% accuracy; robust detection in diverse datasets, handles concept drift effectively.
Mokhtari et al. [12]	MIDS with ML models for SCADA system monitoring	Highly effective in detecting stealthy attacks in ICS, with Random Forest as the best classifier for anomaly detection.
Ahmad et al. [13]	MI with DNN, CNN, RNN, GRU, LSTM for IoT anomaly detection	DNN-based model outperformed others in accuracy and reduced FAR; applying MI with selected features enhances detection efficiency.
Dang et al. [14]	Machine Learning (ML) and Deep Reinforcement Learning (DRL) with SMOTE and ADASYN resampling for fraud detection	ML models achieved over 99% accuracy with resampling, but DRL model only attained 34.8% accuracy; logistic regression degraded with partial resampling.
Mienye & Swart [15]	GAN and RNN hybrid system with Simple RNN, LSTM, and GRU discriminators for fraud detection	GAN-GRU model achieved superior sensitivity and specificity, demonstrating GAN's effectiveness in data balancing and fraud detection.

3. MATERIALS AND METHODS

3.1. Dataset

This study uses a balanced credit card transaction shared dataset from Kaggle that available at https://www.kaggle.com/datasets/iabhishekofficial/creditcard-fraud-detection/ to detect fraud through anomalies. The transaction amount, time difference between transactions, credit card limit, geolocation data (longitude and latitude), and derived metrics (credit utilization ratio and binary anomaly indicator) are important. The dataset was preprocessed and balanced using oversampling to provide equal representation of normal and abnormal transactions for real-time fraud detection model training. Model performance is optimized by standardizing each feature. Table 2 displays features analysis of this shared dataset.

TABLE II. FEATURES ANALYSIS OF THE SHARED DATASET.

	transaction_dollar_amount	**Long**	**Lat**	**credit_card_limit**	**time_diff**	**time_anomaly**
count	559856	559856	559856	559856	559856	559856
mean	85.69007	-76.4022	40.95385	16144.17	225.4738	0.5
std	123.7232	19.01892	5.134072	8068.237	690.6771	0.5
min	0.01	-179.393	-68.0466	2000	0	0
25%	29.8	-80.201	40.53374	10000	1.6997	0
50%	58.46	-72.9986	42.46625	15000	4.991667	0.5
75%	100.3137	-72.0934	43.1772	20000	115.45	1
max	999.97	179.9175	78.91433	55000	60131.85	1

Figure 1 displays the heatmap of the shared anomaly dataset.

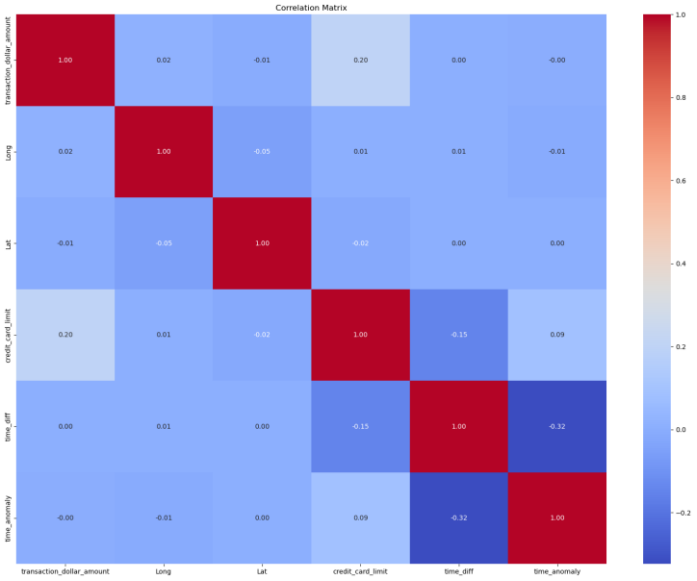


Fig 1. Heatmap of the shared anomaly dataset.

Figure 2 displays the shared anomaly dataset attributes to histogram plot.

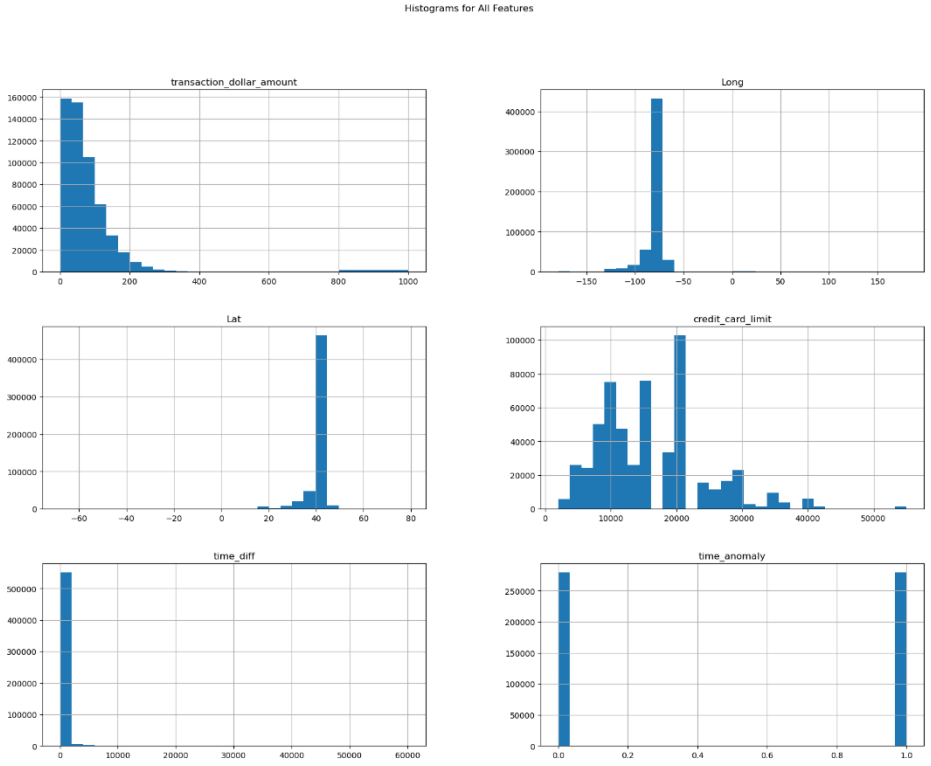


Fig 2. Histogram plot of the anomaly shared dataset according to all features.

Figure 3 displays the distributions of target according to an anomaly shared dataset.

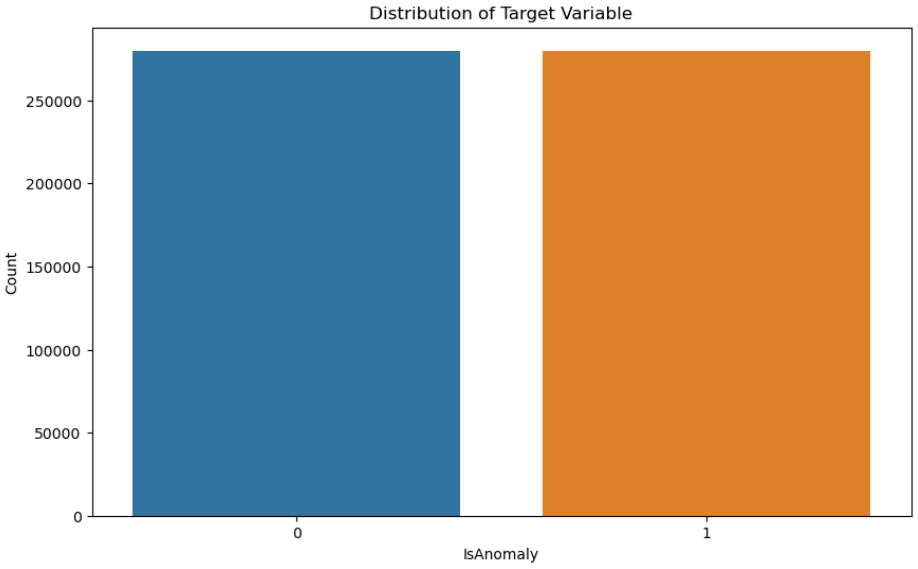


Fig. 4. The distributions of target according to anomaly shared dataset.

3.2 The proposed framework

The credit card transaction anomaly detection model uses deep learning and three types of RNN, LSTM, and GRU. Each model may discover transaction pattern abnormalities by processing sequential data and extracting temporal dependencies. The models used precision, recall, F1-score, and AUC on a balanced shared 559856-record Kaggle repository dataset. RNN shows promise as a real-time anomaly detection method with high performance and low computational cost. Figure 5 displays the proposed model of anomaly detection.

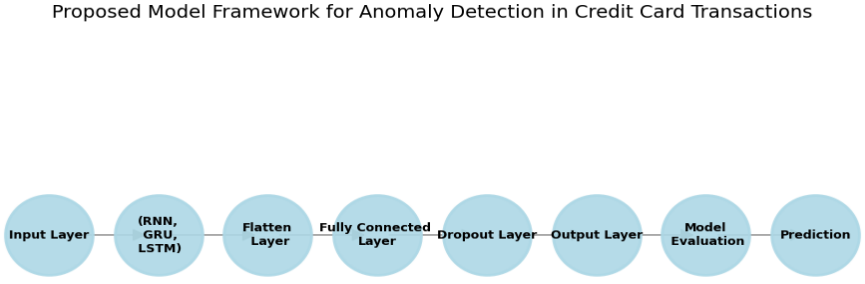


Fig 5. The proposed framework of anomaly detection.

4. RESULTS AND DISCUSSION

This paper exploits DL models to detects transactional data which includes anomalies through RNN, LSTM, and GRU to verify data and mitigate fraud.. RNN was the top fraud detection model with 99.39% accuracy, good recall, and 99.98% AUC. LSTM and GRU had good accuracy (98.61% and 98.75%) but less recall and precision than RNN. All algorithms detected fraudulent transactions with 100% AUC scores. The findings suggest RNN for high-sensitivity applications and LSTM and GRU for computational efficiency. To increase fraud detection, future research may combine, optimize, and test these models in real-world settings. Table 3 displays the performance evaluation of the proposed approach for anomaly detection.

TABLE III. THE PERFORMANCE EVALUATION OF ANOMALY DETECTION.

Model	Accuracy	Precision	Recall	F1 Score	ROC-AUC

RNN	**0.9939**	**0.9879**	**1.0000**	**0.9939**	**0.9998**
LSTM	0.9861	0.9745	0.9983	0.9863	0.9989
GRU	0.9875	0.9757	0.9998	0.9876	0.9992

The models used precision, recall, F1-score, and AUC [16-22] which calculated through the following equations:

$$Accuracy = \frac{\boldsymbol{TP + TN}}{\boldsymbol{TP + FP + FN + TN}} \tag{1}$$

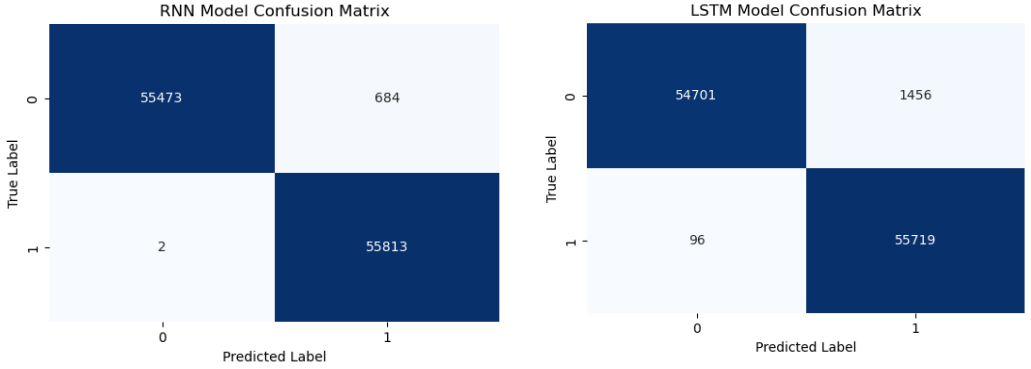
$$Specificity = \frac{\boldsymbol{TN}}{\boldsymbol{TN + FP}} \tag{2}$$

$$Sensetivity = \frac{\boldsymbol{TP}}{\boldsymbol{TP + FN}} \tag{3}$$

$$\boldsymbol{AUC = 1/2\left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP}\right)} \tag{4}$$

$$\boldsymbol{F - score = \frac{2 \times Recall \times Precision}{Recall + Precision}} \tag{5}$$

Figure 6 displays the confusion matrices of anomaly detection DL models.



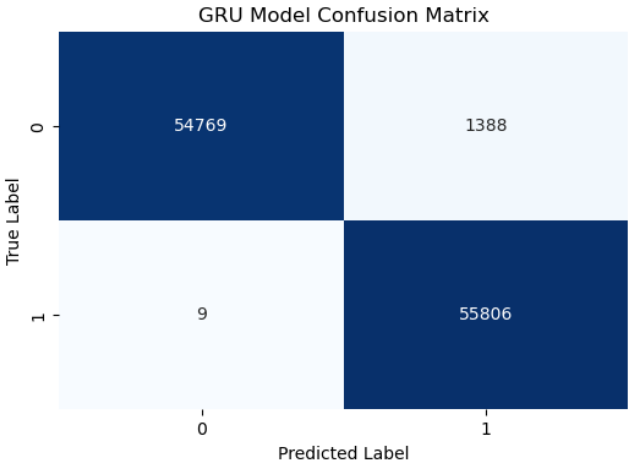


Fig 6. confusion matrices of anomaly detection DL models.

Figure 7 displays the training and validation accuracy of anomaly detection DL models.

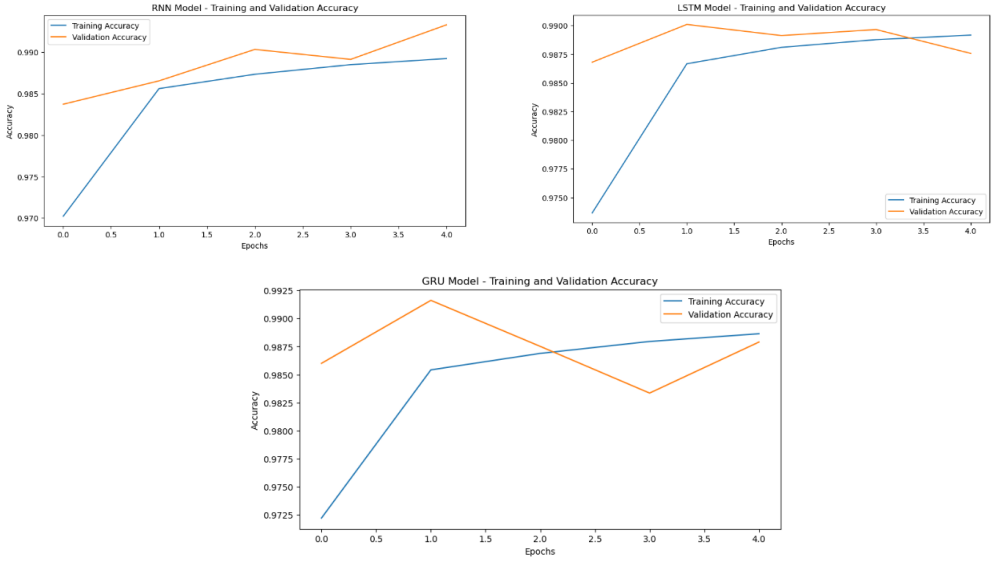


Fig. 7. Training and validation accuracy of the anomaly detection DL models.

5. CONCLUSIONS AND FUTURE WORK

This paper exploits DL models to detect transactional data which includes anomalies through Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Gated Recurrent Unit (GRU) to verify data and mitigate fraud. The models used precision, recall, F1-score, and AUC on a balanced shared 559856-record Kaggle repository dataset. The RNN model detected anomalies with 99.39% accuracy, 0.9939 F1-score, and excellent recall. RNN shows promise as a real-time anomaly detection method with high performance and low computational cost. Ensemble methods that integrate RNN, LSTM, and GRU for greater accuracy is one of the future work in fraud detection models. Other future study involves applying sophisticated hyperparameter tuning techniques to boost performance and testing models on real-world streaming data to determine their practical application. The use of explainability techniques such as SHAP or LIME might further improve the interpretability of models for financial institutions. Furthermore, the combination of transactional data with data from other sources, such as user behavior or geolocation, could potentially raise the robustness of fraud detection.

Conflicts Of Interest

The author's disclosure statement confirms the absence of any conflicts of interest.

Funding

No financial contributions or endorsements from institutions or sponsors are mentioned in the author's paper.

Acknowledgment

The author acknowledges the support and resources provided by the institution in facilitating the execution of this study.

References

[1] M. Jain, et al., "A K-Means clustering and SVM based hybrid concept drift detection technique for network anomaly detection," Expert Systems With Applications, vol. 193, p. 116510, Jan. 2022. DOI: 10.1016/j.eswa.2022.116510.

[2] Ł. Wawrowski, et al., "Anomaly Detection Module for Network Traffic Monitoring in Public Institutions," Sensors, vol. 23, no. 6, p. 2974, Mar. 2023. DOI: 10.3390/s23062974.

[3] T. Kavitha, G. Amirthayogam, J. J. Hephzipah, R. Suganthi, V. A. Kumar G, and T. Chelladurai , Trans., “Healthcare Analysis Based on Diabetes Prediction Using a Cuckoo-Based Deep Convolutional Long-Term Memory Algorithm”, Babylonian Journal of Artificial Intelligence, vol. 2024, pp. 64–72, Jun. 2024, doi: 10.58496/BJAI/2024/009.

[4] A. Zaharaddeen and N. Mukhtar , Trans., “An Author-Centric Framework Error Minimization in Scholarly Recommender System (Acfemsr)”, BJIoT, vol. 2024, pp. 161–168, Dec. 2024, doi: 10.58496/BJIoT/2024/018.

[5] B. Yu, et al., "A Network Traffic Anomaly Detection Method Based on Gaussian Mixture Model," Electronics, vol. 12, no. 6, p. 1397, Mar. 2023. DOI: 10.3390/electronics12061397.

[6] K. Fotiadou, et al., "Network Traffic Anomaly Detection via Deep Learning," Information, vol. 12, no. 5, p. 215, May 2021. DOI: 10.3390/info12050215.

[7] H. M. S. SALEEH, H. Marouane, and A. Fakhfakh , Trans., “A Novel Deep Learning Approach for Detecting Types of Attacks in the NSL-KDD Dataset”, BJN, vol. 2024, pp. 171–181, Sep. 2024, doi: 10.58496/BJN/2024/017.

[8] W. Song, et al., "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," Sensors, vol. 20, no. 6, p. 1637, Mar. 2020. DOI: 10.3390/s20061637.

[9] Y. Feng, et al., "An improved X-means and isolation forest based methodology for network traffic anomaly detection," PLoS ONE, vol. 17, no. 1, p. e0263423, Jan. 2022. DOI: 10.1371/journal.pone.0263423.

[10] L. Vigoya, et al., "IoT Dataset Validation Using Machine Learning Techniques for Traffic Anomaly Detection," Electronics, vol. 10, no. 22, p. 2857, Nov. 2021. DOI: 10.3390/electronics10222857.

[11] M. Jain and G. Kaur, "Distributed anomaly detection using concept drift detection based hybrid ensemble techniques in streamed network data," Cluster Computing, vol. 24, no. 3, pp. 2099–2114, Feb. 2021. DOI: 10.1007/s10586-021-03249-9.

[12] S. Mokhtari, et al., "A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data," Electronics, vol. 10, no. 4, p. 407, Feb. 2021. DOI: 10.3390/electronics10040407.

[13] M. Sheela, G. Amirthayogam, J. J. Hephzipah, R. Suganthi, T. Karthikeyan, and M. Gopianand , Trans., “Advanced Brain Tumor Classification Using DEEPBELEIF-CNN Method ”, Babylonian Journal of Machine Learning, vol. 2024, pp. 89–101, Jun. 2024, doi: 10.58496/BJML/2024/009.

[14] T. K. Dang, et al., "Machine Learning Based on Resampling Approaches and Deep Reinforcement Learning for Credit Card Fraud Detection Systems," Applied Sciences, vol. 11, no. 21, p. 10004, Oct. 2021. DOI: 10.3390/app112110004.

[15] I. D. Mienye and T. G. Swart, "A Hybrid Deep Learning Approach with Generative Adversarial Network for Credit Card Fraud Detection," Technologies, vol. 12, no. 10, p. 186, Oct. 2024. DOI: 10.3390/technologies12100186.

[16] E. Srividhya, J. P, V. Anusuya, K. J. Deepthi, P. Gopalsamy, and S. Gopalakrishnan, “Deep Learning-Driven Disease Prediction System in Cloud Environments using a Big Data Approach”, EDRAAK, vol. 2024, pp. 8–17, Jan. 2024, doi: 10.70470/EDRAAK/2024/002.

[17] N. S. Alfaiz and S. M. Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning," Electronics, vol. 11, no. 4, p. 662, Feb. 2022. DOI: 10.3390/electronics11040662.

[18] G. Zioviris, et al., "Credit card fraud detection using a deep learning multistage model," The Journal of Supercomputing, vol. 78, no. 12, pp. 14571–14596, Apr. 2022. DOI: 10.1007/s11227-022-04465-9.

[19] W. H. Hanoon and A. S. Ibrahim , Trans., “Fuzzy Semi and Fuzzy Strongly Semi Two-Absorbing Second Sub-modules ”, Babylonian Journal of Mathematics, vol. 2024, pp. 95–101, Nov. 2024, doi: 10.58496/BJM/2024/012.

[20] E. Ileberi, et al., "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, no. 1, Feb. 2022. DOI: 10.1186/s40537-022-00573-8.
[21] I. Benchaji, et al., "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," Journal of Big Data, vol. 8, no. 1, Dec. 2021. DOI: 10.1186/s40537-021-00541-8.
[22] A. R. Khalid, et al., "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," Big Data and Cognitive Computing, vol. 8, no. 1, p. 6, Jan. 2024. DOI: 10.3390/bdcc8010006.