iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71450

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Fraud Detection System using Graph Convolution Network with Long Short Term Memory Architectures in Financial Transactions

Aravinda Kumar Appachikumar
Independent Researcher

Abstract: ***Online financial fraud leads to billions of dollars losses and acute challenges across the world due to pervasive threat on digital adoption in banking, financial and Insurance (BFSI) sectors. It outpaces the establishment of robust multilayered security system. Financial fraud is committed over cyberspace by cybercriminals using hacking and social engineering approaches to bypass the security. Traditionally fraud detection methods have been employed to the multilayer security system using machine learning and deep learning methods to detect and combat frauds in the financial transactions. However those models face numerous challenges in terms of poor model performance and inaccurate results due to evolving attack strategies and data imbalances (Training of the model with less fraudulent transaction instances). In order to mitigate those challenges, a real time financial transaction processing model has to be designed using deep learning architecture. Thus a new graph convolution network with long short term memory model has been designed with Synthetic Minority Over-sampling Technique (SMOTE). Initially data is preprocessed with missing value imputation using K-NN approach and normalization using min – max normalization. Preprocessed dataset is applied to Synthetic Minority Over-sampling Technique is to eliminate the class imbalance issues occurred in the dataset. It generates the synthetic instances of the fraudulent transaction to minority classes which balances the dataset. Long Short Term Model Network is applied to capture long term dependency of the temporal features of the balanced dataset using gating mechanism along cell state updates and hidden states. Especially dense layer is interfaced to transform the LSTM output into feature vector. Graph Convolution Network transforms the dataset into graph structured data. Graph structured data represented with node and its edge. In this transaction of the dataset represents the node and transactions relations represent the edge which is obtained using Pearson correlation coefficients. Initially input layer of the graph convolution Network receives the transaction graph and its transaction specific attributes. Further graph convolution layer aggregates information of the neighboring transactions using degree normalized message passing to ensure balanced influence among nodes. The output layer generates updated node embedding which includes features of transaction and aggregated neighbor information. The temporal feature embedding from LSTM model and Relational features embedding from GNN were concentrated to form a unified feature vector. Finally dense layer with activation function and softmax function classifies the transactions with class labels (Fraudulent /Non-Fraudulent) effectively. Experimental analysis of the model is performed using Financial Fraud Detection Dataset on Google colab environment incorporating tensorflow to obtain GPU capabilities. On performance analysis, proposed model attains 96.4% accuracy which found to be better compared to conventional fraud detection approaches.***

Keywords: Financial Fraud Detection, Graph Convolution Network, Long Short Term Memory, Deep Learning, Cyber Attacks

I. INTRODUCTION

Increase in adoption to the digital payment methods has increased online financial fraud. Online Financial Fraud[1] includes wide variety of the malicious activities to loot money in the online financial]transactions which poses great challenges to financial institutions and consumers. Especially financial institutions establish robust multilayered security system[2] to prevent financial frauds still cybercriminals use hacking and social engineering approaches to evade t]he security protocols to create a huge economic loss for financial institutions[3]. Traditionally many fraud detection methods have employed using machine learning such as support vector machine[4], Naïve Bayes{5], Random Forest[6] and deep learning approaches such as convolution neural network and Recurrent Neural Network to determine and combat financial frauds in the transactions. However those models exhibit numerous challenges such as low model performance and inaccurate results on presence of evolving attack strategies and data imbalances.

To mitigate those challenges, a real time financial transaction processing model using graph convolution network with long short term memory model has designed along Synthetic Minority Over-sampling Technique (SMOTE)[15]. Initially dataset is preprocessed with missing value imputation and normalization approach along SMOTE process. Preprocessed dataset is applied to Long Short Term Model Network[7] to capture long term dependency of the temporal features and produces temporal feature embedding. Graph Convolution Network produces relational features embedding which includes features of transaction and aggregated neighbor information. The temporal feature embedding and Relational features embedding were concentrated to form a unified feature vector. Finally dense layer with activation function and softmax function classifies the transactions with class labels (Fraudulent /Non-Fraudulent) effectively.

Rest of the article is segmented into section as follows section 2 defines review of literatures related to the fraud detection approaches from machine and deep learning architectures. Section 3 defines a design of financial transaction processing model using graph convolution network with long short term memory model with preprocessing process with missing value imputation, normalization and dataset balancing. Section 4 mentions experimental and performance results of the proposed model against conventional approaches on cross fold validation of the financial fraud detection dataset. Finally section 5 concludes the article with major findings and suggestions.

II. RELATED WORK

In this section, review of literatures related to the financial fraud detection approaches from machine and deep learning architectures has been analyzed on basis of its performance and architecture capabilities is as follows

A. Convolution Neural Network for online Transaction fraud detection

In this literature, convolution neural network is employed to detect the online transaction frauds. Model composed of multiple convolution layers to extract low level and high level features from financial transactions and establishes feature map with respect to its associations. Those feature maps is processed in dense layer through activation function and softmax function to predict the attack occurrence in the transactions. Experimental analysis and performance analysis proves that model produces 92.1% detection accuracy but it leads to class imbalance issues[8].

B. Recurrent Neural Network for online Transaction fraud detection

In this literature, recurrent neural network is employed to detect the online transaction frauds. Model composed of input layer, hidden layers and output layer with feedback loop. Input layer receives input and creates as input state and those input sequence projected to hidden layer to extract features or patterns from sequences. Those patterns are processed in hidden layer through activation function to predict attack occurrence in the transactions. Further those predicted information represent cell state and it is reiterated for next sequences of input. Experimental analysis and performance analysis proves that model produces 93.1% detection accuracy but it leads to high complexity[9].

III. PROPOSED MODEL

In this section, design of financial transaction processing model using graph convolution network with long short term memory model with preprocessing process with missing value imputation, normalization and dataset balancing is performed.

A. Data Preprocessing

Data Preprocessing is initial phase of the model which transforms dataset to quality dataset with several processing methods to eliminate the gaps in dataset as follow

1) Missing Value Imputation- KNN Approach

Missing value Imputation is performed using K nearest Neighbor approach which imputes the value to the absence of information in the data field of the attribute in the financial transaction dataset[10]. Mean is computed on averaging of the known data points within a specific attribute and utilize the computed mean to determine the distance of data points through Euclidean distance computation. Process is represented in the equation 1 as follows

$$X_{\text{impute}} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

Where X_{impute} signifies computed value to impute in the attribute contain absence of information in the data field. X_i is value of the data point at I and N represent the no of data point without absence of information. Select K value randomly to extract top k data point. The value near to the mean value is selected as optimal missing value and it is imputed to the missing field of the specified attribute. Figure 1 represents architecture of the proposed model.

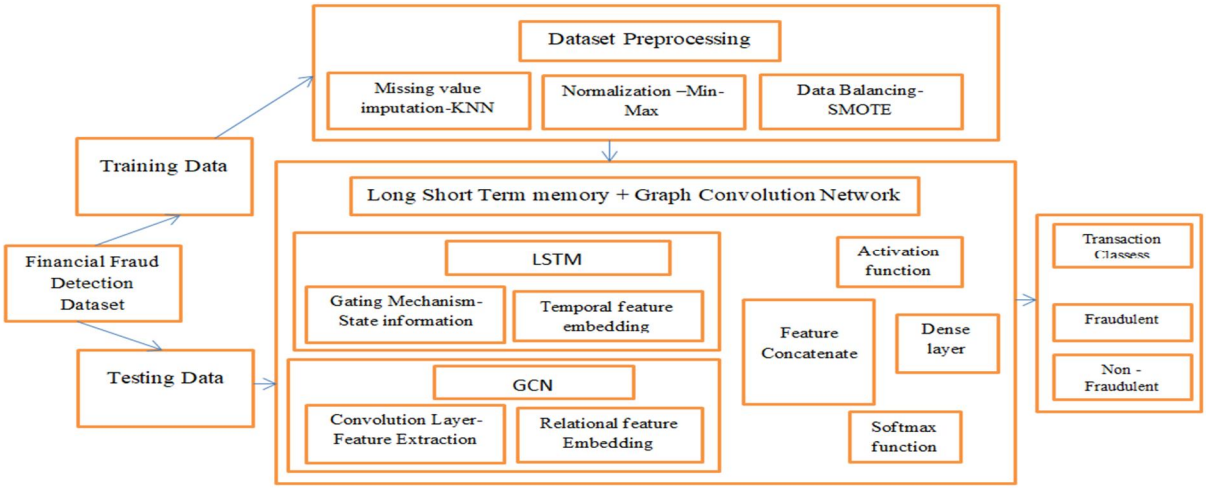


Figure 1: Proposed deep learning Architecture of the Financial Fraud Detection system

2) Normalization - Min- Max Method

Nonstandard format of dataset is normalized or scaled using the min_max normalization method. Min_Max focuses on numerical attributes to transforms it into uniform and comparable scale. It alters the data range of the attributes into specified data range as 0 and 1. Scaling process is used to determine attribute range[11].

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

In this attribute with minimum value is transformed with zero, attribute with highest value is transformed into 1 and finally attribute data value between maximum and minimum is transformed into 0.5.

3) Synthetic Minority Over-sampling Technique

Synthetic Minority Over-sampling Technique is applied to preprocessed data to eliminate the class imbalance issues occurred in the dataset. It occurs due to significant disparity in the number of legitimate transaction compared to fraudulent transactions. It generates the synthetic data points to the fraudulent transaction which is considered as minority classes in the dataset in a way it balances the dataset. Further it retains the underlying patterns and relationships within data. It accomplishes the balanced dataset by creating synthetic instances which occurs between minority class instance and its closest neighbor in the feature space. It yields equitable distribution between the fraudulent transactions and non- fraudulent transactions.

B. Graph Convolution Network integrated Long Short Term Memory

Integrated Graph Convolution Network with Long Short Term Model Network leverages the benefit of feature extraction and detection process to balanced dataset. Proposed model strengthens discriminative capabilities of the features to enhance the performance of the model to detection task. Component of the model is as follows

1) Graph Representation of the Financial Transaction Network

The categorical dataset is transformed into graph structured data. Graph structured data represented with vertex and its edge. In this transaction represents the vertex and transactions relations represent the edge which is obtained using Pearson correlation coefficients[12]. It quantifies linear relationship among values of the each data point of the transactions. Pearson correlation coefficients $p_{i,j}$ among transactions i and j is represented as

$$P_{i,j} = \frac{\sum_{t=1}^{n}(r_{i,t} - r_i)(r_{j,t} - r_j)}{\sqrt{\sum_{t=1}^{n}(r_{i,t} - r_i)^2}\sqrt{\sum_{t=1}^{n}(r_{j,t} - r_j)^2}}$$

Where relationship between the transactions is established to Pearson correlation coefficients $p_{i,j}$ greater than 0.7

2) Long Short Term Model Network

Long Short Term Model Network is applied to capture long term dependency of the temporal features of the balanced dataset using gating mechanism along cell state updates and hidden states. Initially it processes the input sequence over optimized time windows. Further multiple LSTM layers were stacked to learn temporal patterns utilizing forget gate. Especially dense layer is interfaced to transform the LSTM output into feature vector. Table 1 represents the hyperparameter setting of the Long Short Term Model Network for optimal sequence length.

Table 1: Hyperparameter setting of LSTM Network

Hyperparameter	Value
Learning rate	10^{-5}
Batch Size	11
Epoch	10
Loss function	Mean Square Error
Optimizer	Adam

Learning rate, batch size and epoch were employed for early stopping to prevent overfitting. Optimizer was used for efficient training and mean square error as loss function

3) Graph Convolution Network

Graph convolution network is employed to capture relational dependencies among the financial transactions in form of the transforming it into graph. Architecture of the graph convolution network with hyperparameter of the layers is as follows

- Input layer: Input layer of the graph convolution Network receives the financial transaction in form of graph and its transaction specific attributes.
- Convolution Layer : Graph convolution layer uses kernel function generate low dimension features and those features of the each transactions is aggregated using degree normalized message passing to ensure balanced influence among transactions (vertices).
- Activation function : It transform non-linear feature to linear feature
- Dropout layer : It employed for regularizes the features using L2 regularization and It is used to prevent overfitting
- Output layer : It produces the relational embedding which is composed of features of the financial transaction and aggregation of the neighbor information to the financial transaction

Table 2 represents the hyperparameter setting of the Graph Convolution Network for optimal sequence length. Learning rate, batch size and epoch were employed for early stopping to prevent overfitting. Optimizer was used for efficient training and mean square error as loss function

Table 2: Hyperparameter setting of Graph Convolution Network

Hyperparameter	Value
Learning rate	10^{-6}
Batch Size	15
Epoch	20
Loss function	Cross entropy
Activation function	ReLu
Dropout rate	L2 regularization

4) Dense Layer

The temporal feature embedding from LSTM model in form of patterns and Relational features embedding from GNN in form of relation were concentrated to form a unified feature vector. Further complex relations among the features is learned[14]. Finally dense layer with activation function linearizes the complex relations and softmax function with classifier function classifies the transactions with class labels (Fraudulent /Non-Fraudulent) effectively. Algorithm steps of the integrated graph convolution network with long short term memory is as follows

Algorithm: GCN+LSTM
Input: Financial Fraud Detection Dataset – Financial Transactions
Output: Classes - Fraudulent and Non-Fraudulent
Process()
Preprocess_Dataset()
Missing Value Imputation _KNN(Dataset)
Normalization _Min-Max(Dataset)
Dataset Balancing _SMOTE (Dataset)
GCN_LTSM()
LTSM ()
Gating (Preprocessed Dataset)
Cell state = patterns of the sequence
Feature Vector = Long Term Dependency
Temporal Embedding ()
GCN ()
Graph Transformation (Pre-processed dataset)
Graph form of transactions = (V, E)
Input Layer ()
Gathers Transactions and transaction specific attributes as vertices and Edge
Convolution Layer_ Kernel Function (Transaction and its attributes)
Low level features of the transaction
Feature map (Low level feature aggregation of each transactions)
Activation function _ReLu (feature map)
Linear feature map
Dropout layer_L2 Regularization (linear feature)
Regularized feature map
Output layer ()
Relational Embedding
Dense Layer ()
Transformation of Temporal Embedding into feature vector
Transformation of Relational Embedding into feature vector
Feature Concatenation (Temporal Feature Vector + Relational Feature Vector)
Unified Aggregated feature vector
Softmax function _Classifier (feature Vector)
Class= {Fraudulent & Non-Fraudulent}

IV. EXPERIMENTAL ANALYSIS

Experimental analysis of the proposed model is conducted in Google colab which high performance online python environment with tensor flow functionalities and multiple libraries such as NumPy and Pandas for data manipulation, scikit learn for baseline models and Matplotlib for data visualization. Panda's libraries for data processing using financial fraud detection dataset extracted from kaggle repository[15]. Dataset is portioned as 60 percent employed for model training and 40 percent for model testing. Grid search was conducted to identify the optimal hyperparameter for model training to LSTM and GCN.

A. Performance analysis

Performance analysis of the model is performed using test data through confusion matrix. Confusion matrix generates the values to the true positive, false negative, true negative and false positive parameters. Those parameter values of the matrix demonstrates strong performance of the LSTM +GCN model in classifying the financial transaction on integrating the time series data(processed by LSTM network) and relational data(processed GCN network). Model achieved enhanced detection accuracy of 96.4 percent. Further precision analysis, recall analysis and accuracy analysis were performed as follows

1) Precision Analysis

Precision analysis is performed to determine no of the aggregated feature correctly classified into financial transaction classes among the total aggregated features. Precision analysis represented on parameter of confusion matrix is as follows

$$\text{Precision} = \frac{TP}{TP+FP}$$

Figure 2 represents precision analysis of the model against conventional approaches. It represents model ability towards adaption to evolving attack strategies on continuously updating the training model with new data.

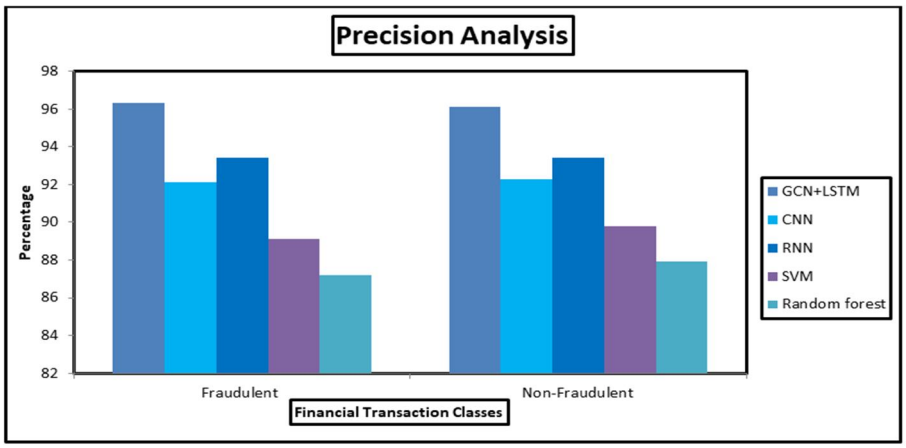


Figure 2: Precision Analysis

2) Recall Analysis

Recall analysis is performed to determine no of the aggregated feature incorrectly classified into financial transaction classes among the total aggregated features. Recall analysis represented on parameter of confusion matrix is as follows

$$\text{Recall} = \frac{TN}{TP+FP}$$

Figure 3 represents Recall analysis of the model against conventional approaches. It represents model ability towards adaption to evolving attack strategies on continuously updating the training model with new data.

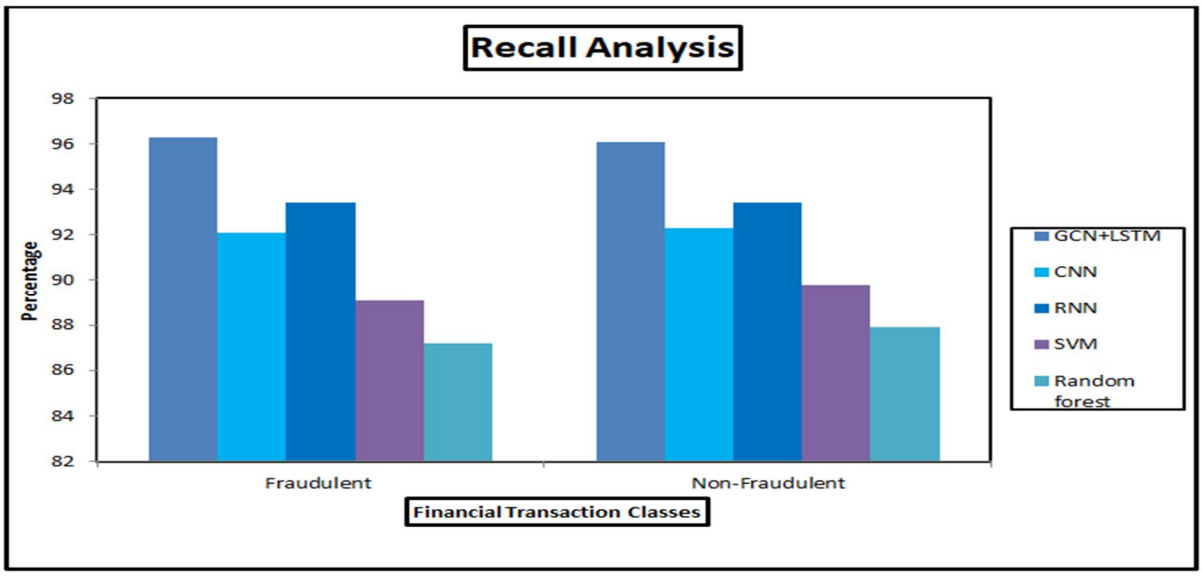


Figure 3: Recall Analysis

3) F-Measure Analysis

F-measure analysis is performed as aggregation of recall and precision towards detecting aggregated feature among total aggregated features into financial transaction classes. F-Measure analysis represented on parameter of confusion matrix is as follows

$$\text{F-Measure} = \frac{TP+TN}{TN+FN+TP+FP}$$

Figure 4 represents F-Measure analysis of the model against conventional approaches. It represents model ability towards adaption to evolving attack strategies on continuously updating the training model with new data.

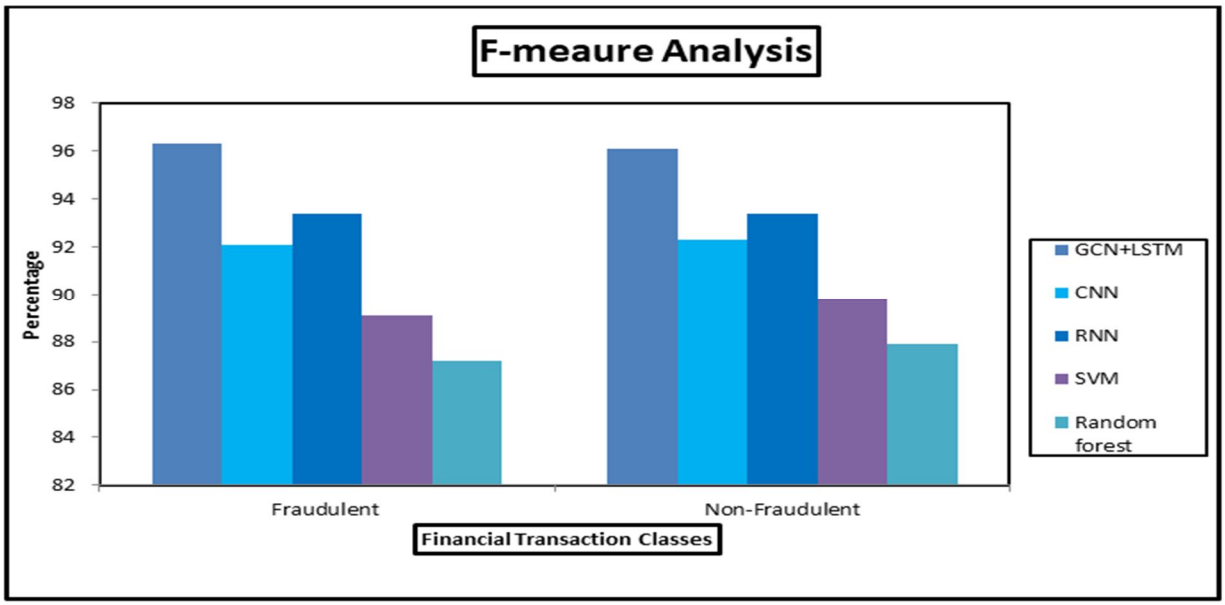


Figure 4: F-Measure analysis

Finally performance of GCN+LSTM architecture performs better with detection accuracy 96.4% on compared to conventional approaches. Table 2 mentions the performance evaluation of the deep learning architectures in financial fraud detection

Table 2: Performance Evaluation of Deep learning architecture in financial fraud detection

Technique	Classes	Precision	Recall	F-Measure
GCN+LSTM – Deep learning	Fraudulent	96.1	94.2	96.4
	Non- Fraudulent	96.4	94.5	96.2
CNN- Deep learning	Fraudulent	93.4	91.7	93.7
	Non- Fraudulent	93.6	91.8	93.3
RNN – Deep learning	Fraudulent	91.6	90.1	91.6
	Non- Fraudulent	92.3	90.5	91.3
SVM-machine learning	Fraudulent	89.1	87.2	89.6
	Non- Fraudulent	89.8	87.3	89.2
Random Forest-machine learning	Fraudulent	87.2	86.3	87.8
	Non- Fraudulent	87.6	86.4	87.2

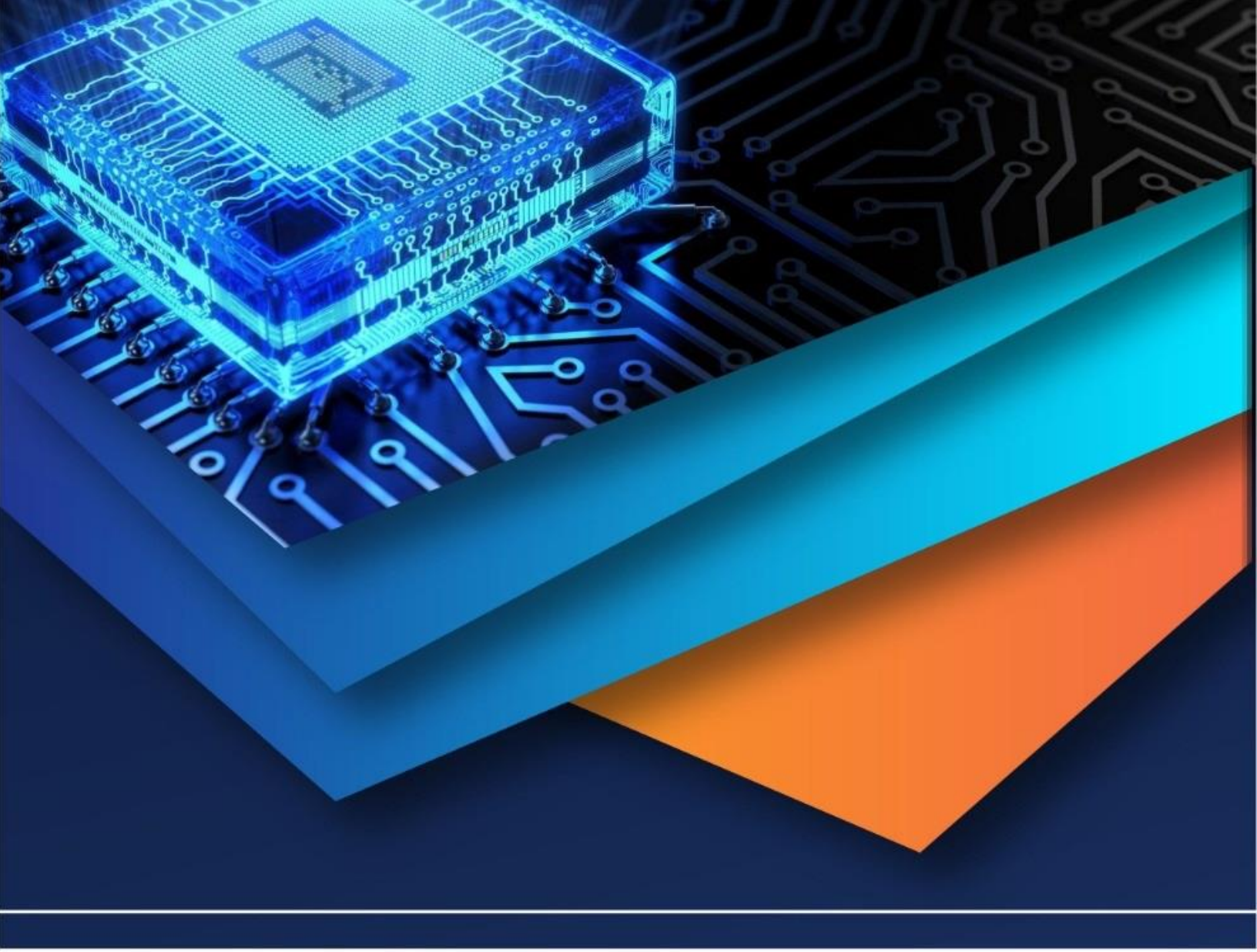
V. CONCLUSION

In this paper, a graph convolution network with long short term memory model has been designed and implemented along group of preprocessing such as Synthetic Minority Over-sampling Technique (SMOTE) for dataset balancing, K-NN approach for missing value imputation and Min-max approach for normalization. Graph convolution network extracts relational features on processing relational data in different layers of the network and long short term memory model extracts temporal features on processing time series data in different layers of the network. Dense layer were concatenated feature vector in unified form and classified those feature vector into fraudulent and non-fraudulent financial transaction.

Experimental analysis defines efficiency of the configuration towards processing the financial fraud detection dataset and Performance analysis of model reports 96.4 % accuracy which is found to be better compared to accuracy value of the traditional architectures in financial fraud detection. As a future work, accuracy of the fraud detection can be enhanced on employing federated architectures.

REFERENCES

[1] K. G. Al-Hashedi and P. Magalingam, ‘‘Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019,’’ IEEE Access, vol. 40, 2021
[2] Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, ‘‘Credit card fraud detection in the era of disruptive technologies: A systematic review,’’ J. King Saud Univ. Comput. Inf. Sci., vol. 35, no. 1, pp. 145–174, Jan. 2023
[3] J. . Forough and S. Momtazi, ‘‘Ensemble of deep sequential models for credit card fraud detection,’’ Appl. Soft Comput., vol. 99, Feb. 2021,
[4] G. Douzas and F. Bacao, ‘‘Effective data generation for imbalanced learning using conditional generative adversarial networks,’’ Expert Syst. Appl., vol. 91, pp. 464–471, Jan. 2018
[5] S. Bagga, A. Goyal, N. Gupta, and A. Goyal, ‘‘Credit card fraud detection using pipeling and ensemble learning,’’ Proc. Comput. Sci., vol. 173, pp. 104–112, Jan. 2020
[6] H. Fanai and H. Abbasimehr, ‘‘A novel combined approach based on deep autoencoder and deep classifiers for credit card fraud detection,’’ Expert Syst. Appl., vol. 217, May 2023,
[7] Ienchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, ‘‘Enhanced credit card fraud detection based on attention mechanism and LSTM deep model,’’ J. Big Data, vol. 8, no. 1, pp. 1–21, Dec. 2021.
[8] S. Nami and M. Shajari, ‘‘Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors,’’ Expert Syst. Appl., vol. 110, pp. 381–392, Nov. 2018.
[9] L. Zheng, G. Liu, C. Yan, C. Jiang, M. Zhou, and M. Li, ‘‘Improved TrAdaBoost and its application to transaction fraud detection,’’ IEEE Trans. Computat. Social Syst., vol. 7, no. 5, pp. 1304–1316, Oct. 2020.
[10] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, ‘‘A neural network ensemble with feature engineering for improved credit card fraud detection,’’ IEEE Access, vol. 10, pp. 16400–16407, 2022.
[11] Y. Chen, N. Ashizawa, C. K. Yeo, N. Yanai, and S. Yean, ‘‘Multi-scale selforganizing map assisted deep autoencoding Gaussian mixture model for unsupervised intrusion detection,’’ Knowl.-Based Syst., vol. 224, Jul. 2021,
[12] S. V. Suryanarayana, G. N. Balaji, and G. V. Rao, ‘‘Machine learning approaches for credit card fraud detection,’’ Int. J. Eng. Technol., vol. 7, no. 2, p. 917, Jun. 2018.
[13] Y. Alghofaili, A. Albattah, and M. A. Rassam, ‘‘A financial fraud detection model based on LSTM deep learning technique,’’ J. Appl. Secur. Res., vol. 15, no. 4, pp. 498–516, Oct. 2020
[14] S. A. Ebiaredoh-Mienye, E. Esenogho, and T. G. Swart, ‘‘Artificial neural network technique for improving prediction of credit card default: A stacked sparse autoencoder approach,’’ Int. J. Electr. Comput. Eng. (IJECE), vol. 11, no. 5, p. 4392, Oct. 2021.
[15] M. Mukherjee and M. Khushi, ‘‘SMOTE-ENC: A novel SMOTE-based method to generate synthetic data for nominal and continuous features,’’ Appl. Syst. Innov., vol. 4, no. 1, p. 18, Mar. 2021



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY