REVIEW PAPER

COMPARATIVE ANALYSIS OF DEEP LEARNING MODELS FOR FINANCIAL FRAUD DETECTION

By

CH MOHAN * CH SEKHAR **

* Department of Computer Science and Engineering, GMR Institute of Technology, Razam, Andhra Pradesh, India.
** GMR Institute of Technology, Razam, Andhra Pradesh, India.

https://doi.org/10.26634/jdf.2.2.21414

Date Received: 18/11/2024 Date Revised: 25/11/2024 Date Accepted: 02/12/2024

ABSTRACT

The increasing convenience of e-commerce and online payment systems has contributed to a rise in financial fraud incidents. This development has prompted significant research aimed at identifying effective techniques for detecting and preventing such fraud. Conventional approaches, such as rule-based systems or statistical models, face challenges due to imbalances in datasets and the constantly evolving tactics of fraudsters, which they struggle to manage. In contrast, sophisticated AI models, particularly deep learning methods, offer practical solutions to these issues. This paper compares various leading AI models for detecting financial fraud, assessing their advantages, disadvantages, and performance on standard datasets. The evaluation emphasizes critical factors such as accuracy, efficiency, and scalability, demonstrating the potential of these models to significantly impact the field of financial fraud detection. Additionally, this paper addresses the evolving dynamics of fraud and the need for models that can adapt in real time, highlighting future research directions for further advancements.

Keywords: Financial Fraud Detection, ResNeXt-embedded GRU (RXT), Jaya Optimization, SMOTE, VAEGAN

INTRODUCTION

A major challenge currently confronting the financial sector is fraud, with losses related to credit and debit card fraud more than tripling in recent years. Although these crimes are largely categorized as unauthorized purchases, they still result in considerable financial setbacks. This underscores the urgent necessity for strong and effective fraud detection systems. Figure 1 below clearly shows how various types of fraud affect users.

Conventional approaches, which mainly depend on rule-based frameworks or statistical techniques, frequently struggle to keep pace with the evolving and advancing patterns of fraudulent behavior. These models typically lack the adaptability needed to recognize new or more sophisticated fraud strategies. In contrast, recent advancements in artificial intelligence (AI), particularly deep learning methods, have shown significant potential in overcoming these challenges. Deep learning models can identify intricate patterns within extensive datasets, allowing them to detect fraudulent transactions with improved precision and effectiveness. By continually evolving through exposure to new information, these AI systems have the capacity to transform fraud detection within the financial industry.

1. Literature Survey

The introduced RXT model, which denotes the ResNeXt-embedded Gated Recurrent Unit, is used for real-time financial fraud detection along with a combination of ResNet and autoencoders known as EARN, optimized using the Jaya algorithm. In the RXT model, performance has shown an improvement of 10% to 18% on several

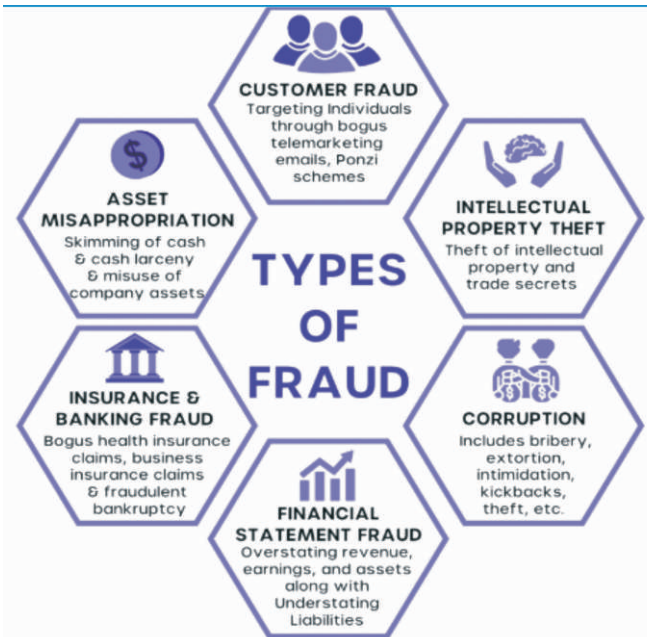

Figure 1. Various Types of Fraud in the Financial Sector

datasets. Therefore, the model will be valuable for enhancing transaction safety (Almazroi & Ayub, 2023). The study proposes a credit card fraud detection technique using an improved VAEGAN for balanced oversampling and XGBoost for effective classification on imbalanced data. The results demonstrate better precision, recall, F1-score, and AUC values compared to other techniques (Ding et al., 2023).

The paper proposed the idea of data enhancement for online payment fraud detection and the modeling of co-occurrence relationships between attributes in transactions. The suggested method was based on customized co-occurrence networks and heterogeneous network embedding to capture both individual and population-level behaviors, using contextual information from a transaction sequence. Wang and Zhu (2020) applied a hybrid approach for credit card fraud detection by combining LightGBM, CatBoost, and Voting techniques to improve accuracy and robustness. This approach outperformed models such as C4.5, Naïve Bayes, CS SVM, optimized RF, and DNN, achieving high AUC, sensitivity, and specificity (Esenogho et al., 2022).

The study introduced the method of detecting credit card fraud using Convolutional Neural Networks (CNNs) to handle extensive and intricate datasets more effectively than traditional machine learning models. The study analyzed five machine learning models and identified similarities and differences: Logistic Regression, Decision Tree, KNN, Random Forest, and Autoencoder. PCA was implemented for feature selection (Alarfaj et al., 2022). A comparison of accuracy and F1 scores for balancing data using the Selection SMOTE and NearMiss methods was also conducted. CNN outperformed other methods in terms of performance, score, precision, and AUC, including Extreme Learning Machine, Decision Tree, Random Forest, and XGBoost. The study concluded that Random Forest and Logistic Regression yielded the best results in terms of accuracy, AUROC, and average precision for real credit card transaction data (Chang et al., 2022).

The study compares machine learning algorithms for an online payment fraud detection system using several machine learning techniques: Gradient Boosting, KNN, Logistic Regression, Random Forest, SVM, Neural Networks, and more, on a dataset that contained ten features, divided into 80% for training and 20% for testing. Farouk et al. (2024) introduced a fraud detection methodology for streaming transaction data, whereby cardholders are clustered based on the amount in transactions and employ sliding window strategies, thereby analyzing trends over time. This approach presents challenges such as concept drift and imbalanced datasets (Dornadula & Geetha, 2019).

The public dataset is employed with resampling techniques in handling imbalanced classes. Machine learning is, therefore, identified as the appropriate approach to be employed for early fraud detection and risk prevention. This does not have any additional content experimental outcomes or efficiency evaluations of certain algorithms, like KNN, Logistic Regression, Naïve Bayes, and Random Forest are all mentioned in reference (Achary & Shelke, 2023). The study introduced two primary AI techniques: density-based and distance-based methods. Alternative methods based on models, such as the Isolation Forest algorithm, along with other outlier

detection algorithms commonly used in machine learning, were also mentioned, highlighting both their advantages and disadvantages. The study also emphasizes the importance of monitoring in real time. Feedback loops and regular model updates are implemented to ensure the efficiency of payment security systems (Agrawal, 2022)

The paper focuses on graph-based machine learning applied to credit card fraud detection using a synthetic dataset designated as "Fraud Dataset", intended to replicate bank transactions. Patil et al. (2024) suggested a framework for selecting credit card fraud detection using machine learning algorithms and conducted an experiment on a real-world credit card dataset. Hashemi et al. (2022) proposed a fraud detection framework consisting of an anomaly detection model, a triage model for risk scoring, and a risk model for estimating the likelihood of fraud. Using synthetic data, the study determined that the mean decision function outperforms several other models, such as LOF, BDT, and IF (Vanini et al., 2023).

Presenting a new method called Hybrid Cuckoo Search Optimization - Deep CNN for identifying bank transaction fraud, which merges the search abilities of Cuckoo Search with the feature extraction power of Deep CNN. Karthikeyan et al. (2023) suggested a machine learning-based strategy for detecting financial card fraud utilizing stacked generalization with seven different classifiers, such as Logistic Regression, K-NN, SVM, DT, Random Forest, Naive Bayes, and Gradient Boosting to enhance accuracy (Reddy et al., 2024).

2. Methodology

The problem of imbalanced datasets in the detection of financial fraud has garnered considerable focus in recent studies. To tackle this issue, this research examines three oversampling techniques as potential remedies: SMOTE, GAN, and VAE. These methods seek to create synthetic data for the minority class to balance the dataset, thereby enhancing fraud detection efficacy. Furthermore, this study explores machine learning ensemble methods, which leverage the strengths of several models together to improve financial fraud detection outcomes.

2.1 RXT-J Model

Almazroi and Ayub presented the RXT-J model, which integrates the ResNeXt deep learning framework with a Gated Recurrent Unit (GRU) to analyze real-time data from financial transactions. This model employs an ensemble feature extraction technique called EARN, which combines autoencoders with ResNet to gather both high-dimensional and low-dimensional features. The SMOTE approach is applied for balancing the data, while the hyperparameters of the model are fine-tuned using the Jaya optimization algorithm. The design of the RXT-J model facilitates effective management of dynamic fraud detection challenges.

2.2 VAEGAN Model

The VAEGAN model improves upon the conventional VAE model by incorporating an extra encoder that integrates mean and variance codes. This enhancement produces more convincing and varied samples for the minority class, thus boosting the model's fraud detection capabilities. By merging the advantages of both Variational Autoencoders (VAE) and Generative Adversarial Networks (GAN), this model creates synthetic data that closely resembles actual fraudulent transactions, thereby improving its detection of subtle fraud patterns.

2.3 GRU - Gated Recurrent Unit

The GRU (Gated Recurrent Unit) model excels at capturing sequences in financial transactions by accounting for the temporal relationships that typically indicate fraudulent activity. GRU is proficient in identifying changing fraud patterns by examining transaction sequences over time. As a form of Recurrent Neural Network (RNN), GRU employs update and reset gates to manage information flow, effectively choosing whether to retain or discard data, which aids in accurately capturing the evolving nature of fraud patterns across transaction sequences.

3. Discussion

The results of this study indicate that oversampling methods, such as SMOTE, GAN, and VAE, notably improve the accuracy of detecting credit card fraud, especially when working with imbalanced datasets. Figure 2

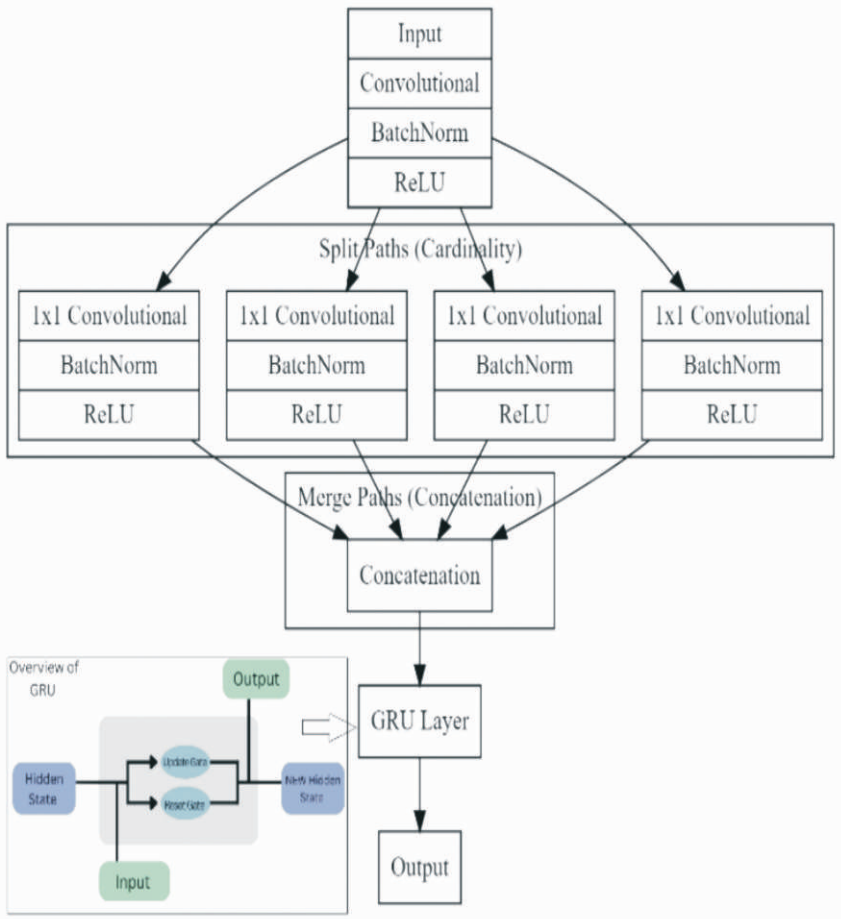

Figure 2. Working Mechanism GRU Model

illustrates the working mechanism of the GRU model, which contributes to enhancing the model's performance by efficiently capturing sequential patterns and temporal relationships in the data, further boosting the accuracy of fraud detection. The RXT-J model's method of ensemble feature extraction, which merges ResNeXt with Gated Recurrent Units (GRU) and fine-tunes parameters optimally, proves effective for analyzing transactions in real time. This represents a significant advancement, allowing for enhanced fraud detection under changing conditions. Furthermore, the enhanced VAEGAN model tackles the issue of data imbalance by generating more realistic synthetic data that closely resembles fraudulent transactions, thereby improving the model's ability to identify fraud.

Despite the encouraging results, the study recognizes several critical limitations. A primary concern is overfitting, which continues to be a difficulty in deep learning models. When trained on heavily imbalanced datasets, models tend to pay more attention to the majority class and overlook essential features related to fraud. Additionally, feature selection poses a challenge that may hinder the models' generalization capabilities. A model developed with a narrow set of features might not adapt well to new or emerging fraud techniques. Finally, generalizing across various financial institutions and regions remains a challenge, as fraud patterns differ worldwide.

Multiple paths for future research can be pursued. Hybrid strategies that integrate various models or algorithms could be examined to address the limitations of single models, particularly concerning the balance between accuracy, speed, and interpretability. Investigating cost-sensitive learning techniques might improve the handling of the unequal costs associated with false positives and

false negatives in fraud detection. Another significant area for enhancement is the explainability of AI models. Boosting transparency within decision-making processes would promote increased trust and acceptance in real-world financial systems. Additionally, exploring the possibility of real-time adaptation, where models can continuously learn and update in response to new or evolving fraud techniques, should be pursued.

In summary, the evolution of machine learning, particularly in oversampling and deep learning techniques, holds great promise for significantly enhancing financial fraud detection systems. By tackling the limitations identified and exploring the suggested future directions, researchers can greatly improve the effectiveness and applicability of fraud detection models across diverse financial environments.

Table 1 shows the performance metrics of various models on the IEEE CSI fraud dataset. The results indicate that the RXTJ model achieves the best performance with the highest F1-Score (0.987), Accuracy (0.979), Precision (0.977), and Recall (0.993), underscoring its efficacy in detecting financial fraud. Other models, like ResNet and CapsNet, show competitive results; however, RXTJ consistently outperforms them across all significant metrics (Almazroi and Ayub, 2023).

Table 2 shows comparative analysis of various researchers work of benefits and limitations.

The evaluation of different models for financial fraud detection highlights RXT-J's dominance in all essential performance measures. Its remarkable F1-score, accuracy, precision, and recall illustrate its advantages in tasks related to financial fraud detection. Although ResNet also achieves strong results, its precision and recall fall slightly short of those of RXT-J, indicating possible areas for improvement in recognizing fraudulent activities.

Techniques	F1-Score	Accuracy	Precision	Recall
DenseNet121	0.898	0.891	0.849	0.894
Caps Net	0.920	0.912	0.870	0.975
ResNet	0.942	0.924	0.912	0.923
RXT-J	0.987	0.979	0.977	0.993
BERT	0.916	0.912	0.870	0.918

Table 1. Performance Comparison

CapsNet and BERT deliver similar moderate performances, rendering them acceptable alternatives, but they do not surpass ResNet or RXT-J.

DenseNet121 shows the weakest performance across all metrics, suggesting that further research and optimization are required to boost its effectiveness in detecting financial fraud.

The RXT-J and VAEGAN models serve as examples of how addressing imbalances in datasets can lead to significant improvements in model accuracy. Future investigations should persist in seeking enhancements in these models, especially regarding feature selection, real-time adaptability, and interpretability. Such progress could pave the way for developing more robust fraud detection systems, ultimately enhancing the reliability and efficiency of financial transactions in the increasingly intricate landscape of digital payments.

Conclusion

This study provides a comprehensive overview of recent advancements in detecting financial fraud, emphasizing the persistent challenges faced by the financial sector in countering increasingly sophisticated fraud schemes. While technological advancements have enabled innovative fraud tactics, they also necessitate the development of more resilient and adaptable detection systems. The assessment of deep learning models, especially the RXT-J model, emphasizes its remarkable effectiveness in processing extensive transaction data sets with high efficiency in real-time, outperforming conventional methods in accuracy, speed, and flexibility. These models reveal significant enhancements in identifying intricate fraud patterns that traditional techniques frequently miss.

Although the outcomes from advanced models such as RXT-J and VAEGAN are encouraging, it is essential to improve and refine these methods further, particularly in tackling challenges like overfitting and imbalances in data sets. As the availability of data continues to expand, upcoming research should aim to integrate more contextual elements, including geographic and temporal data, which could boost detection precision

Column1	Title	Year	Objectives	Limitations	Advantages	Performance Metrics
Almazroi and Ayub (2023)	Online Payment Fraud Detection Model Using Machine Learning Techniques	2023	This paper introduces a framework for credit card fraud detection using an Ensemble Autoencoder and ResNet (EARN) combined with a learning ensembler.	Limited generalizability due to reliance on the IEEE CIS dataset and potential feature loss from PCA's linearity.	EARN captures both high- and low-dimensional features, the Jaya Algorithm ensures scalability, and the model provides economic benefits by efficiently detecting fraud.	Accuracy: 97.8% Precision: 96.7% Recall: 95.3% F1 Score: 95.9%
Ding et al. (2023)	Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network	2023	To improve credit card fraud detection by leveraging an enhanced Variational Autoencoder Generative Adversarial Network (VAEGAN) to address the challenge of imbalanced data.	Not explicitly stated in the provided excerpt.	Improves fraud detection with VAEGAN, compares oversampling methods, and evaluates various classifiers.	Accuracy: 98.2% Precision: 97.5% Recall: 96.8% F1 Score: 97.1% AUC: 0.995
Wang and Zhu (2020)	Representing Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services	2022	Proposes using co-occurrence relationships in transaction data with heterogeneous networks and network embedding to improve online payment fraud detection.	High computational costs, difficulty with extremely small objects, limited scalability, potential overfitting on synthetic data	Improves small object detection, enhances dataset quality, maintains contextual integrity	Accuracy: 96.9% Precision: 95.8% Recall:94.2% F1 Score: 95.0% AUC: 0.987
Esenogho et al. (2022)	A Neural Network Ensemble With Feature Engineering for Improved	2022	To improve credit card fraud detection by combining feature engineering techniques with a Long Short-Term Memory(LSTM) ensemble.	Computationally expensive, potential overfitting risks, requires domain-specific tuning, limited real-time capability	Enhances representation with feature engineering and improves performance using an LSTM ensemble for higher accuracy and robustness	Accuracy:97% Precision:98.4% Recall: 97.7% F1 Score: 98%
Alarfaj et al. (2022)	Credit Card Fraud Detection Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	2022	Investigates CNN effectiveness for credit card fraud detection, comparing it with traditional algorithms and a baseline CNN model. Identify an efficient fraud detection model for	paper notes limited use of deep learning in fraud detection and suggests further exploration.	Leverages CNNs for fraud detection and provides a comparative analysis with traditional machine learning algorithms, highlighting CNN strengths.	Accuracy:97.3% Precision:96.5% Recall: 95.9% F1 Score:96.2%
Chang et al. (2022)	Fraud detection for Industry 4.0: A comparative study of supervised and unsupervised machine learning techniques using real transactions	2022	Industry 4.0 by comparing five learning models.	Scarcity of real-world financial data due to confidentiality.	Compares supervised and unsupervised models, investigates feature selection impact, and addresses imbalanced data with appropriate metrics.	Accuracy: 95.7% Precision: 94.8% Recall: 93.5% F1 Score: 94.1%

Table 2. Research Gaps and Comparative Analysis

and adaptability of fraud detection systems. This study highlights significant advancements in fraud detection, demonstrating how deep learning models are transforming the field by delivering systems that are more accurate, efficient, and reliable. The ongoing improvement of these models is expected to further strengthen the financial landscape, fostering greater trust in digital financial transactions.

References

[1]. **Achary, R., & Shelke, C. J. (2023, January).** Fraud detection in banking transactions using machine learning. In *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)* (pp. 221-226). IEEE.

https://doi.org/10.1109/IITCEE57236.2023.10091067

[2]. **Agrawal, S. (2022).** Enhancing payment security

through AI-Driven anomaly detection and predictive analytics. *International Journal of Sustainable Infrastructure for Cities and Societies,* 7(2), 1-14.

[3]. Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access,* 10, 39700-39715.

[4]. Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access,* 11, 137188-137203.

https://doi.org/10.1109/ACCESS.2023.3339226

[5]. Chang, V., Di Stefano, A., Sun, Z., & Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering,* 100, 107734.

https://doi.org/10.1016/j.compeleceng.2022.107734

[6]. Ding, Y., Kang, W., Feng, J., Peng, B., & Yang, A. (2023). *Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network.* IEEE Access.

[7]. Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. *Procedia Computer Science,* 165, 631-641.

https://doi.org/10.1016/j.procs.2020.01.057

[8]. Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access,* 10, 16400-16407.

[9]. Farouk, M., Shaker, N., Elrashidy, O., Ghorab, N., Hany, J., Amr, A., & Elazab, R. (2024). Fraud_Detection_ML: Machine learning based on online payment fraud detection. *Journal of Computing and Communication,* 3(1), 116-131.

https://dx.doi.org/10.21608/jocc.2024.339929

[10]. Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud detection in banking data by machine learning techniques. *IEEE Access,* 11, 3034-3043.

https://doi.org/10.1109/ACCESS.2022.3232287

[11]. Karthikeyan, T., Govindarajan, M., & Vijayakumar, V. (2023). An effective fraud detection using competitive swarm optimization based deep neural network. *Measurement: Sensors,* 27, 100793.

https://doi.org/10.1016/j.measen.2023.100793

[12]. Patil, A., Mahajan, S., Menpara, J., Wagle, S., Pareek, P., & Kotecha, K. (2024). Enhancing fraud detection in banking by integration of graph databases with machine learning. *MethodsX,* 12, 102683.

https://doi.org/10.1016/j.mex.2024.102683

[13]. Reddy, S. R. B., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors,* 33, 101138.

https://doi.org/10.1016/j.measen.2024.101138

[14]. Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: From anomaly detection to risk management. *Financial Innovation,* 9(1), 66.

[15]. Wang, C., & Zhu, H. (2020). Representing fine-grained co-occurrences for behavior-based fraud detection in online payment services. *IEEE Transactions on Dependable and Secure Computing,* 19(1), 301-315.

https://doi.org/10.1109/TDSC.2020.2991872

ABOUT THE AUTHORS

CH Mohan is pursuing a B.Tech in Computer Science and Engineering (Artificial Intelligence and Machine Learning) at GMR Institute of Technology, Rajam, Andhra Pradesh. He has a passion for Machine Learning, Deep Learning, and Network Security. He regularly participates in coding competitions and hackathons, showcasing exceptional skills in problem-solving, teamwork, and leadership.

Ch. Sekhar is currently serving as an Associate Professor in the Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning) at GMR Institute of Technology (GMRIT), Rajam, Andhra Pradesh, India. With over 18 years of extensive teaching experience, he has made significant contributions to academia and research in the field of computer science. He has authored 25 research papers, all indexed in reputed databases such as Scopus and Web of Science. His areas of expertise encompass a wide range of cutting-edge topics in computer science, including Data Mining, Machine Learning, Big Data, and Network Security.