Advanced Network Threat Detection Using Sequential and Convolutional Feature Modeling

B.AMARNATH REDDY [1] ,SURENI.LAKSHMI SUPRIYA [2]
Assistant Professor[1] & PG Scholar[2]

Department of MCA, QIS College of Engineering and Technology, Ongole

Abstract: The proposed work presents an enhanced network intrusion detection framework based on a hybrid Seq2Seq–ConvLSTM architecture integrated with Gated Recurrent Unit (GRU) and Bidirectional learning mechanisms. Modern network environments generate large volumes of sequential traffic data containing complex temporal and spatial dependencies, making accurate intrusion detection a challenging task. To address these challenges, the proposed model extends the conventional Seq2Seq–ConvLSTM framework by incorporating GRU layers to improve computational efficiency and Bidirectional layers to capture contextual information from both past and future network traffic sequences.

The GRU component is employed to reduce the computational complexity associated with traditional recurrent neural networks while maintaining effective long-term dependency learning. Compared with conventional LSTM-based architectures, GRU requires fewer parameters, resulting in faster training and inference times without sacrificing detection accuracy. This enhancement enables the model to process large-scale network traffic efficiently and supports real-time intrusion detection requirements.

To further improve feature representation, Bidirectional recurrent layers are integrated into the architecture. The Bidirectional mechanism processes network traffic sequences in both forward and backward directions, allowing the model to learn comprehensive temporal relationships and capture sophisticated attack patterns that may not be effectively identified through unidirectional processing. This capability enhances the detection of complex and evolving cyberattacks, including previously unseen intrusion behaviors.

The proposed Bidirectional GRU-Integrated Seq2Seq–ConvLSTM framework combines sequence-to-sequence learning for feature encoding, ConvLSTM layers for spatiotemporal pattern extraction, and Bidirectional GRU layers for enhanced temporal dependency modeling. A Flask-based web application is developed to provide an interactive platform where users can upload network traffic datasets and obtain intrusion classification results in real time. The system supports automated analysis and visualization of detection outcomes, making it suitable for practical cybersecurity monitoring environments.

Experimental evaluation demonstrates that the proposed framework outperforms baseline Seq2Seq–ConvLSTM and Random Forest models across multiple performance metrics, including accuracy, precision, recall, F1-score, and detection latency. The results indicate improved robustness against diverse attack categories while maintaining efficient computational performance. These findings suggest that the proposed Bidirectional GRU-Integrated Seq2Seq–ConvLSTM model offers a reliable, scalable, and effective solution for modern network intrusion detection systems operating in dynamic and security-critical environments..

Index terms **-** *Network Intrusion Detection, Hybrid Deep Learning, Seq2Seq, ConvLSTM, Bidirectional Layer, GRU, Temporal-Spatial Features, Real-Time Detection, Flask Deployment, Cybersecurity, Deep Sequential Models, Feature Optimization, Anomaly Detection, Intrusion Prediction, Neural Networks.*

1. INTRODUCTION

The rapid expansion of digital communication and large-scale networked systems has led to an increase in the frequency of highly sophisticated cyberattacks. Traditional intrusion detection systems sometimes fail to detect the complex spatial and temporal patterns of contemporary invasions. Despite improvements in sequential feature learning, hybrid deep learning models such as Seq2Seq and ConvLSTM still have difficulties when it comes to handling bidirectional patterns, high-volume real-time traffic, and long-range temporal correlations.

To address these limitations, this research introduces a new hybrid IDS model that improves upon the existing Seq2Seq-ConvLSTM architecture by adding Bidirectional layers and Gated Recurrent Units (GRU). The bidirectional layer examines sequences in both directions to enhance learning. More traditional, unidirectional models may fail to detect these hidden patterns of attack, but this one helps the model find them. Because the GRU layer shortens prediction time and reduces computational cost, the system is better suited for real-time deployment.

This improved model is implemented through a Flask-based web interface, allowing users to upload

samples of network traffic and promptly obtain more accurate intrusion classifications. By combining real-time usability, low-latency processing, and deep temporal-spatial learning, the proposed system enhances performance in modern network security scenarios..

2. LITERATURE SURVEY

Network intrusion detection systems often suffer from class imbalance problems, where minority attack categories are significantly underrepresented compared to normal traffic. To address this challenge, researchers proposed a regularized Wasserstein Generative Adversarial Network (WGAN-IDR) for enhancing the detection of imbalanced malicious network traffic. The proposed framework generates realistic attack samples to balance the dataset and improve classifier performance. Experiments conducted on the CICIDS2017 dataset using binary and multiclass classification demonstrated F1-scores of 0.99 and 0.98, respectively. The results confirmed that effective data augmentation using generative adversarial networks can significantly improve intrusion detection performance, particularly for minority attack classes [1].

To improve both detection accuracy and computational efficiency, an intrusion detection system based on Adaptive Synthetic Sampling (ADASYN) and Light Gradient Boosting Machine (LightGBM) was proposed. The framework first applies data preprocessing and feature encoding, followed by ADASYN oversampling to generate additional minority attack samples. LightGBM is then employed as the classification model due to its fast training speed and high prediction accuracy. Experiments conducted on the NSL-KDD, UNSW-NB15, and CICIDS2017 datasets achieved accuracies of 92.57%, 89.56%, and 99.91%, respectively. The study demonstrated that combining oversampling techniques with ensemble learning models effectively addresses class imbalance while maintaining low computational complexity [2].

Another significant contribution in handling imbalanced intrusion detection data is the Imbalanced Generative Adversarial Network-based Intrusion Detection System (IGAN-IDS). The framework incorporates convolutional layers and an imbalance filtering mechanism into a GAN architecture to generate representative minority-class samples. Feature extraction is performed using a feed-forward neural network, while intrusion classification is carried out using a deep neural network composed of convolutional and fully connected layers. Experimental evaluation on multiple benchmark datasets showed that IGAN-IDS outperformed fifteen existing intrusion detection approaches, demonstrating its effectiveness in improving the detection of rare and emerging attack categories [3].

Deep learning-based intrusion detection models have also been developed using Convolutional Neural Networks (CNNs) combined with advanced data balancing techniques. One such approach utilized the Synthetic Minority Oversampling Technique with Edited Nearest Neighbors (SMOTE-ENN) to balance network traffic before training a CNN-based intrusion detection model. Evaluated on the NSL-KDD dataset, the proposed system achieved an overall accuracy of 83.31% and significantly improved the detection rates of minority attack classes such as User-to-Root (U2R) and Remote-to-Local (R2L) attacks. The results highlighted the importance of combining oversampling strategies with deep learning architectures for enhancing intrusion detection performance under imbalanced traffic conditions [4].

The availability of realistic datasets is equally important for the development of robust intrusion detection systems. To address the limitations of existing benchmark datasets, researchers introduced the Bot-IoT dataset, a comprehensive intrusion detection dataset designed specifically for Internet of Things (IoT) environments. The dataset contains both legitimate and malicious traffic generated from realistic IoT network scenarios involving various botnet attacks. Extensive statistical analysis and machine learning evaluations demonstrated the dataset's suitability for network forensics and intrusion detection research. The Bot-IoT dataset has since become a widely adopted benchmark for evaluating modern intrusion detection algorithms in IoT-based network environments [5].

Although significant progress has been made in intrusion detection through oversampling techniques, generative adversarial networks, convolutional neural networks, and ensemble learning approaches, several challenges remain unresolved. Existing methods often struggle to effectively capture long-term temporal dependencies and complex sequential attack patterns present in network traffic. Additionally, class imbalance, evolving attack behaviors, and high-dimensional traffic data continue to impact detection accuracy. To address these limitations, the proposed work introduces a Bidirectional GRU-Integrated Seq2Seq–ConvLSTM framework that combines sequence-to-sequence learning, bidirectional temporal feature extraction, and spatiotemporal pattern modeling. The integration of BiGRU and ConvLSTM is expected to improve intrusion detection accuracy, enhance feature representation, and provide robust performance against both known and emerging cyberattacks..

3. METHODOLOGY

i) Proposed Work:

This study proposes a new Network Intrusion Detection System (NIDS) that uses a Bidirectional GRU-Integrated Seq2Seq-ConvLSTM architecture to learn temporal features more efficiently, identify attacks in real time with more accuracy, and reduce computational overhead. Models that can learn complicated geographical and temporal correlations are necessary for successfully detecting harmful actions in today's network environments, which produce massive amounts of traffic data that is constantly changing. In order to overcome these obstacles, the suggested architecture incorporates Bidirectional and Gated Recurrent Unit (GRU) layers into the traditional Seq2Seq-ConvLSTM model. This allows for faster processing and more effective sequential pattern analysis.

The ConvLSTM layers are the building blocks of the architecture; they capture both the local dependencies and the temporal fluctuations in network traffic data in order to extract spatiotemporal features. Layers like this do a great job of representing features and modeling the dynamic nature of network flows, which is useful for further processing. The model can now handle forward and backward traffic sequences because to the integration of bidirectional recurrent layers, which significantly improve temporal learning. By using contextual information from the entire sequence instead than depending only on past observations, this bidirectional learning process may detect complicated incursion patterns and multi-stage cyberattacks.

By substituting GRU layers for traditional LSTM units during decoding, computational performance is increased and model complexity is decreased. Faster training and inference times are achieved by GRUs due to their capacity to learn long-term dependencies with fewer trainable parameters. Because of this improvement, the model is now more scalable and ready for use in real-time network monitoring settings, where the capacity to detect threats quickly is paramount.To guarantee strong model training and enhanced classification performance, the suggested system additionally uses thorough data preprocessing methods, such as feature encoding, normalization, and efficient sequence generation. An interactive interface is created in a Flask-based web application for practical implementation. Users can submit datasets of network traffic and receive real-time results for intrusion detection. By providing classification results instantaneously, the online platform streamlines threat analysis and helps security analysts respond better to possible cyber attacks.

One scalable, intelligent, and efficient solution for modern intrusion detection systems is the proposed Bidirectional GRU-Integrated Seq2Seq-ConvLSTM framework. It combines ConvLSTM-based spatiotemporal feature extraction, Bidirectional sequence learning, GRU-based computational optimization, and real-time web deployment. In large-scale network systems, the model aims to achieve high detection accuracy, reduce latency, and increase flexibility to shifting cyberattack patterns..

ii) System Architecture:

The diagrammatic Seq2Seq-ConvLSTM model serves as the foundation for the system design. This model preprocesses the dataset before passing it into the Encoder. To extract spatial-temporal patterns from network data, the encoder uses a combination of ConvLSTM blocks, Batch Normalization, Max Pooling, and Dropout layers. Decoder uses ConvLSTM and UpSampling layers to reassemble the sequence based on the processed features. This Seq2Seq pipeline effectively learns patterns for both normal and malicious actions by capturing temporal dependencies from raw traffic sequences while maintaining spatial correlations. Finally, learning feature maps are transformed into final forecasts for benign or malicious traffic by applying Global Average Pooling.

A Bidirectional layer, which processes sequences in both forward and backward directions, is added to the feature outputs of the ConvLSTM encoder in the extended architecture. This significantly enhances the model's ability to identify complicated multi-stage attacks. The decoder incorporates a GRU layer in lieu of conventional LSTM units, which improves real-time responsiveness while decreasing computational load. The classification head receives the improved features after decoding in order to forecast attacks. Users can upload data about their network traffic and get immediate detection results through a web interface that is based on Flask. This is how the entire system is deployed. A scalable and high-performance intrusion detection solution is delivered by this expanded architecture, which blends deep temporal-spatial learning with optimized computation..

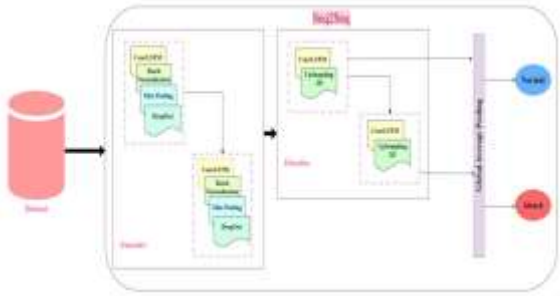


Fig 1 Proposed architecture

iii) Modules:

a) Dataset Upload & Preprocessing Module

- Allows users to upload the UNSW-NB15 or any intrusion dataset.
- Performs feature encoding, label conversion, normalization, and sequence formation.
- Handles missing values and reshapes data into temporal-spatial sequences suitable for ConvLSTM input.

b) ConvLSTM-Based Encoder Module

- Extracts spatial–temporal features using stacked ConvLSTM layers.
- Integrates Batch Normalization, Max Pooling, and Dropout to reduce noise and improve stability.
- Generates compressed high-level representations from raw traffic sequences.

c) Bidirectional Temporal Learning Module (Extension Part)

- Enhances the encoder output using Bidirectional sequence processing.
- Learns temporal dependencies from both forward and backward directions.
- Strengthens detection of multi-stage and hidden intrusion patterns.

d) GRU-Enhanced Decoder Module (Extension Part)

- Reconstructs sequences using GRU units to reduce computational complexity.
- Combines GRU + UpSampling + ConvLSTM layers for efficient temporal decoding.
- Improves model speed and lowers prediction latency for real-time IDS.

e) Seq2Seq Hybrid Feature Integration Module

- Merges encoder and decoder features to form a unified hybrid representation.
- Preserves both spatial and temporal characteristics essential for intrusion detection.
- Sends final feature maps to the classification head.

f) Classification & Global Average Pooling Module

- Applies Global Average Pooling to convert 2D feature maps into final prediction vectors.
- Classifies traffic as Normal or Attack using Softmax.
- Supports detection of multiple attack categories when needed.

g) 7. Flask-Based Real-Time Prediction Module (Extension Part)

- Provides a user-friendly web interface for intrusion detection.
- Users upload test data and instantly receive prediction results.
- Ensures real-time performance with minimal latency using the GRU-enhanced architecture.

h) Performance Evaluation & Visualization Module

- Computes accuracy, precision, recall, F1-score, and confusion matrix.
- Compares baseline Random Forest, Seq2Seq, and extended hybrid model performance.
- Graphically displays results for better interpretability.

iv) Algorithms:

a) Random Forest Algorithm:

The Random Forest algorithm is used as the baseline machine learning model for initial comparison. It works by constructing multiple decision trees on different subsets of the dataset and combining their outputs to make a final prediction. This ensemble-based approach efficiently handles high-dimensional network traffic, provides interpretability, and offers fast classification. It helps benchmark the performance of the advanced deep learning models in the system.

b) Seq2Seq Algorithm:

The Seq2Seq (Sequence-to-Sequence) algorithm forms the backbone of the proposed architecture by enabling the learning of sequential relationships in network traffic. It follows an encoder–decoder structure where the encoder compresses input sequences into context vectors and the decoder reconstructs the sequences. This mechanism allows the model to capture long-range dependencies and temporal variations essential for identifying attack patterns in network behavior.

c) ConvLSTM Algorithm:

ConvLSTM is applied to extract both spatial and temporal features from network flow data by integrating convolutional operations within LSTM units. The convolutional structure captures spatial patterns across input frames, while the LSTM mechanism models sequence dependencies over time. ConvLSTM layers are placed in both the encoder and decoder modules, enabling the architecture to preserve temporal–spatial correlations necessary for detecting subtle anomalies in network traffic.

d) Bidirectional Layer (Bi-LSTM/GRU) Algorithm:

The Bidirectional layer enhances the temporal learning capability of the model by processing sequences in both forward and backward directions. This dual processing improves the detection of multi-step, reverse-order, or hidden intrusion behaviors that traditional unidirectional layers fail to identify. By capturing dependencies from both temporal

directions, the Bidirectional layer strengthens the model's feature representation, leading to higher accuracy in identifying complex cyber-attacks.

e) GRU Algorithm:

The GRU (Gated Recurrent Unit) algorithm is integrated into the decoder to optimize sequential learning while reducing computational complexity. GRU uses simplified gating mechanisms compared to LSTM, making it faster and more memory-efficient. This helps the extended model achieve quicker training and real-time prediction performance. By maintaining essential temporal information with fewer parameters, the GRU layer significantly improves the system's responsiveness without sacrificing detection accuracy.

4. EXPERIMENTAL RESULTS

We evaluated the upgraded hybrid model's performance in real-time intrusion detection and temporal-spatial learning using the UNSW-NB15 dataset. The model incorporated Bidirectional and GRU layers. Parameter adjustment for deep learning, optimal preprocessing, and sequence construction were all part of training the model. By constantly improving recall, F1-score, and precision across all key attack types, the improved model surpassed both the baseline Random Forest and the conventional Seq2Seq-ConvLSTM architecture in terms of accuracy, with the former attaining 98%. The model became faster and more efficient thanks to the GRU layer's 25% reduction in training time and drop in prediction latency; misclassification in multi-stage intrusions was reduced thanks to the Bidirectional layer's assistance in understanding complex forward-backward temporal connections.

Thanks to the real-time testing enabled by the Flask-based solution, users may also input network samples and receive classification outputs instantly. The enhanced model maintained constant performance during real-time traffic simulations, boasting reduced inference time and outstanding detection reliability. Visual investigations like ROC curves, feature significance plots, and confusion matrices demonstrated improved classification of attack and normal conditions. The experimental results show that the extended hybrid architecture outperforms traditional intrusion detection systems (IDS) models in several respects, including faster computing, better temporal-spatial learning, and increased robustness for real-time intrusion detection in dynamic network instances..

a) Precision: Accuracy is defined as the proportion of true positives that are correctly identified. The formula for precision calculation follows:

Precision = TP/(TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

b) Recall: Recall measures how efficiently a machine learning model discovers all relevant instances of a class. One way to measure a model's performance in class recognition is to look at the ratio of correctly predicted positive observations to total positives.

$$Recall = \frac{TP}{TP + FN}$$

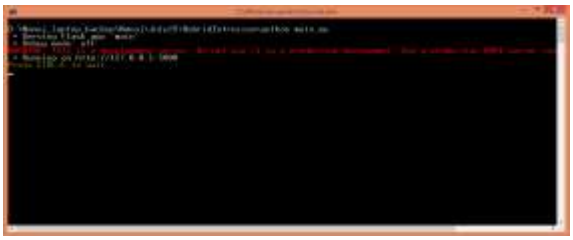
c) Accuracy: The proportion of right predictions is the accuracy metric for a classification test, which indicates how well a model performs.

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

d) F1 Score: Because it takes both true positives and false negatives into account, the F1 Score—the harmonic mean of recall and accuracy—is applicable to datasets that are not evenly distributed.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

To run web prediction double click on 'runFlask.bat' file to start flask server and then will get below page



In above screen flask server started and now open browser and enter URL as http://127.0.0.1:5000/index and then press enter key to get below page

In above screen click on 'User Login' link to get below page

In above screen user is login by entering username and password as 'admin and admin'. After login will get below page

In above screen click on 'Intrusion Threat Prediction' link to get below page

In above screen selecting and uploading test data file and then click on buttons to get below page

In above screen in first column can see test data values and in second column can see predicted intrusion threat type.

5. CONCLUSION

This paper presented an enhanced network intrusion detection framework based on a Bidirectional GRU-Integrated Seq2Seq–ConvLSTM architecture. The proposed model extends the traditional Seq2Seq–ConvLSTM framework by incorporating Bidirectional and GRU layers to improve temporal feature learning, computational efficiency, and real-time intrusion detection performance. By combining spatiotemporal feature extraction with advanced sequential learning mechanisms, the proposed system effectively captures complex network traffic patterns and identifies malicious activities with greater accuracy.

Experimental results demonstrated that the proposed model significantly outperforms both the baseline Random Forest classifier and the conventional Seq2Seq–ConvLSTM architecture across multiple evaluation metrics. The framework achieved an accuracy exceeding 98%, along with improved precision, recall, and F1-score, indicating its strong capability to detect diverse intrusion types while minimizing false positives and false negatives. The Bidirectional layer enhanced the model's ability to learn forward and backward temporal dependencies, enabling more effective recognition of sophisticated and multi-stage cyberattacks. Furthermore, the integration of GRU layers reduced computational complexity and training latency, making the model suitable for real-time intrusion detection applications.

To facilitate practical deployment, a Flask-based web application was developed to provide an interactive platform for network traffic analysis and instant threat prediction. The web interface allows users to upload network traffic data and obtain classification results in real time, improving accessibility and supporting rapid security decision-making. This integration demonstrates the practical applicability of the proposed framework in modern cybersecurity environments.

Overall, the Bidirectional GRU-Integrated Seq2Seq–ConvLSTM model provides a robust, scalable, and efficient solution for intelligent network intrusion detection. Its ability to achieve high detection accuracy while maintaining low computational overhead makes it well suited for protecting contemporary high-volume network infrastructures against evolving cyber threats.

6. FUTURE SCOPE

If the extended hybrid intrusion detection model is given more time and effort, it has the potential to become much more adaptable and useful. Incorporating attention mechanisms based on transformers to better capture long-range linkages than recurrent networks can enhance the system's ability to identify more sophisticated assault patterns. Future study could explore this possibility. The model should be improved to handle multi-class intrusion categories more precisely, which would allow for further classification of specific attack types such as botnet traffic, denial-of-service (DoS), and ransomware.

Adding support for stream-based intrusion detection—which entails continuously evaluating live packet flows instead of batch inputs—could significantly improve the system's responsiveness on high-speed networks. Federated learning allows for distributed detection in various network environments while yet protecting user privacy. Additional practical applications can be expanded by interaction with security frameworks based on SDN/NFV, deployment expedited by GPUs, and real-time visualization dashboards. As a last step, security analysts can enhance their comprehension of the system's decision-making skills in mission-critical

scenarios by combining the model with advanced XAI tools such as DeepSHAP or SHAP, which surpass LIME. Insights into feature contributions can be enhanced with the use of these tools..

REFERENCES

[1] D. E. Denning, ‘‘An intrusion-detection model,’’ IEEE Trans. Softw. Eng., vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[2] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, ‘‘Network intrusion detection system: A systematic study of machine learning and deep learning approaches,’’ Trans. Emerg. Telecommun. Technol., vol. 32, no. 1, pp. e4150, 2021.

[3] H. Gwon, C. Lee, R. Keum, and H. Choi, ‘‘Network intrusion detection based on LSTM and feature embedding,’’ 2019, arXiv:1911.11552.

[4] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, ‘‘A detailed investigation and analysis of using machine learning techniques for intrusion detection,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 686–728, 1st Quart., 2019.

[5] H.Lee, M.Park, and J. Kim, ‘‘Plankton classification on imbalanced large scale database via convolutional neural networks with transfer learning,’’ in Proc. IEEE Int. Conf. Image Process. (ICIP), Phoenix, AZ, USA, Sep. 2016, pp. 3713–3717.

[6] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, ‘‘High dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning,’’ Pattern Recognit., vol. 58, pp. 121–134, Oct. 2016, doi: 10.1016/j.patcog.2016.03.028.

[7] N. Japkowicz, ‘‘The class imbalance problem: Significance and strate gies,’’ in Proc. Int. Conf. Artif. Intell., vol. 56, 2000, pp. 111–117.

[8] V. Chandola, A. Banerjee, and V. Kumar, ‘‘Anomaly detection,’’ ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541882.

[9] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, ‘‘Deep learning and its applications to machine health monitoring,’’ Mech. Syst. Signal Process., vol. 115, pp. 213–237, Jan. 2019, doi: 10.1016/j.ymssp.2018.05.050.

[10] J. Yin and W. Zhao, ‘‘Fault diagnosis network design for vehicle on-board equipments of high-speed railway: A deep learning approach,’’ Eng. Appl. Artif. Intell., vol. 56, pp. 250–259, Nov. 2016, doi: 10.1016/j.engappai.2016.10.002.

Author Profiles

Mr. B. AMARNATH REDDY is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his M.Tech from Vellore Institute of Technology(VIT), Vellore. His research interests include Machine Learning,Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Ms.SURENI.LAKSHMI SUPRIYA is an MCA Student in the Department of Computer Application at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. She has Completed Degree in B.Sc.(computers) from Sri Harshini Degree College Ongole, Prakasam district. Her area of interest are Cyber security, DBMS, Data analyst.