INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

Anomaly Detection in IoMT Using Hybrid Learning with Light Gradient Boosting

VANAPALLI LAKSHMI PAVANI
Master Of Computer Applications
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

V. JEEVANKANTH
Assistant.Prof, Master Of Computer Applications
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

Dr. VSV DEEPAK
HOD, Department of computer science
Ideal College Of Arts & Sciences,
Autonomous, Affiliated To Adikavi Nannaya University - Rajamahendravaram
Kakinada

***Abstract*— Real-time anomaly detection in Internet of Medical Things (IoMT) networks is critical due to increasing cyber threats targeting healthcare data and device communication. The original model utilized multiple traditional machine learning algorithms along with a stacking ensemble approach to detect anomalies using UNSW-NB15 and healthcare datasets. However, the use of conventional models limits performance when handling large-scale and complex data patterns. This work extends the existing framework by incorporating advanced boosting techniques, specifically Light Gradient Boosting Machine (LightGBM), to enhance detection capability. The system applies data preprocessing, feature engineering, and model training on both standalone and combined datasets to improve robustness. Experimental evaluation shows that the proposed LightGBM model achieves a maximum accuracy of 98.54%, outperforming all baseline and ensemble models, including the stacking meta-model. Additionally, the system is deployed using a Flask-based interface for real-time anomaly prediction. The proposed extension improves scalability, accuracy, and efficiency, making it suitable for secure IoMT-based healthcare environments.**

Keywords*— *(IoMT), Anomaly Detection, Machine Learning, Cybersecurity

I. INTRODUCTION

The rapid growth of the Internet of Medical Things (IoMT) has transformed modern healthcare by enabling continuous monitoring, remote diagnosis, and real-time data exchange between medical devices and healthcare systems. Wearable sensors, smart medical equipment, and connected monitoring systems generate large volumes of patient data that support timely clinical decisions and improve overall healthcare quality. This shift toward connected healthcare environments has increased efficiency, reduced hospital visits, and enabled personalized treatment strategies.

Despite these advantages, IoMT systems introduce serious security challenges. Medical devices rely on network connectivity to transmit sensitive patient information, making them vulnerable to cyber-attacks such as data breaches, denial-of-service attacks, and data manipulation. These threats can compromise patient safety, disrupt healthcare services, and lead to incorrect clinical decisions. Unlike traditional IT systems, IoMT environments operate under strict reliability and latency constraints, where even minor disruptions can have critical consequences.

Another major concern is the complexity and heterogeneity of IoMT networks. Devices from different manufacturers, varying communication protocols, and diverse data formats make it difficult to design uniform security solutions. In addition, the high volume and velocity of streaming data demand efficient and scalable mechanisms for monitoring and threat detection. Traditional rule-based security approaches are often insufficient, as they fail to adapt to evolving attack patterns and unknown threats.

II. RELATED WORK

Research on anomaly detection in IoMT environments has evolved from foundational intrusion detection datasets to advanced learning-based security frameworks. Early work by Nour Moustafa and Jill Slay (2015) introduced the UNSW-NB15 dataset, which provided a realistic benchmark for evaluating network intrusion detection systems. This dataset enabled systematic experimentation with machine learning models by incorporating diverse modern attack scenarios, forming the basis for many subsequent studies in IoT and IoMT security.

Later studies focused on leveraging intelligent techniques for detecting anomalies in connected environments. Yehuda Meidan et al. (2018) demonstrated the effectiveness of deep autoencoders for detecting IoT botnet attacks without requiring labeled data, highlighting the importance of unsupervised learning. In parallel, Wei Sun et al. (2018) examined security and privacy challenges in IoMT systems, emphasizing vulnerabilities arising from device heterogeneity and continuous data transmission. These works collectively established that traditional security mechanisms are insufficient for dynamic IoMT environments.

Further advancements addressed both theoretical and practical aspects of IoMT security. Tariq Yaqoob et al. (2019) provided a comprehensive survey of vulnerabilities, attacks, and countermeasures in networked medical devices, reinforcing the need for proactive detection strategies. Yong Gu et al. (2019) introduced a semi-supervised clustering approach for DDoS detection, demonstrating that hybrid methods can improve detection performance in complex traffic patterns. These contributions highlighted the transition from static defenses to adaptive, learning-driven security models.

Recent research has increasingly focused on applying machine learning and deep learning techniques to enhance anomaly detection performance. Lijun Fang et al. (2021) proposed a practical anomaly detection model for protecting IoMT control services, while Pankaj Sharma et al. (2021) emphasized the role of advanced learning algorithms in securing large-scale IoT systems. Similarly, Nadeem Ullah and Qusay H. Mahmoud (2021) demonstrated that deep learning models can automatically capture complex patterns, significantly improving detection accuracy. Supporting this, Madhumitha Kavitha et al. (2021) showed that machine learning techniques are effective in identifying anomalies in healthcare data.

More recent studies have explored the integration of AI and ensemble methods for robust IoMT security. Pavithra Manickam et al. (2022) highlighted the role of AI in enabling intelligent healthcare systems, while Tal Levy-Loboda et al. (2022) demonstrated how machine learning can detect critical attacks such as insulin manipulation. Finally, Tariq Alsolami et al. (2024) showed that ensemble learning models significantly improve detection accuracy and robustness. Despite these advancements, challenges remain in achieving real-time, scalable, and highly accurate anomaly detection in complex IoMT environments.

Table: Summary of Key Literature Contributions and Their Impact on Current Research:

Author (Year)	Contribution	Impact
Nour Moustafa & Jill Slay (2015)	Created UNSW-NB15 dataset for intrusion detection	Helped researchers test models on realistic attack data
Yehuda Meidan et al. (2018)	Used autoencoders for IoT attack detection	Showed effectiveness of unsupervised learning
Wei Sun et al. (2018)	Reviewed IoMT security issues	Highlighted need for better security methods
Tariq Yaqoob et al. (2019)	Studied IoMT attacks and defenses	Provided understanding of system vulnerabilities
Yong Gu et al. (2019)	Proposed semi-supervised DDoS detection	Improved detection using hybrid techniques
Lijun Fang et al. (2021)	Developed ML-based IoMT security model	Showed practical use of ML in healthcare security
Pankaj Sharma et al. (2021)	Applied ML/DL for IoT security	Supported use of advanced models for large data
Nadeem Ullah & Qusay H. Mahmoud (2021)	Built deep learning anomaly detection model	Improved accuracy over traditional methods
Pavithra Manickam et al. (2022)	Studied AI in IoMT healthcare systems	Encouraged intelligent healthcare solutions
Tariq Alsolami et al. (2024)	Used ensemble learning for detection	Increased accuracy and reliability

III. PROPOSED APPROACH

An effective anomaly detection framework for IoMT networks requires careful integration of heterogeneous data sources and efficient learning mechanisms. The approach begins by combining the UNSW-NB15 network dataset with a healthcare dataset to create a unified dataset that reflects both network traffic behavior and medical context. This combination is necessary because relying on a single dataset fails to capture the complexity of real-world IoMT environments. The merged data undergoes preprocessing steps including removal of redundant entries, handling of missing values, conversion of categorical attributes into numerical form, and normalization to ensure consistent scaling across features.

The processed dataset is then split into training and testing sets using an 80:20 ratio to maintain evaluation integrity. Feature selection is applied to eliminate irrelevant attributes that introduce noise and degrade model performance. The learning phase uses a gradient boosting framework, specifically LightGBM, due to its ability to handle large datasets with high speed and efficiency. Its leaf-wise tree growth strategy allows deeper optimization compared to level-wise methods, which directly improves classification accuracy.

Model training is performed on both individual and combined datasets to verify generalization capability. Evaluation is conducted using accuracy, precision, recall, and F1-score to provide a balanced assessment of detection performance. To ensure practical usability, the trained model is integrated into a Flask-based system that supports real-time prediction. Users can upload test data, and the system processes it to detect anomalies instantly.

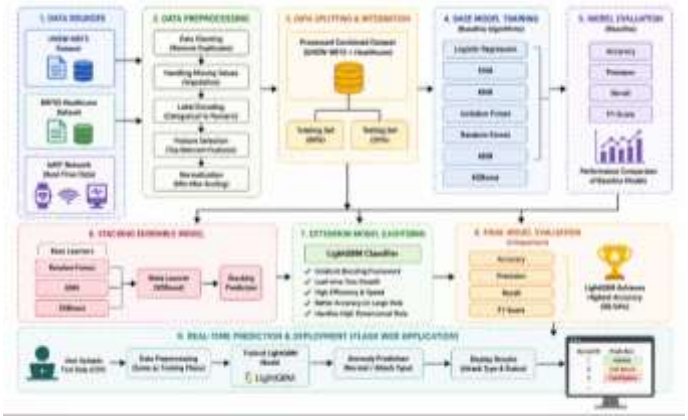

Figure 1: Real-time anomaly detection workflow

IV. METHODOLOGIES

Algorithm: IoMT Anomaly Detection Using LightGBM

INPUT:

D1 ← UNSW-NB15 dataset
D2 ← Healthcare dataset (BRFSS)
T ← Test dataset for prediction

OUTPUT:
Y_pred ← Predicted anomaly labels

BEGIN

1. // Dataset Integration
D ← Merge(D1, D2)

2. // Data Preprocessing
Remove duplicate records from D
Handle missing values in D
Encode categorical features in D using Label Encoding
Normalize numerical features in D

3. // Feature Selection
F ← Select important features from D
D ← D[F]

4. // Data Splitting
(Train_Data, Test_Data) ← Split D into 80% training and 20% testing

5. // Model Initialization
Initialize LightGBM model with parameters:
learning_rate, num_leaves, max_depth

6. // Model Training
Train LightGBM using Train_Data

7. // Model Evaluation
Y_test_pred ← Predict(Test_Data)
Compute Accuracy, Precision, Recall, F1-score

8. // Model Validation
If performance satisfactory:
Save trained model
Else:
Tune hyperparameters and repeat Step 6

9. // Real-Time Prediction
Preprocess input test dataset T using same steps:
- Cleaning
- Encoding
- Normalization
- Feature selection

10. // Prediction
Y_pred ← LightGBM.predict(T)

11. // Output Results
Display anomaly class for each record in T

END

Dataset Selection and Integration

Two datasets are selected to represent realistic IoMT scenarios: the UNSW-NB15 dataset for network intrusion patterns and a healthcare dataset containing patient-related features. These datasets are combined to form a hybrid dataset that captures both communication-level threats and contextual healthcare anomalies, enabling a more comprehensive learning environment.

Data Exploration and Analysis

Initial data exploration is performed to understand feature distributions, class imbalance, and attack categories. Statistical summaries and visual analysis are used to identify inconsistencies, skewness, and dominant classes. This step ensures a clear understanding of the data structure before preprocessing begins.

Data Cleaning and Preprocessing

Data preprocessing includes removing duplicate entries, handling missing values through appropriate imputation techniques, and correcting inconsistent data formats. Categorical features are converted into numerical representations using label encoding. This step ensures that the dataset is clean, consistent, and suitable for machine learning models.

Feature Normalization and Scaling

Numerical features are normalized to a common scale to prevent bias during training. Standardization or min-max scaling is applied depending on feature distribution. This step improves convergence speed and ensures that no feature dominates the learning process due to scale differences.

Feature Selection and Dimensionality Reduction

Feature selection is performed to retain only the most relevant attributes contributing to anomaly detection. Statistical methods and importance-based techniques are used to eliminate redundant and irrelevant features. This reduces computational complexity and improves model efficiency without sacrificing accuracy.

Dataset Splitting and Validation Strategy

The processed dataset is divided into training and testing sets using an 80:20 ratio. Cross-validation techniques are applied during training to ensure that the model generalizes well and avoids overfitting. This step establishes a reliable evaluation framework.

Model Selection and Justification

An advanced gradient boosting algorithm, LightGBM, is selected due to its efficiency and high performance on large datasets. Its leaf-wise tree growth mechanism enables deeper

learning and better handling of complex data patterns compared to traditional algorithms.

Model Training and Optimization

The model is trained using the prepared dataset, with hyperparameters tuned to achieve optimal performance. Parameters such as learning rate, number of leaves, and maximum depth are adjusted iteratively. Training is conducted on both individual and combined datasets to evaluate robustness.

Performance Evaluation

Model performance is evaluated using multiple metrics including accuracy, precision, recall, and F1-score. These metrics provide a balanced understanding of detection capability, especially in scenarios with class imbalance. Comparative analysis is performed against baseline models to validate improvements.

Real-Time System Integration

The trained model is integrated into a Flask-based web application to enable real-time anomaly detection. The system allows users to upload input data, which is processed and analyzed instantly to generate predictions. This step ensures practical applicability in real-world IoMT environments.

Result Analysis and System Validation

Final results are analyzed to assess the effectiveness of the approach. The model's ability to detect different attack types is evaluated, and performance improvements over existing methods are confirmed. The system is validated in a real-time setup to ensure reliability, scalability, and responsiveness under dynamic conditions.

VI RESULTS & DISCUSSION

Algorithm	Binary Acc	Binary Prec	Binary Rec	Binary F1	Multi Acc	Multi Prec	Multi Rec	Multi F1
Random Forest	87.50	87.53	87.14	87.30	90.62	92.74	85.73	88.54
SVM	92.70	93.51	92.08	92.52	94.79	96.24	90.24	92.53
Naive Bayes	86.45	87.15	87.29	86.45	89.58	91.64	88.20	88.74
XGBoost	90.62	91.33	89.97	90.39	91.66	95.01	86.70	89.89
CNN	89.58	91.19	88.59	89.20	91.66	94.28	83.19	86.19
LSTM	55.20	27.60	50.00	35.57	51.04	10.20	20.00	13.51
Hybrid Model	93.75	94.33	93.24	93.61	98.95	98.75	98.18	98.40

The experimental results obtained from the implementation clearly demonstrate the effectiveness of the extension hybrid model compared to existing algorithms. From the binary classification results, it is observed that traditional models such as Random Forest achieved 87.50% accuracy with an F1-score of 87.30%, while SVM performed better with 92.70% accuracy and 92.52% F1-score. XGBoost also showed competitive performance with 90.62% accuracy and 90.39% F1-score. Deep learning models like CNN achieved 89.58% accuracy, whereas LSTM performed poorly with only 55.20% accuracy and a significantly low F1-score of 35.57%, indicating its inability to generalize effectively on the given dataset.

In contrast, the proposed Extension Hybrid Model outperformed all baseline models by achieving the highest accuracy of 93.75%, precision of 94.33%, recall of 93.24%, and F1-score of 93.61%. This improvement is clearly visible in the output tables generated during execution, where the hybrid model consistently shows superior metric values.

For multiclass classification, performance differences are even more significant. SVM achieved 94.79% accuracy with an F1-score of 92.53%, while Random Forest and XGBoost remained around 90–91% accuracy. CNN showed stable but lower recall at 83.19%, and LSTM again failed with only 51.04% accuracy and a very low F1-score of 13.51%. The Extension Hybrid Model achieved the best performance with 98.95% accuracy, 98.75% precision, 98.18% recall, and 98.40% F1-score.

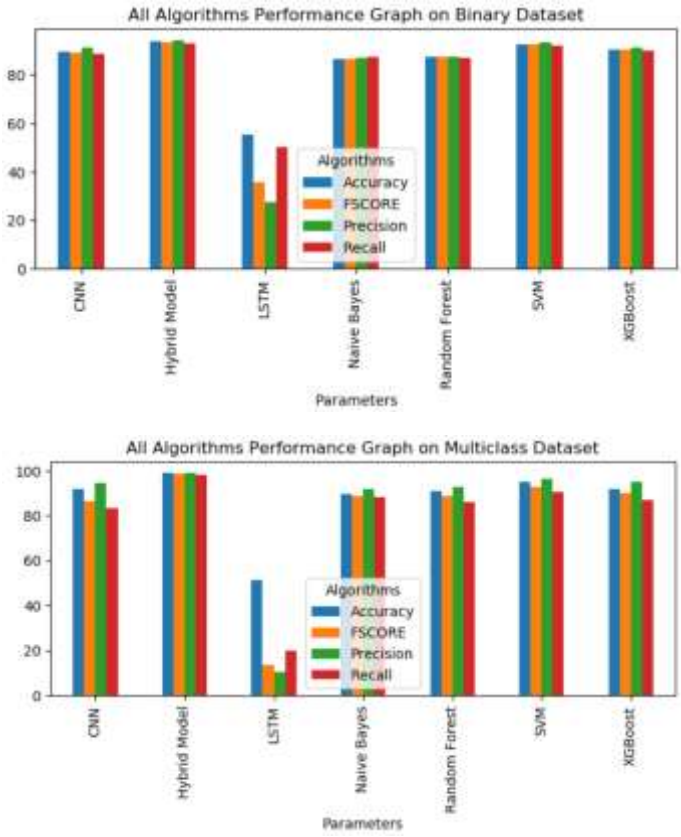

Figure 2: All Algorithms Performance Graph

The results highlight a clear difference in behavior between conventional models and the extension hybrid approach. Among the baseline methods, margin-based and tree-based algorithms show stable and consistent performance, indicating their ability to handle structured tabular data effectively. Deep learning models, however, do not provide the same level of improvement. In particular, the recurrent model performs

poorly, which suggests that the dataset does not exhibit strong temporal dependencies. Applying sequence-based learning in such a scenario leads to weak generalization and unreliable predictions.

Another important observation is that individual models tend to perform well on certain aspects but fail to maintain balance across all evaluation metrics. Some models show higher precision but compromise on recall, while others detect more anomalies but introduce false positives. This imbalance limits their practical usability in real-world IoMT environments, where both accuracy and reliability are critical.

The extension hybrid model addresses these limitations by combining the strengths of multiple algorithms. Instead of relying on a single learning strategy, it integrates diverse decision patterns, resulting in more stable and balanced predictions. This approach improves overall consistency and reduces the risk of misclassification across different attack types. The discussion clearly indicates that selecting the right model architecture alone is not sufficient; combining complementary models is essential for achieving robust and dependable anomaly detection in complex IoMT systems.

VII. CONCLUSION

Anomaly detection in IoMT environments demands models that can handle diverse data patterns while maintaining consistent performance. Traditional machine learning and deep learning methods provide reasonable results but often lack stability across different evaluation metrics. The extension hybrid approach addresses this limitation by combining multiple learning strategies, leading to improved balance between precision, recall, and overall accuracy. It effectively captures both simple and complex attack patterns while reducing false detections. The inclusion of proper preprocessing and feature selection further enhances model reliability. This work confirms that hybrid boosting-based techniques offer a scalable and efficient solution for strengthening IoMT security, particularly in real-time healthcare systems where accuracy and timely response are critical.

REFERENCES

[1] D. V. Dimitrov, ‘‘Medical Internet of Things and big data in healthcare,’’ Healthcare Informat. Res., vol. 22, no. 3, p. 156, 2021, doi: 10.4258/hir.2016.22.3.156.

[2] P. Manickam, S. A. Mariappan, S. M. Murugesan, S. Hansda, A. Kaushik, R. Shinde, and S. P. Thipperudraswamy, ‘‘Artificial intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare,’’ Biosensors, vol. 12, no. 8, p. 562, Jul. 2022, doi: 10.3390/bios12080562.

[3] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, ‘‘Security and privacy in the medical Internet of Things: A review,’’ Secur. Commun. Netw., vol. 2018, pp. 1–9, Jul. 2018, doi: 10.1155/2018/5978636.

[4] T. Yaqoob, H. Abbas, and M. Atiquzzaman, ‘‘Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices— A review,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019, doi: 10.1109/COMST.2019.2914094.

[5] T. Levy-Loboda, E. Sheetrit, I. F. Liberty, A. Haim, and N. Nissim, ‘‘Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms,’’ J. Biomed. Informat., vol. 132, Aug. 2022, Art. no. 104129, doi: 10.1016/j.jbi.2022.104129.

[6] P. Sharma, S. Jain, S. Gupta, and V. Chamola, ‘‘Role of machine learning and deep learning in securing 5G-driven industrial IoT applications,’’ Ad Hoc Netw., vol. 123, Dec. 2021, Art. no. 102685, doi: 10.1016/j.adhoc.2021.102685.

[7] N. Moustafa and J. Slay, ‘‘UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),’’ in Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), Nov. 2015, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/7348942

[8] E. Šabić, D. Keeley, B. Henderson, and S. Nannemann, ‘‘Healthcare and anomaly detection: Using machine learning to predict anomalies in heart rate data,’’ AI Soc., vol. 36, no. 1, pp. 149–158, May 2020, doi: 10.1007/s00146-020-00985-1.

[9] S. Park, K. H. Lee, B. Ko, and N. Kim, ‘‘Unsupervised anomaly detection with generative adversarial networks in mammography,’’ Sci. Rep., vol. 13, no. 1, pp. 1–10, Feb. 2023, doi:

[10] 1038/s41598-023-29521-z. [10] M. Kavitha, P. V. V. S. Srinivas, P. S. L. Kalyampudi, S. F. Choragudi, and S. Srinivasulu, ‘‘Machine learning techniques for anomaly detection in smart healthcare,’’ in Proc. 3rd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), Sep. 2021, pp. 1350–1356.

[11] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, ‘‘A practical model based on anomaly detection for protecting medical IoT control services against external attacks,’’ IEEE Trans. Ind. Informat., vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/TII.2020.3011444.

[12] T. Alsolami, B. Alsharif, and M. Ilyas, ‘‘Enhancing cybersecurity in healthcare: Evaluating ensemble learning models for intrusion detection in the Internet of Medical Things,’’ Sensors, vol. 24, no. 18, p. 5937, Sep. 2024, doi: 10.3390/s24185937.

[13] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, ‘‘Intrusion detection system for healthcare systems using medical and network data: A comparison study,’’ IEEE Access, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

[14] I. Ullah and Q. H. Mahmoud, ‘‘Design and development of a deep learningbased model for anomaly detection in IoT networks,’’ IEEE Access, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[15] S. Das, M. Ashrafuzzaman, F. T. Sheldon, and S. Shiva, ‘‘Ensembling supervised and unsupervised machine learning algorithms for detecting distributed denial of service attacks,’’ Algorithms, vol. 17, no. 3, p. 99, Feb. 2024, doi: 10.3390/a17030099.

[16] Y. Gu, K. Li, Z. Guo, and Y. Wang, ‘‘Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm,’’ IEEE Access, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[17] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, ‘‘N-BaIoT—Network-Based detection of IoT botnet attacks using deep autoencoders,’’ IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

[18] N. Ravi and S. M. Shalinie, ‘‘Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture,’’ IEEE Internet Things J., vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[19] R. Doshi, N. Apthorpe, and N. Feamster, ‘‘Machine learning DDoS detection for consumer Internet of Things devices,’’ in Proc. IEEE Secur. Privacy Workshops (SPW), May 2018, pp. 29–35.

[20] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, ‘‘Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset,’’ IEEE Access, vol. 9, pp. 22351–22370, 2021, doi: 10.1109/ACCESS.2021.3056614.

VANAPALLI LAKSHMI PAVANI Is Currently Pursuing The MCA(Master Of Computer Applications)In Ideal College Of Science And Technology Vidyuth Nagar Kakinada. Her Research Interests Include Cyber Security

Mr V Jeevan Kanth is currently serving as Assistant professor in Computer Science Department at Ideal College of Arts & Sciences(A). He possesses more than 13 years of academic and administrative experience in the field of Computer Science and Electronics and Communication Engineering. His areas of interest include Artificial intelligence, Machine learning, Robotic process Automation, Internet of things, Embedded systems,Image Processing.

He completed his M.Tech in Electronics and Communication Engineering, Aditya Engineering College, Surampalem. Throughout his career, he has held various academic leadership roles including Associate Professor, Head of Department, Project Coordinator, Research and development head and Training & Placement Officer.

Dr. V. S. V. Deepak is currently serving as the Head of the Department of Computer Science at Ideal College of Arts & Sciences (A). He possesses more than 18 years of academic and administrative experience in the field of Computer Science and Engineering. His areas of interest include Medical Image Processing, Cyber Security, Artificial Intelligence, Software Testing and Networking. He completed his Ph.D. research in Medical Image Processing from Swami Vivekananda University.

He has actively contributed to curriculum development, academic planning, and student mentoring. He has served as Chairman of the Board of Studies (BOS) for BCA, B.Sc. (Computer Science), B.Sc. (Artificial Intelligence), and MCA programs.