Journal of ICT, Design, Engineering and Technological Science (JITDETS)
VOL. 9, NO. 2, pp. 88-95, 2025
DOI: https://doi.org/10.33150/JITDETS-9.2.3

ORIGINAL CONTRIBUTION

BERT-LSTM-LGBM Approach for DDoS Attacks Detection in IoT Network Using ML

Imdad Ali Shah[1*], Noor Zaman Jhanjhi[2]

[1]FEST, Iqra University, Karachi, Pakistan

[3]School of Computer Science, Malaysia

***Abstract*— New cybersecurity challenges have increased as the interconnected IoT devices grow, such as DDoS attacks, which are observed as more attacks exploit resource-constrained IoT devices. Conventional detection mechanisms often fail to capture the dynamic and diverse nature of IoT network traffic, and several researchers and professionals have addressed these concerns. In view of the issues raised by the researchers, the presented models need to enhance their accuracy and performance. The BERT_LSTM-LGBM model has been proposed for an intelligent and accurate DDoS attack detection in IoT devices. BERT component is used to remove deep contextual features from network traffic data, capturing intractable relationships and semantic dependency. The long Short-Term Memory (LSTM) network further improves temporal arrangements learning to detect sequential anomalies, while the LGBM classifier promises high-speed and comprehensible decision-making. The results show that the BERT-LSTM-LGBM framework is robust and can detect diverse DDoS attack patterns, offering a scalable and intelligent solution for securing next-generation IoT infrastructures. Our proposed model presents its exceptional proficiency in threat detection within the IoT environment. We achieved remarkable results such as 99.8%, 98%, and 99%.**

***Index Terms*— BERT-LSTM, DDoS attacks, IoT devices traffic environment, LGBM**

Received: 28 July 2025; **Accepted:** 3 October 2025; **Published:** 19 December 2025

I. INTRODUCTION

The quick growth of IoT networks has significantly increased exposure to large-scale DDoS attacks that can disrupt critical services and compromise network availability. To address this issue, a hybrid detection framework integrating BERT, LSTM, and LightGBM is proposed for intelligent DDoS attack identification. In this approach, BERT is utilized to capture rich contextual representations from network traffic features, while LSTM effectively models temporal and sequential patterns of malicious behavior.

IoT networks are integrating sensors, embedded computers, and devices in various sectors, including agriculture, smart cities, and hazardous industries such as mining. IoT technology has enhanced living by streamlining processes and increasing productivity[1, 2, 3]. By 2030, there will likely be over 29 billion linked devices, which has increased the susceptibility of IoT ecosystems to changing cyber threats [4, 5]. Quality of service, security standards, appropriate administration of privacy, ongoing serious, precise service addressing privacy information, and confidentiality are some of the major issues facing IoT ecosystems. Figure 1 presents the DDoS attacks detected in IoT networks from 2020 to 2025, adopted from studies.

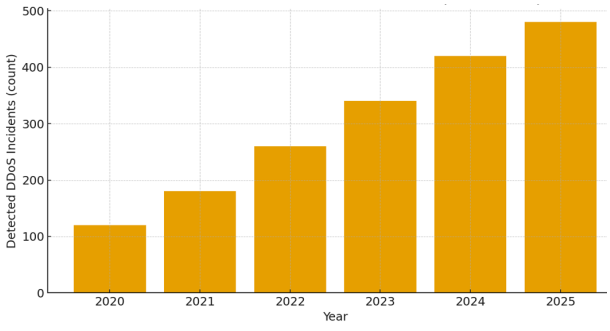

Fig. 1. DDoS attacks detected in IoT networks

Figure 1 demonstrates that DDoS attack detection is increasing each year till 2025. This creates significant security vulnerabilities, primarily in IoT contexts. The use of DL and ML for secure IoT needs to be explored [6, 7]. However, based on the variables the dataset used, the characteristics chosen, the algorithms employed, and the evaluation measures, their efficacy and dependability differ significantly. Furthermore, there is a critical requirement to successfully balance detection accuracy with resource limits because many studies have not focused on creating resource-efficient models for IoT devices with limited computational resources.

Conventional detection mechanisms often fail to adapt to the dynamic, diverse nature of IoT network traffic. Several researchers and professionals have addressed these types of issues and need to work more on enhanc-

*Corresponding author: Imdad Ali
†Email: imdad.ali@iqra.edu.pk

ing the model's accuracy.

A. Paper organization

- In the first section, this research presents an introduction and a comprehensive literature Review.
- In the second section, this research presents the methodology, such as data collection and a flowchart.
- In the third section, this research presents the details of the Conventional Neural Network (CNN) and LSTM.
- In this section, this research presents the details of the dataset, data preprocessing, binary classification flow chart, Algorithm 1, and Algorithm 2.
- In the fourth section, this research presents the details of the proposed framework, architecture, and model.
- In the fifth section, this research presents the results, the confusion matrix, training and validation metrics, a summary of classes, and accuracy over epochs, and a benchmark table.
- In the sixth and last, this research presents the conclusion and future work.

II. LITERATURE REVIEW

IoT device integration has greatly increased operational efficiency across a range of businesses, but it has also brought about several security issues. Significant risks to IoT ecosystems are posed by cyber threats that target IoT devices, such as coordinating compromised devices to launch extensive cyber-attacks. This makes it perfect for low-resource IoT devices. However, it has issues with adaptability to sophisticated attacks, scalability, and a high false positive rate in diverse IoT scenarios [8, 9]. Overcoming the drawbacks of conventional methodologies, large datasets can be generalized by ML models to find new approaches, including supervised, unsupervised, and reinforcement learning. Presented ensemble-based learning frameworks that maximise detection accuracy by utilising feature engineering and dimension reduction strategies [10, 11, 12]. The F1-SEFL methodology documents data dimensionality by 86.9% by using extremely radonised trees for feature significance analysis. Figure 2: Overview of the LR of our proposed model.

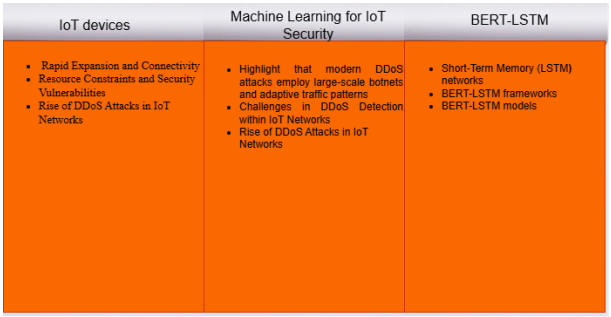

Fig. 2. LR of proposed model

Figure 2 shows the rapid expansion and connectivity, explaining machine learning support for IoT security. Furthermore, BERT-LSTM frameworks support.

These methods demonstrate how ML may optimise resource usage without sacrificing detection precision. DL methods, such as CNNs, LSTM hybrid models. A CNN-LSTM hybrid architecture that reduced dimensionality using Principal Component Analysis (PCA). The framework incorporates advanced optimization techniques, quantization, and pruning to provide high scalability and detection in IoT environments with limited processing capability. Achieved a 96% detection accuracy using data from Raspberry Pi-infected IoT devices by applying CNNs for extraction and LSTMs for classification [13, 14]. Introduced a DNN-based malware system that proved feasible for real-time deployment with a 93% detection accuracy and a 92% F1-score. The resilience of hybrid architectures is further demonstrated by studies conducted in IIoT contexts. CNN, LSTM, and GRU are combined in the generated models to reach 100% anomaly detection accuracy [15, 16, 17]. These technologies are especially appropriate for large-scale IIoT systems, as they incorporate asynchrony and federated learning, which guarantee privacy and facilitate decentralised model training.

Investigated Bidirectional Gversarial Networks (BiGAN) and Adversarial Autoencodes(AAE) for the detection of zero-day attacks. These models showed great effectiveness in addressing new risks and obtained an amazing result. A hierarchical analysis detection system that combines auto encoders (AES) and Generation Adversarial Networks (AEs), and Generative Adversarial Networks (GANs) [18, 19]. Thereby resolving privacy and data scarcity issues. Table 1 presents the research analysis.

TABLE I
RESEARCH ANALYSIS

Reference	Techniques	Datasets	Challenges
[20]	RF	Used BOT-IoT dataset	Real-time data analysis
[21]	RF and XGBoost	Used a robust dataset	Need to work on models to enhance accuracy and improve
[22]	DL and Convolution network	Real-world and synthetic datasets got	to enhance overall security factors in SDN
[23]	SVM	CICIDS2017 dataset	Need to work on lightweight security
[24, 25]	DL and CNN	BoTNet dataset	Need to continue work on evolving DDoS attacks
[26, 27]	Research methods	Domain	Explanations
[28]	Review	IoT	IoT attacks
[29, 30]	Survey	IoT	IoT security areas
[31]	Survey	IoT	Threats and attacks based ananysis of IoT
[32]	Framework	IoT	IoT attack surfaces
[33]	Low-power	IoT	Assessmentin IoT network

In Table 1, the researchers discussed in detail the DDoS attacks detection models analysis. Further, the authors explain research objectives, techniques, findings, and challenges in the dynamic IoT environment. Its improved performance over traditional models was demonstrated in the evaluation of the UNSW BoT-IoT dataset, highlighting the usefulness of integrating GANs with AEs for distributed IoT ecosystems. Robust IoT intrusion detection relies on handling class imbalance and feature selection. Developing a universal feature section technique by addressing these issues with datasets [34, 35]. The bagging approach used a random forest-based feature, shuffle methods in conjunction with SMOTE resampling

techniques, to determine which characteristics had the greatest influence. The result models demonstrated robustness in situations with unbalanced data and improved detection performance as measured by metrics.

There are still significant obstacles to be addressed despite the progress made in ML and DL for IoT stack detection. Real-time processing and resource limitations are difficult for many approaches to balance. The creation of reliable, universal solutions is further hampered by reliance on labelled data and a lack of diversity in datasets. Although new methods, such as hybrid and generative models, exhibit potential [36, 37], they are still not yet ready for widespread use. Furthermore, it is uncommon for ML and DL techniques to be fully integrated, with a significant gap in the area.

III. METHODOLOGY

In this section, we mentioned the data collection source. In this study, we utilised multiple sources to download relevant articles, international conference proceedings, and book chapters; the details are in Table 2.

TABLE II
DETAILS OF THE DATA COLLECTION

Data Source	2020	2021	2022	2023	2024	2025
IEEE	04	03	05	06	08	06
Elsevier	03	04	06	04	03	06
ScienceDirect	02	05	07	05	04	07
Google Scholar	03	04	03	04	03	08

Table 1 shows that the last five years' studies have been downloaded from multiple online databases, such as the IEEE, Elsevier, ScienceDirect, and Google Scholar. Figure 3 presents the Data collection and database names for the research.

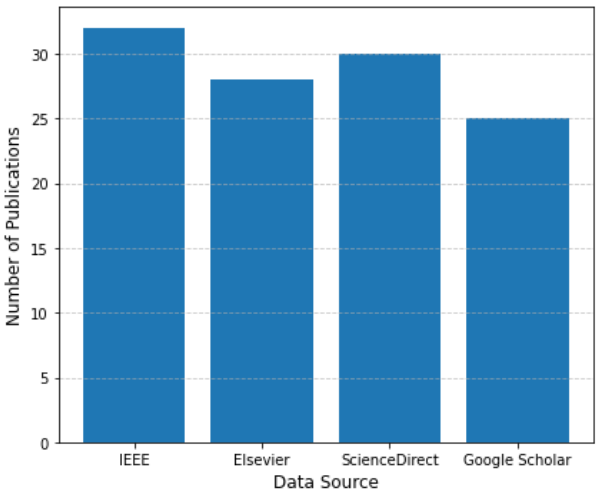

Fig. 3. Data collection and database names for the research

This bar chart presents the data collection and the databases' names, used in this article, such as IEEE, Elsevier, ScienceDirect, and Google Scholar, which were collected from 2020 to 2025 for this study. Figure 4: Flowchart of the data collection process for the proposed model.

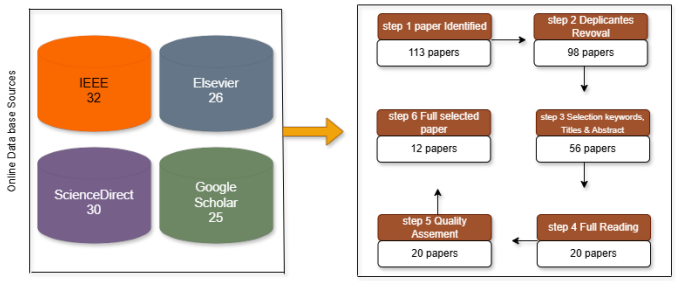

Fig. 4. Flowchart of the data collection process for the proposed model

A. Conventional neural network

In this section, we present the different authors' contributions about CNN. In this model, it has been proven that decision-making results significantly and effectively. [38, 39], these developments have opened new doors and are supporting the reach of solutions in the CNN is transforming age, including multiple industries. Furthermore, it plays a significant role in security and offers strong time detection tools for threats [40]. These types of multiple convolutional layers consist of a nonlinear activation function and fully connected layers that permit the capture of complex patterns and textures in images, making them specifically well-suited for visual data interpretation applications. Figure 5 presents the convolutional neural network.

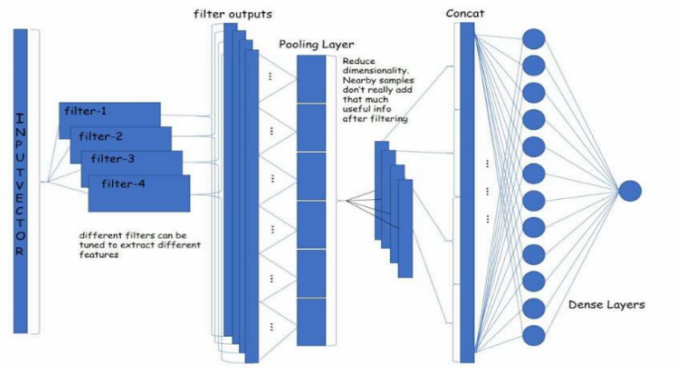

Fig. 5. Convolutional neural network

B. LSTM

The LSTM classifier uses AI-based models to improve the model's accuracy. The authors have applied the LSTM classifiers in their research studies and have achieved the required accuracy in different models using LSTM, and have given limitations that need to be enhanced to improve model results [41]. The proposed model received a 97% accuracy [42]. Getting the evaluation of the LSTM prediction accuracy, for this root mean-square logarithmic error has been chosen [43]. The CNN-LSTM model has been chosen as a novel method for an inherent IoT environment in dealing with spatial and temporal components. Figure 5: Overview of the LSTM architecture adopted from studies.

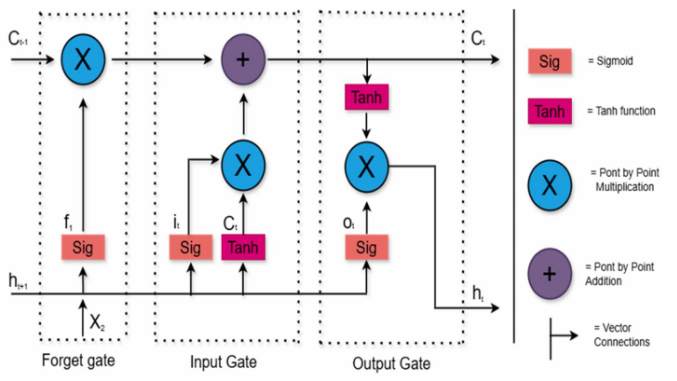

Fig. 6. Overview of the LSTM architecture adopted from studies

C. Dataset

We have collected the IoT-23 dataset [44], which comprises the collected data from open sources of various network traffic statistics from three innocuous IoT devices and twenty Raspberry Pi devices infected with malware. The dataset divides traffic into 10 different labels, each of which represents one benign case and nine attack scenarios. This dataset was used in our study to create a system that uses neural networks to classify DDoS attacks into two categories: harmful and benign[39]. This dataset was used in our study to build an improved detection model into two categories: benign and harmful. Table 3 presents the summary dataset's attacks.

TABLE III
SUMMARY DATASET'S ATTACKS

Classes	No of Samples
Benign	443402
DDoS	144,662
PartOfAHorizontalPortScan	144,662
Okiru	144,662
Attacks	9398
File download	18

D. Data preprocessing

The IoT-23 dataset was preprocessed to prepare it for modelling. We merged 500,000 benign samples with 44,662 examples each from the PartO Horizontal PortScan, Okiru, and DDoS classes, together with low-frequency labels. We divided the dataset into training, validation, and testing sets 60%, 20% and for binary and multiclass classification. Figure 6 presents a binary classification flowchart.

Algorithm 1: DDoS attack in a web application

Input HTTP request data and build a DDoS attack block (payload)
Output: malicious request with decreased DDoS attack
1: BEGIN
2:True: malicious request with illegitimately decreased DDoS
3:If
4:web_app_DDoS = 0,
5: web_app_DDoS = 0,
6: Infinite_DDoS limited to 522, &&
7: sqli_recalculate_sqli = null, then
8: mal_request select the parent
9: Attack is instigated
10: Else
11: False: request = begin
12: Until the decreased DDoS attack is launched
13: web_app = attacked
14: END

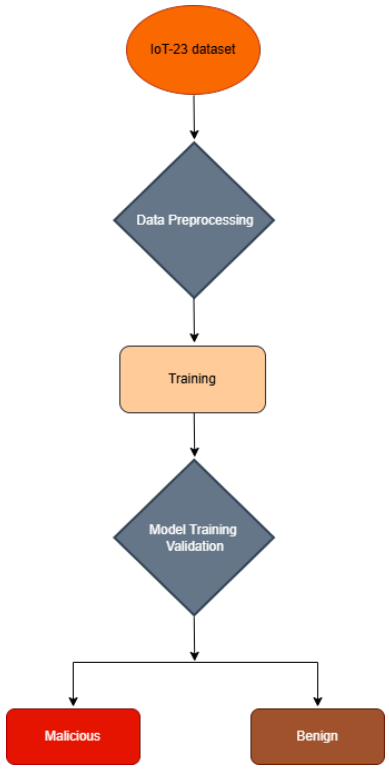

Fig. 7. Binary classification flowchart

Algorithm 2: BERT-LSTM -LGBM Preparation for the Model

Result: Trained model parameter Pr
Input: Set all dataset [z1,z2,z3,.....zy] in IoT-23 LGBM data pool
Output: prepared, pre-processed, feature-engineered IoT-23 dataset, DDoS HTTP
1: BEGIN for z belonging to IoT-23 dataset, LGBM, do
2:Import: panadas as 'pd', && numpy as 'as',&& cvs
3: Load: IoT-23 dataset,LGBM [z1,z2,z3,.....zy]
4. END
5. BEGIN for all x belonging to IoT-23 dataset, LGBM, do
6. Data = pd.read_csv ('payload_rpl.csv',r)
8.(dp.data = = empty || empty||undefiened
9. Dp.data = = NaaN || dp.data = = 1
10. if (f1.data = = fn.data)
11. Fn = drop
12. Else
13.Dp.data = value && f.data = intact
14. If (data.dtpes ≠ numerical)
15. Data.dtypes = oneHotEncode
16. Else
17. Data.dtypes = num
18. Check data. isnull ()
19. True if dp.data = = True
20. For (data.data.isnull() = = True
21.Data = oneHotEncode
22. Until
23. Return preprocessed, prepared, IoT-23 dataset, DDoS HTTP
24. EN

E. Proposed framework

Presents the architecture in Figure 7, a powerful combination of two models, CNN+LSTM+LGBM. The ML-based firewall enhances traditional firewall using ML to analyze network traffic and identify both known and unknown threats through static rule sets. The features extracted from the CNN model, which are present in Figure 8, are used as the input to the LSTM model. The output of the LSTM model identifies the malicious features, which will be classified using the LGBM for the final classification. This can take preventive measures against the malicious devices and their activities. Figure 8 presents the proposed architecture.

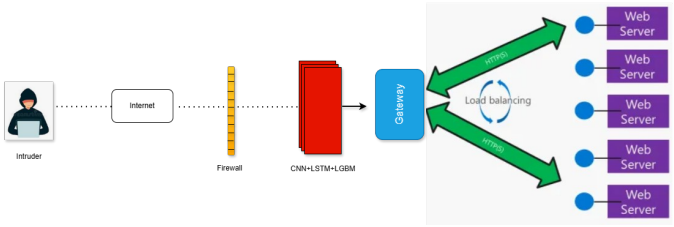

Fig. 8. Proposed architecture

In this figure, there is an extra layer, which is working, namely CNN+LSTM. In this layer, LGBM provides the final classification, and the results go through the gateway for further processing of the data.

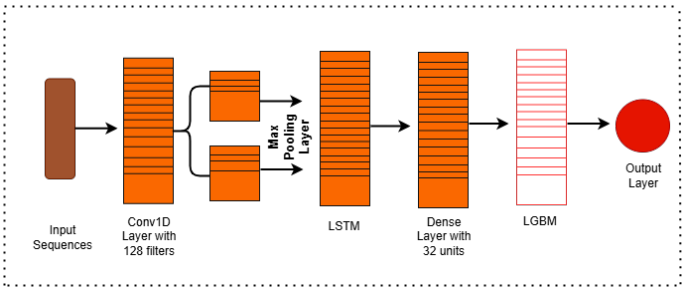

Fig. 9. Hybrid proposed model

We have added a layer in our proposed LSTM model of temporal awareness to the feature extraction process. Temporal dependencies in the data are captured, enabling the model to better detect and react to emergency threats, and it can learn over time. Furthermore, the proposed LGBM got the required classifications, specifically when it deals with malicious activities.

$$\text{Packet Rate} = \frac{\text{Total Packets}}{\text{Flow Duration}} \tag{1}$$

$$\text{TP Rate} \Rightarrow \text{Better DDoS Detection} \tag{2}$$

$$\text{Precision} \Rightarrow \text{Low False Alarms} \tag{3}$$

$$\text{F1-Score} \Rightarrow \text{Strong DDoS Detection Performance} \tag{4}$$

IV. RESULTS

The CNN, BiLSTM, and DNN were used to classify network traffic as either benign. We got excellent performance in binary and multi-class classification tasks, which is further supported by the confusion matrices shown in Figures 10 and 11. This demonstrates how well the hybrid CNN–BiLSTM–LGBM model generalizes. Figure 9 presents training and validation metrics.

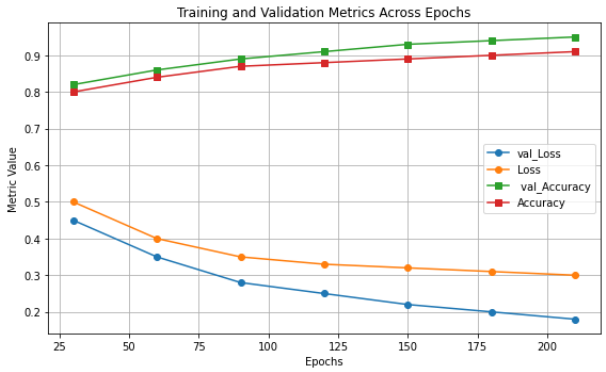

Fig. 10. metrics of the training and validation

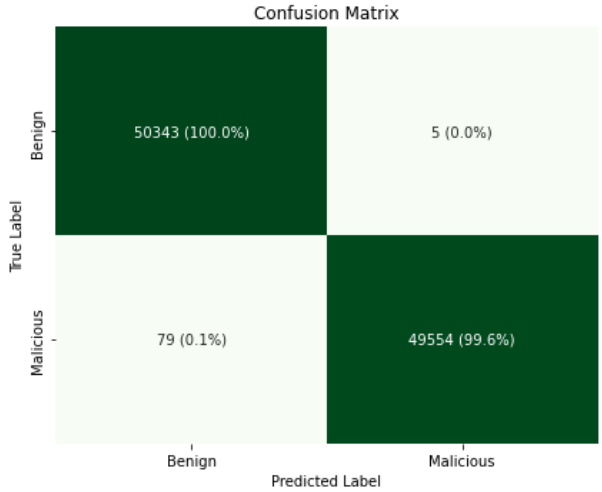

Fig. 11. Binary classification confusion matrix

Table overview of the CNN-BiSTM-LGBM model using the IoT-23 dataset for binary classification. Figure 10: Binary classification confusion matrix and Figure 11: Confusion matrix for multi-class classification. Table 4 presents the summary of the class. Table 5 presents the binary classification of the model using the IoT-23 dataset.

TABLE IV
SUMMARY OF THE CLASS

Class	Accuracy	Recall	Precision	F1 Score
Benign	99.95%	99.99%	99.90%	99.95%
Malicious	99.95%	99.85%	99.96%	99.95%

TABLE V
BINARY CLASSIFICATION OF THE MODEL USING IOT-23 DATASET

Class	Accuracy	Recall	Precision	F1 Score
Benign	99.98%	99.99%	99.96%	99.98%
DDoS	99.98%	99.97%	99.99	99.95
Okiru	99.98%	99.99%	100.0%	100.0%
PortScan	99.98%	99.98%	99.98	99.98%

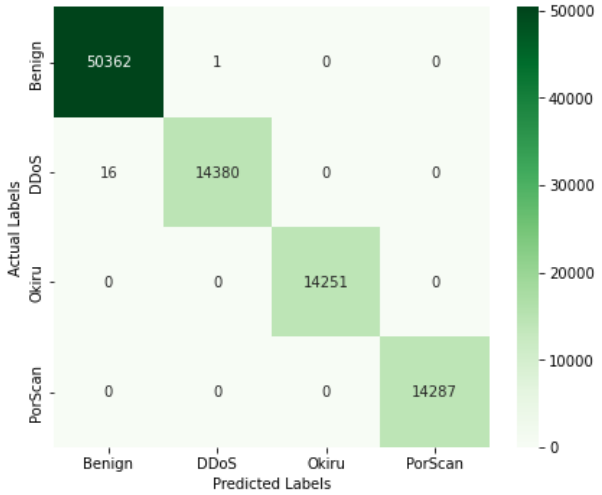

Fig. 12. Confusion matrix of multi-class classification

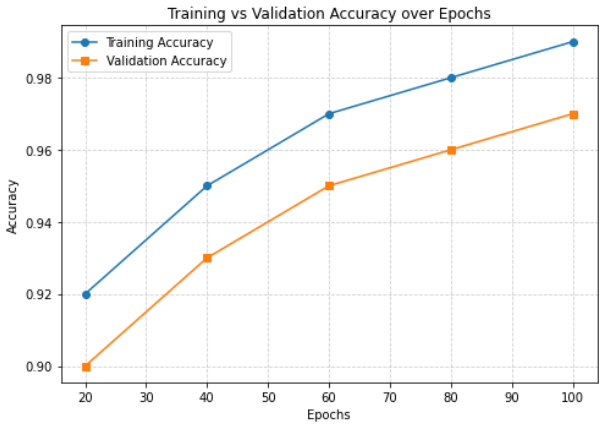

Fig. 13. Training vs validation accuracy epochs

V. DISCUSSION

1 We presented an analysis of our proposed model's performance in detecting DDoS attacks within IoT networks. which cover a broad range of attack situations and types. Furthermore, Table 6 gives a detailed comparison of the dataset used in this study with the dataset.

TABLE VI
COMPARISON OF OUR MODEL WITH THE ADVANCED STUDY

Study	Dataset	Model	Accuracy
31	Edge-IIoTset	DNN	94%
25	IoT-23	CNN and LSTM	96%
30	N-BaIoT CICIDS2017	CNN–LSTM	99% 99%
Proposed model	IoT-23	CNN–BiLSTM–LGBM	99.8%

Table 6 presents a comparison of our model with advanced studies with five relevant models, which are advanced in the software market. Figure 12 presents the model accuracy comparison.

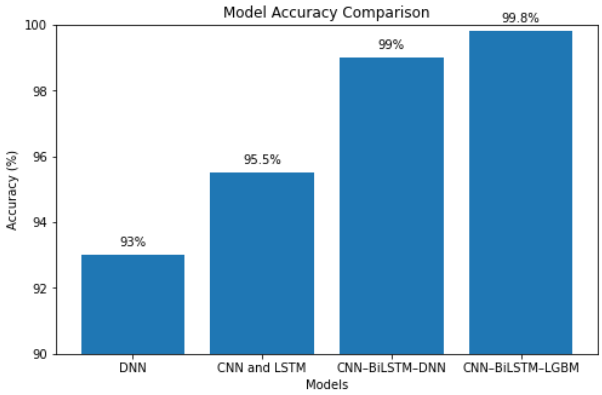

Fig. 14. Model accuracy comparison

This figure shows the comparison of model accuracy, such as DNN, 93%, CNN, and LSTM, 95.5%, CNN-BiLSTM-DNN, 99%, and our proposed model got the highest results, CNN-BiLSTM-LGBM, 99.8%, as compared to the existing models Liu, Y. and Dai, Y., 2024.

1. Conclusion In conclusion, we carefully assess the efficiency of the BERT-LSTM-LGBM model on the datasets. Our research focuses on the BERT-LSTM-LGBM model's subtle capabilities, specifically, its proficiency at extracting intricate features. This model presents high results in DDoS attack detection with the IoT environment using the IoT-23 dataset; in this regard, we got the required model's performance. We have developed a unique model for IoT DDoS attack detection to provide effective security measures in the IoT domain.

VI. ABBREVIATIONS

IoT: Internet of Things
DDoS: Distributed denial of services
ML: Machine Learning
BERT: Bidirectional Encoder Representations from Transformers
LGBM: Light Gradient Boosting Machine
DL: Deep Learning

References

[1] R. Pandey and J. P. Singh, "BERT-LSTM model for sarcasm detection in code-mixed social media post," *Journal of Intelligent Information Systems*, vol. 60, no. 1, pp. 235-254, 2023. doi: 10.1007/s10844-022-00755-z

[2] A. Ezen-Can, "A comparison of LSTM and BERT for small corpus," Cornell University, Tech. Rep., 2020.

[3] M. Abbas, T. I. Khan, and F. A. Jam, "Avoid excessive usage: Examining the motivations and outcomes of generative artificial intelligence usage among students," *Journal of Academic Ethics*, vol. 23, no. 4, pp. 2423–2442, 2025.

[4] K. Kaur and P. Kaur, "Improving BERT model for requirements classification by bidirectional LSTM-CNN deep model," *Computers and Electrical Engineering*, vol. 108, p. 108699, 2023. doi: https://doi.org/10.1016/j.compeleceng.2023.108699

[5] C. Sriharsha, S. Rithwik, K. P. Prahlad, and L. S. Nair, "Intelligent learning assistant using BERT and LSTM," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2021.

[6] A. Kumar, J. P. Singh, and A. K. Singh, "Explainable BERT-LSTM stacking for sentiment analysis of COVID-19 vaccination," *IEEE Transactions on Computational Social Systems*, vol. 12, no. 3, pp. 1296-1306, 2023. doi: 10.1109/TCSS.2023.3329664.

[7] S. Jamshidi, M. Mohammadi, S. Bagheri, H. E. Najafabadi, A. Rezvanian, M. Gheisari, M. Ghaderzadeh, A. S. Shahabi, and Z. Wu, "Effective text classification using BERT, MTM LSTM, and DT," *Data & Knowledge Engineering*, vol. 151, p. 102306, 2024. doi: https://doi.org/10.1016/j.datak.2024.102306

[8] A. Noorian, A. Harounabadi, and M. Hazratifard, "A sequential neural recommendation system exploiting BERT and LSTM on social media posts," *Complex & Intelligent Systems*, vol. 10, no. 1, pp. 721-744, 2024. doi: 10.1007/s40747-023-01191-4

[9] N. Mandela and F. Etyang, "Comparative analysis of deep learning models for effective Denial of Service (DoS) attack detection in network security," *Journal of Electrical Systems and Information Technology*, vol. 12, no. 1, p. 73, 2025.

[10] Y. Liu and Y. Dai, "Deep learning in cybersecurity: A hybrid BERT-LSTM network for SQL injection attack detection," *IET Information Security*, vol. 2024, no. 1, p. 5565950, 2024.

[11] Y. E. Seyyar, A. G. Yavuz, and H. M. Ünver, "An attack detection framework based on BERT and deep learning," *IEEE Access*, vol. 10, pp. 68 633-68 644, 2022. doi: 10.1109/ACCESS.2022.3185748

[12] A. Bano, S. H. Hamzah, and E. B. Hafiz, "Interplay between gender & and influencing factors to determine physical activity of school children," *Journal of Management Practices, Humanities and Social Sciences*, vol. 9, no. 2, pp. 120-135, 2025.

[13] A. Gupta and D. C. Misra, "Hybrid IoT security model with integration of LSTM, BERT, ROBERTA and transform learning for attack classification," *International Journal of Information Technology*, vol. 17, no. 8, pp. 4505-4522, 2025. doi: https://doi.org/10.1007/s41870-025-02672-0

[14] M. N. Swileh and S. Zhang, "Unseen attack detection in software-defined networking using a BERT-based large language model," *AI*, vol. 6, no. 7, p. 154, 2025. doi: https://doi.org/10.3390/ai6070154

[15] M. Marali, R. Dhanalakshmi, and N. Rajagopalan, "A hybrid transformer-based BERT and LSTM approach for vulnerability classification problems," *International Journal of Mathematics in Operational Research*, vol. 28, no. 3, pp. 275-295, 2024.

[16] B. G. Bokolo, L. Chen, and Q. Liu, "Detection of web-attack using DistilBERT, RNN, and LSTM," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2023, pp. 1-6.

[17] A. Alwan, A. Shah, A. A. A. R. Alwan, and S. U. A. Laghari, "Evaluating machine learning models for real-time IoT intrusion detection: A comparative study with RTSS analysis," *Journal of ICT, Design, Engineering and Technological Science*, vol. 8, no. 2, pp. 1-5, 2024.

[18] Y. Yang and X. Peng, "BERT-based network for intrusion detection system," *EURASIP Journal on Information Security*, vol. 2025, no. 1, p. 11, 2025. doi: https://doi.org/10.1186/s13635-025-00191-w

[19] A. S. Shah, A. Maqsood, A. Shah, M. A. K. Khani, J. Anjum, and S. Zafar, "Enhanced airport operations: Automated baggage drop-off and boarding pass generation for travelers," *Journal of Advances in Technology and Engineering Research*, vol. 10, no. 2, pp. 1-6, 2024.

[20] S. Dey, P. S. Kate, V. Upadhyay, and A. Vaish, "A transformer-based approach for ddos attack detection in iot networks," Cornell University, Tech. Rep., 2025.

[21] Z. Ali, W. Tiberti, A. Marotta, and D. Cassioli, "Empowering network security: Bert transformer learning approach and mlp for intrusion detection in imbalanced network traffic," *IEEE Access*, vol. 12, pp. 137 618-137 633, 2024. doi: doi: 10.1109/ACCESS.2024.3465045

[22] A. Kachavimath, S. Vaishyar, A. Chugani, P. Singh, and S. A. More, "DDoS attacks detection in SDN using multi-feature selection approach and LLMs," in *International Conference on Inventive Communication and Computational Technologies*. Springer, 2025.

[23] Y. E. Seyyar, A. G. Yavuz, and H. M. Ünver, "Detection of web attacks using the BERT model," in *2022 30th Signal Processing and Communications Applications Conference (SIU)*. IEEE, 2022.

[24] I. A. Shah, "Privacy and security challenges in Unmanned Aerial Vehicles (UAVs)," *Cybersecurity in the Transportation Industry*, pp. 93-115, 2024.

[25] S. Sattarpour, A. Barati, and H. Barati, "EBIDS: Efficient BERT-based intrusion detection system in the network and application layers of IoT," *Cluster Computing*, vol. 28, no. 2, p. 138, 2025. doi: https://doi.org/10.1007/s10586-024-04775-y

[26] I. A. Shah, Q. Sial, and S. Fateh, *Generative AI Techniques for Sustainability in Healthcare Security*. IGI Global, 2024.

[27] I. A. Shah, N. Jhanjhi, and S. N. Brohi, "Proposing model for classification of malicious SQLi code using machine learning approach," in *2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR)*. IEEE, 2024, pp. 1-6.

[28] S. AboulEla and R. Kashef, "Enhancing IOT intrusion detection with transformer-based network traffic classification," in *2025 IEEE International systems Conference (SysCon)*. IEEE, 2025.

[29] Q. Sial, I. A. Shah, and N. Jhanjhi, "Generative AI applications for enhancing medical training," in *Generative AI techniques for sustainability in healthcare security*. IGI Global Scientific Publishing, 2025.

[30] S. Fateh, Q. Sial, S. H. Dar, I. A. Shah, and A. Rani, "Smart healthcare system in industry 4.0," in *Advances in Computational Intelligence for the Healthcare Industry 4.0*. IGI Global Scientific Publishing, 2024.

[31] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, 2019.

[32] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in IoT architectures," in *Bodynets*, 2012.

[33] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636-1675, 2018. doi: 10.1109/COMST.2018.287497

[34] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, 2021. doi: https://doi.org/10.3390/su13169463

[35] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT threats: Survey of risks and vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, 2024. doi: https://doi.org/10.3390/fi16110389

[36] P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," in *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2017.

[37] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721-82 743, 2019. doi: doi: 10.1109/ACCESS.2019.2924045

[38] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, "Survey on IoT: Security threats and applications," *Journal of Robotics and Control (JRC)*, vol. 2, no. 1, pp. 42-46, 2021.

[39] O. G. Dorobantu and S. Halunga, "Security threats in IoT," in *2020 International Symposium on Electronics and Telecommunications (ISETC)*. IEEE, 2020.

[40] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "Iot threat detection advances, challenges and future directions," in *2020 workshop on emerging technologies for security in IoT (ETSecIoT)*. IEEE, 2020, pp. 22-29.

[41] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, "Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," *International Journal of Communication Systems*, vol. 33, no. 12, p. e4443, 2020. doi: https://doi.org/10.1002/dac.4443

[42] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," Cornell University, Tech. Rep., 2018.

[43] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "A new approach to investigate IoT threats based on a four layer model," in *2016 13th international conference on new technologies for distributed systems (NOTERE)*. IEEE, 2016.

[44] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber security threats to IoT applications and service domains," *Wireless Personal Communications*, vol. 95, no. 1, pp. 169-185, 2017.