A Hybrid Deep Learning-Powered SDN-Based Intrusion Detection Architecture for Cognitive IoT Security

Tejaswini Panse
Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India
tejaswini.deshmukh@gmail.com

Venugopal Gaddam
Department of Computer Science and Engineering (AI & ML), B. V. Raju Institute of Technology, Narsapur, Hyderabad, Telangana, India
venugopal.gaddam@gmail.com (corresponding author)

Bhima Sankar Manthina
Department of Electronics and Communication Engineering, IIIT Hyderabad, Telangana, India
sankar.bhima@gmail.com

Hanumantha Rao Battu
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Vaddeswaram, Guntur, Andhra Pradesh, India
hanuma9999@yahoo.com

Pamarthi Sunitha
Department of Electronics and Communication Engineering, Aditya University, Surampalem, Andhra Pradesh, India
sunitha4949@gmail.com

Vemuri Sailaja
Department of Electronics and Communication Engineering, Pragati Engineering College, Surampalem, Andhra Pradesh, India
sailajagiet@gmail.com

Received: 4 June 2025 | Revised: 21 June 2025 | Accepted: 9 July 2025

 DOI: https://doi.org/10.48084/etasr.12564

ABSTRACT

Various sectors, including smart homes, healthcare, transportation, agriculture, and manufacturing, derive significant advantages from Internet of Things (IoT) technology. This innovative method of interacting with the world enhances efficiency, convenience, and productivity. Nonetheless, it raises concerns regarding security, privacy, and data governance. This article introduces a cognitive hybrid Deep Learning (DL) approach, facilitated by Software-Defined Networking (SDN), to address security concerns in IoT networks through intrusion detection. The principal objective of this methodology is to consistently and effectively detect cybersecurity risks within the IoT ecosystem. Inspired by the cognitive computing paradigm, the proposed system can analyze, comprehend, and respond to diverse traffic targeting IoT devices. The suggested model is trained and evaluated utilizing the advanced N-BaIoT and CICDDoS2019 datasets. The experimental results exhibit a high degree of accuracy, producing an acceptable false positive rate alongside a tolerable testing duration. Moreover, the architecture takes into account the constrained resources of IoT devices, guaranteeing they are not excessively taxed during the process. The proposed

model achieved an accuracy rate of 99.86%, precision of 99.96%, recall of 99.903%, and F1-Score of 99.93%. The proposed model surpassed existing hybrid DL methods.

Keywords-intrusion detection; cognitive system; Internet of Things (IoT); cyber attacks; Deep Learning (DL); Machine Learning (ML); Software-Defined Networking (SDN)

I. INTRODUCTION

Smart homes, industry, and healthcare are just a few examples of the many practical applications that benefit from the Internet of Things (IoT), a collection of protocols that enables the interconnection of various computing devices and sensors. IoT has revolutionized many fields and aspects of everyday life by enabling the interconnection of billions of devices and generating an unprecedented amount of data [1]. Over the last ten years, IoT has grown into a new paradigm in smart technology, with the potential to revolutionize industrial systems. Several intelligent IoT communication protocols have been created to enable the intelligent communication of commonplace items [2]. For example, in a smart home, IoT devices can remotely control lighting, temperature, and security, whereas in a factory, IoT sensors can monitor machine health and provide maintenance recommendations. The number of IoT devices in use today exceeds eight billion, with projections indicating it will reach forty-one billion by 2027 [3, 4]. Substantial economic gains and automation have emerged from the IoT revolution, demonstrating its ubiquitous impact on society. Real-time data collection and analysis through IoT enable machines to make smarter and more accurate decisions, reducing human intervention and paving the way for autonomous operations [5].

IoT enables the development of time-sensitive platforms and meets the demands of real-time, low-latency systems. Interfacing with IoT networks is made possible by Software-Defined Networking (SDN), open-flow protocols, and the IEEE 802.1 time-sensitive network. SDN provides centralized control and programmability, which is essential for dynamic and intelligent intrusion detection across distributed IoT nodes.

An essential concept in IoT is the traditional three-tiered architecture, which provides a simplified and effective framework for organizing the various components of an IoT network. Data are exchanged across three layers: the perception, network, and application layers. The perception layer is responsible for sensing and collecting environmental data. The network layer connects the perception and application layers, transmitting data using various protocols and network elements. The application layer hosts use-case-specific applications [6].

IoT systems face numerous security challenges due to their size, diversity, limited resources, and global accessibility. There are many architectural and design challenges in IoT systems with numerous connected devices [7, 8]. These challenges include latency, security, privacy, and network coverage issues. Advanced Persistent Threats (APTs) and Distributed Denial-of-Service (DDoS) attacks are among the most common ways attackers compromise vulnerable systems. Although multiple security mechanisms exist, new attacks often circumvent them, highlighting the need for a comprehensive system that monitors devices, detects intrusions, and makes intelligent decisions.

Existing Machine Learning (ML) approaches for IoT intrusion detection can misidentify important data patterns or misclassify them, resulting in false positives. Traditional intrusion detection technologies are implemented at the infrastructure level to protect devices [9]. These may include firewalls or physical Intrusion Detection Systems (IDSs). Collected data, such as byte transfer, connection duration, request rate, and error rate, provide limited insight into cyberattacks. Consequently, traditional ML methods fall short in identifying attacks in real-world scenarios.

Deep Learning (DL) offers a potential solution, improving prediction and classification accuracy while providing a more comprehensive understanding of data through multiple processing layers. DL models can automatically learn complex patterns in high-dimensional data, including temporal behaviors, without manual feature engineering, making them suitable for real-time intrusion detection in IoT. Numerous DL-based IoT security mechanisms have been proposed [10]. DL has proven effective for network intrusion detection, particularly given the diversity of attacks and the complexity of network environments [11]. However, IoT devices' limited power, computational capacity, and storage make implementing complex DL models challenging. Thus, it is crucial to deploy an IDS that is efficient, cost-effective, and adaptable.

We propose an SDN-enabled hybrid-DL cognitive model for detecting cyberattacks in the IoT ecosystem, with the goals of improving system efficiency and addressing security challenges. SDN is a cutting-edge method of networking that offers greater adaptability compared to older methods. It allows centralized configuration and control, simplifying network management and separating the data and control planes. However, if the controller is attacked, the entire network will become compromised due to its logically centralized control attribute. For this reason, SDN intrusion detection is crucial [12]. SDN-enabled architectures simplify network management in diverse, dynamic IoT environments, optimize resource usage for low-capacity devices, and allow efficient, effective detection. Integrating SDN with AI-based security enhances security by leveraging AI programmability and exponential growth [13]. Finally, Cognitive computing aims to emulate human reasoning and decision-making using Artificial Intelligence (AI) and DL algorithms.

II. RELATED WORK

Several research efforts have investigated intrusion detection in IoT environments. A lightweight DL-Bidirectional Long Short-Term Memory (BiLSTM) model was proposed in [11] to identify IoT threats by combining DNN and BiLSTM methods. The study used the CICIDS2017, N-BaIoT, and CICIoT2023 datasets, applying IPCA for feature reduction and

dynamic quantization to minimize computational cost. The CICIoT2023 dataset achieved the best attack detection accuracy of 93.13 %.

A DL-driven vulnerability inspection model using three classifiers, including CNN, DNN, and RNN, was presented in [14], evaluated on KDDCup99, KDD, and UNSW-NB15 datasets. This approach successfully prevented multiple security breaches. In [15], the authors introduced real-time edge anomaly detection to reduce communication costs and bandwidth, employing Spark distributed processing, VCNN modules, dropout, hidden Long Short-Term Memory (LSTM) layers, and Mayfy optimizers. Their SDN-based intelligent threat detection achieved 97.39% accuracy on UNSW-NB15 and UNSW_BOT_IoT datasets.

Authors in [16] developed RepuTE, an IoT DoS/DDoS and Sybil detection program. RepuTe preprocesses live IoT traffic in the fog layer and applies extra-trees, K-Nearest Neighbors (KNN), and quadratic discriminant analysis for traffic analysis. Experiments with CICDDoS2019, TON_IoT, and NSL-KDD datasets yielded an attack detection accuracy of 99.9851 % on TON_IoT_DDoS. Similarly, authors in [17] employed transfer learning for image-based threat analysis in cloud IoT devices using CNNs, trained on CICIDS2017 and CICIDS2018 datasets, achieving high detection accuracy.

In [18], researchers introduced CICIoT2023, a large dataset covering 33 IoT attack types grouped into seven categories, including DDoS, brute force, spoofing, and Mirai. An LSTM-autoencoder model for Industrial Internet of Things (IIoT) threat detection was explored in [19], trained on GP and SWaT datasets. Although effective, it produced many false positives. The two-stage anomaly detection method P2ADF was proposed in [20], combining feature reduction, a meta-classifier (XGBoost), and three base learners (AdaBoost, LR, KNN). It achieved 99.98% DDoS detection accuracy on CICDDoS2019 and 99.95% on TON_IoT.

A boosting-based IIoT intrusion detection model using XGB, RF, ET, and ADB ensemble classifiers was introduced in [21], with experiments on TON_IoT telemetry data. In [22], a CNN classifier was trained on the BoT-IoT dataset, achieving 92.46% accuracy but with a high false positive rate. A CNN-BiLSTM hybrid model for IoT intrusion detection was developed in [23], achieving 98.27% accuracy on the NSL-KDD dataset.

DL-based IIoT bot detection using a cascade forward-back propagation neural network was proposed in [24], trained on BoT-IoT, UNSW-NB15, CICIDS2018, and TON_IoT datasets. However, the framework required significant computational resources. Finally, an ensemble IDS combining RF, ET, and DNN was presented in [25], evaluated on NSL-KDD, BoT-IoT, and CICIDS2018 datasets. The model achieved 98.21% accuracy on CICIDS2018, demonstrating strong efficacy.

III. PROPOSED METHOD

Over the past decade, SDN has emerged as the leading networking design and integration solution. By separating the control and data planes, SDN enhances flexibility and simplifies network management. The architecture consists of data, application, and control layers, interconnected through northbound and southbound Application Programming Interfaces (APIs). The northbound interface enables communication between controllers and applications, whereas southbound APIs manage the switching fabric, network virtualization protocols, and distributed networking devices. The control plane serves as a centralized, intelligent component responsible for data processing and decision-making [8], whereas the data plane consists of SDN agents and forwarding devices. This modular separation allows the framework to be easily expanded with additional modules.

This paper presents an IDS that leverages DL and SDN to detect intrusions in IoT environments. SDN provides flexible control and management of network resources through its full programmability and supports the addition and expansion of IoT devices within the data plane due to its total programmability. OpenFlow switches address heterogeneity between controllers and IoT devices during deployment and optimize device utilization without excessive resource consumption. The integration of SDN and IoT enables effective analysis of network data for attacks, threats, and unauthorized activities. The overall structure remains centralized and cost-effective, with IoT devices on the SDN data plane including sensors, smart devices, and wireless technologies. Figure 1 illustrates the overall architecture of the proposed method.

The neural network employs a hybrid BiLSTM-GRU architecture to analyze network traffic data. BiLSTM captures both forward and backward temporal dependencies, allowing the model to identify long-range contextual relationships and similar patterns within the input sequence [26]. The first recurrent layer processes the mirrored version of the input sequence, while the second layer handles the original sequence. Both layers feed into a single output layer. Gated Recurrent Unit (GRU) offers a simplified alternative to LSTM by using only an update and a reset gate, eliminating the need for a separate memory cell. This reduces computational complexity while maintaining performance comparable to LSTM in sequential modeling tasks, such as polyphonic music and voice signal analysis [27]. In some cases, GRUs even outperform LSTMs on smaller datasets. By combining the hidden state with its internal memory, GRU efficiently captures temporal dependencies in IoT network traffic, making it well-suited for intrusion detection.

In this study, the N-BaIoT dataset, containing real-time traffic from IoT devices such as the Danmini doorbell, Provision PT-737E security camera, and Ecobee thermostat, was used to evaluate attacks including Bashlite and Mirai [28]. In addition, the CICDDoS2019 dataset [29], which provides diverse DDoS scenarios in a realistic testbed, was employed to further assess the robustness of the proposed model.

Table I summarizes the hyperparameters used for training the hybrid BiLSTM-GRU model. The Adam optimizer was selected for its adaptive learning capabilities and effective handling of sparse gradients, with a learning rate of 0.001 to ensure stable convergence. A batch size of 64 was used to maximize GPU utilization without exceeding memory limits. The model was trained for 50 epochs to balance convergence and prevent overfitting. A dropout rate of 0.3 was applied after

recurrent layers to reduce neuron co-adaptation and improve generalization. Since the task involves multiple intrusion classes, the categorical cross-entropy loss function was applied, and the output layer provided probabilistic outputs for each class using Softmax activation. The BiLSTM and GRU layers use 128 and 64 units, respectively, to capture long-term dependencies and sequential behavior in network traffic data. These hyperparameters were optimized for model accuracy, precision, recall, and F1-score, which are the main evaluation metrics.

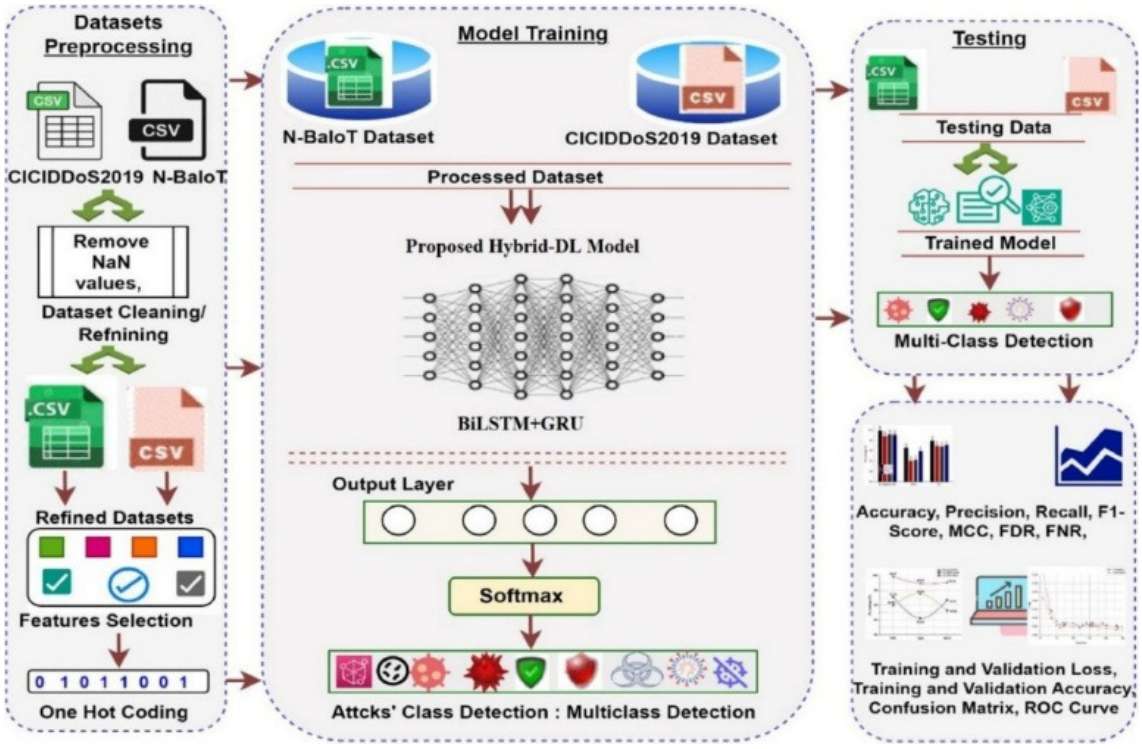

Fig. 1. Proposed hybrid BiLSTM-GRU framework for IoT network intrusion detection.

TABLE I. HYPERPARAMETERS USED FOR BILSTM-GRU MODEL TRAINING

Parameter	Value
Learning rate	0.001
Optimizer	Adam
Batch size	64
Number of epochs	50
Dropout rate	0.3
Loss function	Categorical cross-entropy
Activation function	Softmax (output layer)
BiLSTM units	128
GRU units	64
Return sequences	True (for first layers)
Evaluation metrics	Accuracy, precision, recall, F1-score

IV. RESULTS AND DISCUSSION

Evaluation metrics play a crucial role in assessing the success of ML and DL models. Depending on the specific problem and model, different metrics may be employed. Some metrics are particularly effective for regression tasks, whereas others are better suited for classification. Commonly utilized evaluation metrics include F1-score, accuracy, recall, and precision. Accuracy measures the ratio of correctly predicted instances to the total number of instances, precision measures the proportion of correctly predicted attacks among all predicted attacks, recall measures the proportion of actual attacks correctly identified, and F1-score provides the harmonic mean of precision and recall, balancing both metrics in a single value. The performance of our proposed IDS on both datasets is illustrated in Figures 2 and 3.

Fig. 2. Comparison of the proposed IDS with Cu-GRU+LSTM and Cu-GRU+DNN on the N-BaIoT dataset.

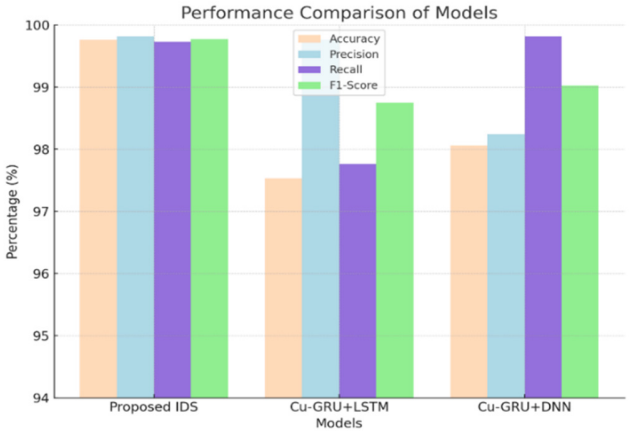

Fig. 3. Comparison of the proposed IDS with Cu-GRU+LSTM and Cu-GRU+DNN on the CICDDoS2019 dataset.

Figure 2 compares the proposed model with other models on the N-BaIoT dataset, whereas Figure 3 shows the comparison for the CICDDoS2019 dataset. In both cases, the proposed IDS outperforms existing benchmark approaches, including the Cu-GRU+LSTM and Cu-GRU+DNN classifiers, achieving superior accuracy and robustness.

Approximately 100,000 instances were processed with a 70:30 training-to-testing split. The proposed system effectively detects DDoS, Mirai, Bashlite, botnet attacks, and other common IoT network intrusions.

Figures 4(a) and 4(b) illustrate the training accuracy (Tacc) and validation accuracy (Vacc) of the proposed IDS for the N-BaIoT and CICDDoS2019 datasets, respectively. The results indicate that the model achieves high accuracy during both training and validation phases, with Vacc slightly exceeding Tacc in some cases.

Figures 5(a) and 5(b) show the corresponding training loss (Tloss) and validation loss (Vloss) metrics. The results indicate that the proposed IDS achieves minimal loss values for both datasets, with Vloss showing a clear advantage over Tloss.

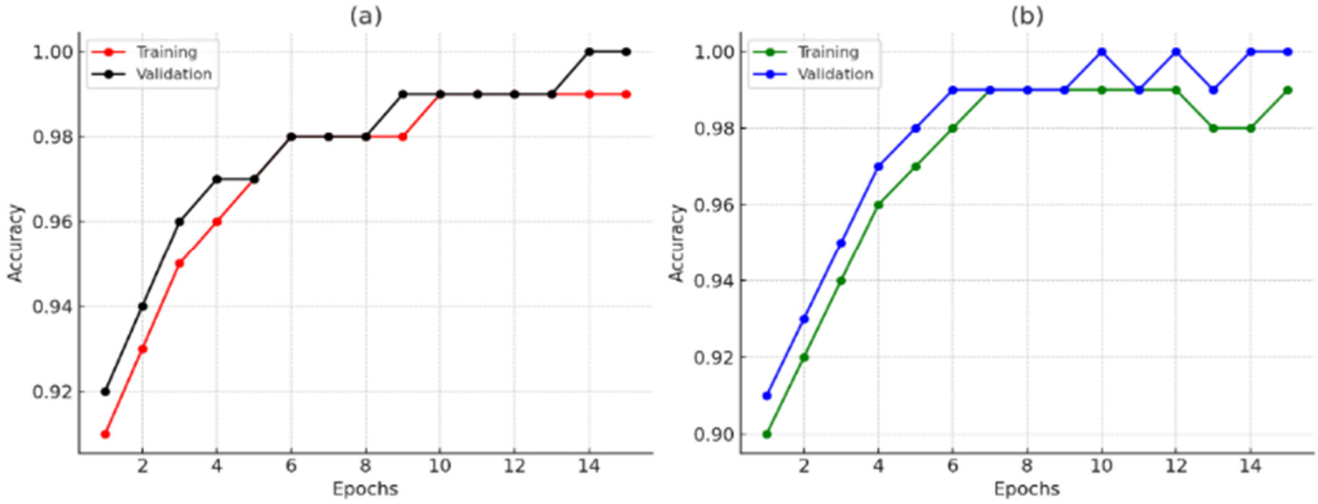

Fig. 4. Training and validation accuracy (Tacc and Vacc) of the proposed IDS: (a) N-BaIoT dataset, (b) CICDDoS2019 dataset.

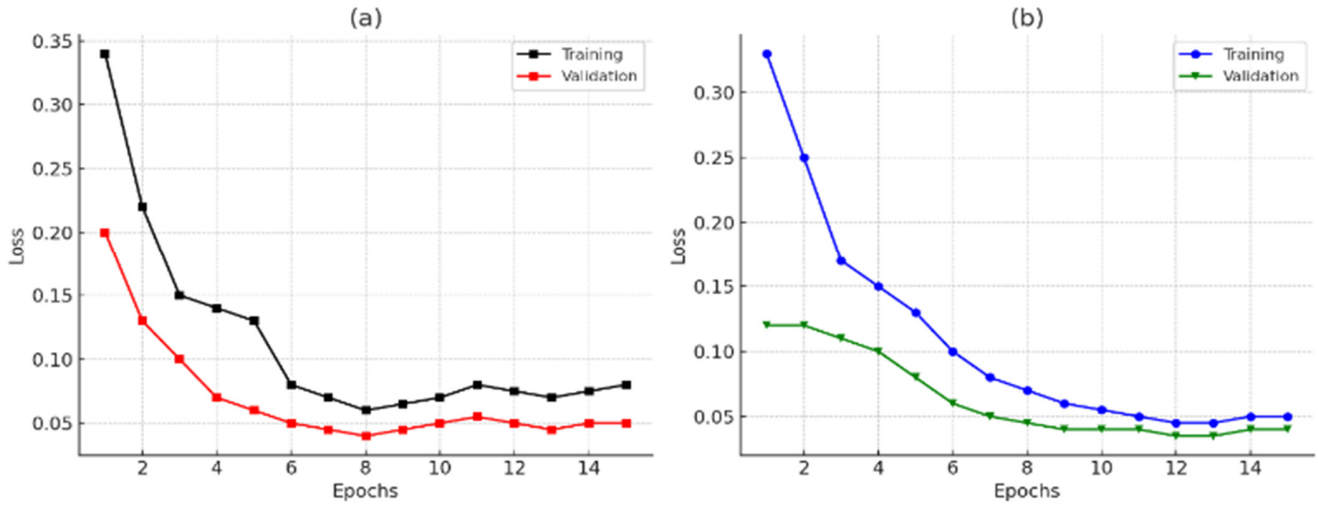

Fig. 5. Training and validation loss (Tloss and Vloss) of the proposed IDS: (a) N-BaIoT dataset, (b) CICDDoS2019 dataset.

V. CONCLUSION

The rapid growth of Internet of Things (IoT)-enabled devices has greatly expanded connectivity but also increased the risk of cybercrime and information compromise. Although the benefits and applications of IoT are well recognized, its extensive interconnectivity and heterogeneity make it highly vulnerable to security threats. This article presents the design and development of a cognitive Deep Learning (DL)-driven hybrid Software-Defined Networking (SDN) framework capable of detecting attacks in IoT devices. The proposed hybrid approach yields an accurate, cost-effective, and robust solution. Two additional classifiers, Cu-Gated Recurrent Unit + Long Short-Term Memory (Cu-GRU+LSTM) and Cu-Gated Recurrent Unit + Deep Neural Network (Cu-GRU+DNN), were trained and evaluated under the same conditions, and their results were compared with those of the proposed model. The proposed Intrusion Detection System (IDS) outperformed existing benchmark models by achieving high precision, accuracy, F1-score, and recall metrics. The computational complexity of the proposed IDS is significantly lower than that of other classifiers. We achieved an accuracy rate of 99.86%, with precision at 99.96%, recall at 99.90%, and F1-score at 99.93% on the N-BaIoT dataset.

While our proposed technique demonstrates strong performance, it possesses a limitation that we intend to address in future work. We aim to improve the model's capacity for detecting insider threats, thereby significantly increasing its effectiveness. Future work will also explore alternative DL techniques alongside advanced technologies, including three-way clustering, federated learning, and blockchain, to develop a novel IDS for analogous scenarios. Overall, SDN-enabled, DL-based IDSs offer a promising approach to strengthen the security of IoT systems.

REFERENCES

[1] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101162, https://doi.org/10.1016/j.iot.2024.101162.

[2] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83, Feb. 2023, https://doi.org/10.1016/j.jpdc.2022.10.002.

[3] J. Huang, H. Gao, S. Wan, and Y. Chen, "AoI-aware energy control and computation offloading for industrial IoT," *Future Generation Computer Systems*, vol. 139, pp. 29–37, Feb. 2023, https://doi.org/10.1016/j.future.2022.09.007.

[4] P. S. Rao, T. G. Krishna, and V. S. S. R. Muramalla, "Next-Gen Cybersecurity For Securing Towards Navigating the Future Guardians of the Digital Realm," *International Journal of Progressive Research in Engineering Management and Science*, vol. 3, no. 9, pp. 178–190, Sep. 2023, https://doi.org/10.58257/IJPREMS32006.

[5] M. Saied, S. Guirguis, and M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," *Engineering Applications of Artificial Intelligence*, vol. 127, no. A, Jan. 2024, Art. no. 107231, https://doi.org/10.1016/j.engappai.2023.107231.

[6] A. Vijay, M. Kasiselvanathan, P. Sridhar, R. Sharan, G. Surya, and M. Vishva Surjith, "Recent Developments in Designing Internet of Things Architectures," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing*, Salem, India, 2024, pp. 1575–1580, https://doi.org/10.1109/ICAAIC60222.2024.10574910.

[7] R. Pawar, A. P. Singh, and K. Sharma, "Mitigating Denial of Service Attacks in Software-Defined Networking Environments," in *2024 International Conference on Optimization Computing and Wireless Communication*, Debre Tabor, Ethiopia, 2024, pp. 1–5, https://doi.org/10.1109/ICOCWC60930.2024.10470827.

[8] D. Javeed, T. Gao, M. T. Khan, and D. Shoukat, "A Hybrid Intelligent Framework to Combat Sophisticated Threats in Secure Industries," *Sensors*, vol. 22, no. 4, Feb. 2022, Art. no. 1582, https://doi.org/10.3390/s22041582.

[9] D. A. M, V. Menon, S. Ezekiel, and P. Chaudhary, "Exploring the tractability of data fusion models for detecting anomalies in IoT-based dataset," in *Big Data V: Learning, Analytics, and Applications*, Orlando, FL, USA, 2023, pp. 82–89, https://doi.org/10.1117/12.2662802.

[10] V. Ravi, T. D. Pham, and M. Alazab, "Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things," *IEEE Internet of Things Magazine*, vol. 6, no. 2, pp. 50–54, Jun. 2023, https://doi.org/10.1109/IOTM.001.2300021.

[11] Z. Wang, H. Chen, S. Yang, X. Luo, D. Li, and J. Wang, "A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization," *PeerJ Computer Science*, vol. 9, Sep. 2023, Art. no. e1569, https://doi.org/10.7717/peerj-cs.1569.

[12] R. H. Altaie and H. K. Hoomod, "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16740–16743, Oct. 2024, https://doi.org/10.48084/etasr.7657.

[13] A. Chetouane and K. Karoui, "Risk based intrusion detection system in software defined networking," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 9, 2024, Art. no. e7988, https://doi.org/10.1002/cpe.7988.

[14] I. A. Kandhro *et al.*, "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," *IEEE Access*, vol. 11, pp. 9136–9148, 2023, https://doi.org/10.1109/ACCESS.2023.3238664.

[15] M. A. Ahmed and S. Alnatheer, "Intrusion Detection in a Digital Twin-Enabled Secure Industrial Internet of Things Environment for Industrial Sustainability," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21263–21269, Apr. 2025, https://doi.org/10.48084/etasr.10128.

[16] R. Verma and S. Chandra, "RepuTE: A soft voting ensemble learning framework for reputation-based attack detection in fog-IoT milieu," *Engineering Applications of Artificial Intelligence*, vol. 118, Feb. 2023, Art. no. 105670, https://doi.org/10.1016/j.engappai.2022.105670.

[17] O. D. Okey, D. C. Melgarejo, M. Saadi, R. L. Rosa, J. H. Kleinschmidt, and D. Z. Rodríguez, "Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN," *IEEE Access*, vol. 11, pp. 1023–1038, 2023, https://doi.org/10.1109/ACCESS.2022.3233775.

[18] A. H. A. Saq, A. Zainal, B. A. S. Al-Rimy, A. Alyami, and H. A. Abosaq, "Intrusion Detection in IoT using Gaussian Fuzzy Mutual Information-based Feature Selection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 17564–17571, Dec. 2024, https://doi.org/10.48084/etasr.8268.

[19] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," *Digital Communications and Networks*, vol. 9, no. 1, pp. 101–110, Feb. 2023, https://doi.org/10.1016/j.dcan.2022.09.008.

[20] J. Kaur, A. Agrawal, and R. A. Khan, "P2ADF: a privacy-preserving attack detection framework in fog-IoT environment," *International Journal of Information Security*, vol. 22, no. 4, pp. 749–762, Aug. 2023, https://doi.org/10.1007/s10207-023-00661-7.

[21] J. B. Awotunde *et al.*, "An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks," *Applied Sciences*, vol. 13, no. 4, Feb. 2023, Art. no. 2479, https://doi.org/10.3390/app13042479.

[22] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, Apr. 2022, Art. no. 107810, https://doi.org/10.1016/j.compeleceng.2022.107810.

[23] T. Acharya, A. Annamalai, and M. F. Chouikha, "Efficacy of CNN-Bidirectional LSTM Hybrid Model for Network-Based Anomaly Detection," in *2023 IEEE 13th Symposium on Computer Applications & Industrial Electronics*, Penang, Malaysia, 2023, pp. 348–353, https://doi.org/10.1109/ISCAIE57739.2023.10165088.

[24] P. L. S. Jayalaxmi, G. Kumar, R. Saha, M. Conti, T. Kim, and R. Thomas, "DeBot: A deep learning-based model for bot detection in industrial internet-of-things," *Computers and Electrical Engineering*, vol. 102, Sep. 2022, Art. no. 108214, https://doi.org/10.1016/j.compeleceng.2022.108214.

[25] C. A. de Souza, C. B. Westphall, and R. B. Machado, "Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments," *Computers & Electrical Engineering*, vol. 98, Mar. 2022, Art. no. 107694, https://doi.org/10.1016/j.compeleceng.2022.107694.

[26] S. Sivamohan and S. S. Sridhar, "An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework," *Neural Computing and Applications*, vol. 35, no. 15, pp. 11459–11475, May 2023, https://doi.org/10.1007/s00521-023-08319-0.

[27] G. R. Mode, P. Calyam, and K. A. Hoque, "False Data Injection Attacks in Internet of Things and Deep Learning enabled Predictive Analytics." arXiv, Dec. 13, 2019, https://doi.org/10.48550/arXiv.1910.01716.

[28] Y. Meidan *et al.*, "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, Jul. 2018, https://doi.org/10.1109/MPRV.2018.03367731.

[29] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology*, Chennai, India, 2019, pp. 1–8, https://doi.org/10.1109/CCST.2019.8888419.