A Survey of Advanced Intrusion Detection Systems Using Deep Learning in Cloud-Edge IoT Environments

Mohammed Assiri
Department of Mechanical Engineering, College of Engineering in Al-Kharj, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia
m.assiri@psau.edu.sa (corresponding author)

Received: 23 February 2026 | Revised: 14 March 2026 and 19 March 2026 | Accepted: 20 March 2026

 DOI: https://doi.org/10.48084/etasr.18328

ABSTRACT

The Internet of Things (IoT), Cloud Computing (CC), and Edge Computing (EC) represent an important shift from conventional structures on virtualized resource provisioning, introducing better adaptability and transparency for host systems, allowing cloud providers, on-premises sources, and edge nodes to fully realize the "everything-as-a-service" notion. This survey provides a comprehensive review of emerging cybersecurity threats in Cloud-Edge IoT systems and systematically examines AI-driven deep learning approaches for Intrusion Detection Systems (IDSs). The foundational concepts are first presented, including an overview of cybersecurity principles, cloud computing architecture, edge computing paradigms, and the advantages and challenges of IoT integration with cloud and edge infrastructures. Then, it further explores the role of ML and DL models in IDSs, highlighting architectures. A comparative analysis of recent studies is conducted based on datasets, performance metrics, scalability, computational efficiency, and robustness. Key findings are synthesized, identifying research gaps and evaluating practical deployment constraints. Finally, the survey outlines critical challenges and future research directions to support the development of secure, intelligent, and resilient Cloud-Edge IoT ecosystems.

Keywords-Internet of Things (IoT); cloud computing; edge computing; cybersecurity; deep learning; machine learning

I. INTRODUCTION

The growing prevalence of Internet of Things (IoT) devices and Edge Computing (EC) structures is revolutionizing digital infrastructures to enable more scalable, responsive, and decentralized edge processing [1]. These changes have inspired a broad range of applications, from smart transportation and active surveillance to intelligent healthcare and industrial automation, which are based on lower-latency data analytics and limited decision-making [2]. To reduce reliance on central servers, EC helps minimize bandwidth consumption, enhance response times, and protect data privacy by processing sensitive data closer to its source. However, as the number of interlinked devices continues to develop, so does the attack surface of these distribution models, revealing them to a broad range of advanced cyber threats [3]. In recent studies, edge and IoT systems are increasingly targeted by cyberattacks, with attackers leveraging heterogeneous structures and restricted security prevention against large-scale threats such as Denial of Service (DoS), Distributed Denial of Service (DDoS), and injection attacks.

The latest attacks, including ransomware, insider threats, and advanced persistent threats, remain a significant challenge to the security of cloud infrastructures [4]. These threats are made worse because the security in the cloud is shared between the client and the provider, often resulting in inadequate protection. Furthermore, the distribution and highly scalable nature of Cloud Computing (CC) models make conventional security solutions ineffective and exposed to challenges such as configuration errors, unauthorized access, and information losses. These security threats emphasize the need for innovative solutions that incorporate advanced technology to ensure the protection of cloud data. Deep Learning (DL) and Machine learning (ML) models have proven effective in centralizing IDS structures [5], but their performance in decentralized edge scenarios is limited without a privacy-protecting collaborative learning method. The application of ML models represents the latest developments in data storage, processing, and acquisition, advancing human discernment of complex patterns and tendencies with increased efficacy [6]. DL is a subdivision of ML based on Artificial Neural Networks (ANNs) that mimic biological neural structures using multiple layers. Although the implementation of smart technologies in Intrusion Detection Systems (IDSs) can reduce the burden on human analysts, the most advanced DL and ML solutions are not well-suited for IoT environments [7].

A. Overview of Cybersecurity

Cybersecurity deals with understanding the concerns on numerous cyberthreats and creating defense approaches to maintain the integrity, confidentiality, and availability of any digital and information technology.

- Confidentiality is the term employed to maintain the confidentiality of information from unauthorized systems or individuals.
- Integrity is the term leveraged to prevent any modification/deletion in an unauthorized way.
- Availability is the term utilized to ensure that the systems responsible for delivering and processing data are available when required and by those who need them.

B. Cloud Computing (CC) Architecture

CC indicates an underlying structure that allows the on-demand admission to an internet-based computer resource. It is a set of connected services and elements that work together to provide effective and adaptable computing. This structure is essentially broken down into two major parts: deployment and service models. There are numerous techniques to advance cloud services that deliberate aspects such as access, security requirements, and ownership.

C. Advantages and Challenges of IoT Integration with Cloud and Edge Computing

The incorporation of IoT and CC unites two distinct, rapidly developing technological paradigms, each with unique features. IoT contains devices connected to a global network characterized by dynamic frameworks, whereas CC boasts an extensive processing capability and nearly unlimited storage. However, IoT challenges, such as limited processing capabilities and storage, can be effectively addressed by incorporating it with CC. EC provides a substantial benefit to manage a volume of services, data, and computation applications, enabling the devolution of processing capabilities from a central hub to the edge of the network. This method employs present resources effectively, storing and maintaining data while permitting control through numerous actions. Within the context of IoT, EC turns into a beneficial asset by enhancing pooled EC sources. The major advantage of EC lies in its proficiency in processing data and storing data in closer proximity to end-users. This proximity helps to speed up and reduce costs, allowing faster decision-making. Nevertheless, the limitations of EC are in its restricted remote serviceability and relatively lesser computation proficiency when contrasted with CC.

D. Machine Learning and Deep Learning in IDS

Unsupervised learning is dependent on similarity-based clustering. Modeling frameworks, such as association and clustering, allow it to extract previously unseen patterns. Anomalies could be recognized utilizing IDS approaches that search for any behavior that diverges from the norm. DL approaches are employed to model complex notions. Regarding feature representation, DL frameworks vary from ML ones. Data-driven models autonomously extract features, with the model self-correcting depending on its own errors.

E. Research Contribution

This survey comprehensively analyses cybersecurity threats in Cloud-Edge IoT systems and critically analyzes AI-enabled DL methods for intrusion detection. It offers foundational knowledge covering cybersecurity concepts, cloud and edge platforms, and IoT integration challenges. The study assesses ML- and DL-based IDS models with emphasis on structural design and performance optimization. A comparative valuation of recent works is conducted considering datasets, detection accuracy, computational efficiency, scalability, and robustness. The analysis identifies prevailing research gaps and utilization challenges, outlining promising future research directions to improve the security and intelligence of Cloud-Edge IoT frameworks.

II. COMPARATIVE ANALYSIS OF EXISTING WORKS

In [8], the Agentic Intelligence Self-Adaptive Framework (AISAF) was proposed, which is a self-adjusting attack classification method for heterogeneous computing systems. AISAF uses a hybrid of Long Short-Term Memory (LSTM), Convolutional Neural Network (CNN), and Transformer backbone to capture temporal, contextual, and spatial dependencies in network traffic. Drift is identified across lightweight behavioral observation, tracking prediction-confidence variations and latent-space deviations in stream data. In case a drift is identified, an agentic meta-optimizer controls a selective upgrade only for the impacted sub-models, decreasing retraining cost and protecting against catastrophic forget. An attention-driven explanation layer offered adaptable feature-level interpretations, providing auditable threat reasoning and supporting transparency. In [9], ML models were examined in network intrusion detection in distributed IoT environments to inspect efficiency, scalability, and accuracy. Data collection, throughout selection, thematic synthesis, and identification of relevant research, focused on types of models, performance measures, architectural techniques, and execution tasks. By classifying the most efficient method to solve the unique features of a distributed IoT system, this study contributed practical insights into more reliable and adaptive IoT security models.

In [10], a tinyML model was proposed to observe the voluminous IoT information for cyberattacks, resolving the limitations of devices by leveraging the Federated Learning (FL) technique to share local detection knowledge while protecting information. The 3-layer structure, integrating tinyML and FL to improve the autonomous identification of cyber threats and identification precision, and reduce resource consumption. In [11], the restrictions of existing IoT threat identification approaches, which frequently struggle with the dynamic nature of IoT systems and the increasing difficulty of cyberthreats, were resolved using an innovative hybrid structure that integrated CNN, BiLSTM, and Deep Neural Networks (DNN) for precise and effective IoT attack detection. Modern optimizer methods, involving quantization and pruning techniques, were used to improve deployment effectiveness in limited-resource IoT systems.

In [12], an Advancing Intelligent Cybersecurity over Ensemble Deep Representation Learning and Feature Dimensionality Reduction (AICEDRL-FDR) model was proposed for Cloud-Edge-IoT systems. The Maximum Relevance Minimum Redundancy (MRMR) method was used to reduce dimensionality by removing irrelevant and redundant features. In [13], a framework was presented to protect wireless and IoT networks by incorporating a testing approach with predictive modeling and anomaly detection techniques. Predictive modeling used both Support Vector Machines (SVM) and Logistic Regression (LR) for binary identification to classify malicious traffic, leading to higher precision and accuracy outcomes. XGBoost achieved enhanced performance over RF in every metric when performing multi-class classification to detect DoS, DDoS, and brute force attacks.

In [14], an IoT IDS combined ensemble DL and SDN Cloud-Edge collaboration. Primarily, the edge control realized the precise identification of suspicious and normal traffic throughout a joint Naive Bayesian and Back Propagation NNs (NB - BP) method, and transmitted the suspicious traffic to the cloud. The detection of suspicious traffic was performed using the EDL technique in cloud detection, and the results were reviewed by the edge controller. This controller could accept consistent prevention metrics to protect network security according to the type of attack. In [15], an innovative Deep Ensemble learning with Pruning (DEEPShield) technique was proposed to effectively detect both higher- and lower-volume DDoS attacks in limited resource systems. This model utilized ensemble learning by combining an LSTM and a CNN with a network traffic analysis model. This approach preprocessed and analyzed network traffic, becoming data-agnostic and leading to higher detection precision. This framework used pruning to refine the ensemble techniques, optimizing them for use in edge devices while maintaining a balance between precision and computational efficacy.

In [16], cloud security for SCADA models and IoT devices was examined, focusing on new security metrics such as zero-trust structures, IDS, and ML-improved cybersecurity protocols. This study inspected the difficulties of applying this structure, involving compliance with regulatory standards, scalability, and upholding operational effectiveness in automated systems. In [17], a DL approach was proposed for a cloud threat detection framework. This method could classify and detect insider threats, zero-day attacks, and improve incident response abilities, offering an invaluable resource for cloud security. In [18], an ML-driven IDS utilized an enhanced feature selection model that employed the Black Hole Algorithm (BHA). This model used a hybrid fitness function and an innovative star encoded scheme to improve classifier outcomes and solution convergence. Feature selection was performed using an XGBoost technique. Moreover, statistical analysis of the experimental results verified the model, proving an important improvement. In [19], an innovative cybersecurity model integrated CNNs to classify spatial characteristics, Gated Recurrent Units (GRUs) for detecting time-driven anomalies, and XGBoost for final identification. The Prairie Dog Optimizer (PDO) model was used for automatic hyperparameter tuning.

The growth of cyberattacks targeting IoT environments requires the development of a cybersecurity model beyond conventional methods. In [20], the disadvantages of recent IDS solutions were highlighted, including their dependence on shallow ML models, presenting an innovative hybrid Autoencoder-Multi-Layer Perceptron (AE-MLP) technique for the detection of DDoS attacks. This model utilized the ability of the AE feature extractor to capture complex patterns and irregularities in network traffic information. The extracted features were passed into an MLP system, allowing the DL model to analyze and classify potential attacks. In [21], an IDS was based on cloud-edge collaboration. This method decreased the computational cost to speed up model training, protect data privacy leakage, improve training data, and identify attacks unidentified by local edge devices. A Stacked Sparse Autoencoder (SSAE) was used to reduce data dimensionality and address the bottleneck of limited resources in edge devices. Then, longer-term serial features of the IoT traffic data were passed through a Temporal Convolutional Network (TCN) to detect attacks. Finally, an FL-based Cloud-Edge structure was utilized to coordinate multi-party training IDS. In [22], an IoT-driven Edge-Cloud structure was proposed for VANETs, which used blockchain to address the need for security.

In [23], a lightweight DL approach used a trained WGAN on the Edge to supplement data instances. In [24], a malicious traffic recognition approach was based on a DL algorithm. In order to solve the problem of small sample data of malicious traffic, this study enriched data diversity using an adversarial network. In [25], an AI-driven IDS for IoT platforms used a recognition component on the edge layer to identify malicious traffic. FedDynST [26] performed DDoS threat recognition based on a Cloud-Edge collaborative approach. CECN-DNN [27] enables collaborative Cloud-Edge computing for both single-task and constant multi-task inference on malicious traffic. In [28], a lightweight Transfer-Learning (TL) model was based on an integrated framework of a CNN-GRU model for IoT intrusion detection.

Table I provides a comprehensive comparison of existing studies, highlighting the techniques, datasets, key findings, and identified research gaps in AI-enabled Cloud-Edge IoT security. Several DL-based intrusion detection approaches display strong performance on reported datasets, but their generalizability to various IoT and Cloud-Edge environments remains limited by variations in network environments and attack patterns. Previous studies also lack deep ensemble modeling, real-time validation, and evaluation against various or adversarial threats. In addition, challenges such as computational complexity, scalability in large-scale IoT systems, and energy effectiveness at the Edge are still not sufficiently explored. These gaps highlight the need for more scalable, efficient, and adaptive DL frameworks for IoT security.

TABLE I. RECENT INTRUSION DETECTION AND CYBERSECURITY FRAMEWORKS FOR CLOUD, EDGE, AND IOT SYSTEMS

Study	Purpose	Techniques	Dataset	Key findings	Research gaps
[8]	Unified cyber defense across Cloud-Edge-IoT systems	CNN, LSTM, and Transformer	PaySim, IEEE-CIS Fraud Detection, CICIDS2018, UNSW-NB15, CICIDS2017, and BoT-IoT	DRI of 0.9	Limited benchmarking against deep ensemble approaches
[9]	Assess ML approach for IoT intrusion detection	ML classifiers	Synthetic dataset	Achieved better performance	Lack of DL and real-time validation
[10]	Resilient IoT-edge with federated tinyML	FL and tinyML	N-BaIoT dataset	NA	Restricted threat diversity testing
[11]	Detect IoT cybersecurity attacks	CNN, BiLSTM, and DNN	IoT-23 and Edge-IIoTset datasets	99% accuracy on both datasets.	High computational complexity.
[12]	AI-enabled cybersecurity in Cloud-Edge-IoT infrastructures	mRMR, DCAE, FDBN, and TCN	Edge-IIoT and ToN-IoT datasets	Accuracies of 99.31% and 99.24%	Scalability in ultra-large IoT was not validated.
[13]	IoT smart city penetration testing	LR and SVM models	CIC-IDS2017 dataset	Accomplished better performances	Limited DL integration
[14]	SDN Cloud-Edge collaborative IDS	NB and BP NN.	NA	Attained better outcomes	Security against adversarial threats was not analyzed.
[15]	DDoS detection in an IoT platform	CNN and LSTM methods	HL-IoT, ToN-IoT, CICIDS-17, and ISCX-12	Accomplished an accuracy of over 90%	Generalization to other threat types unclear
[16]	Cloud security for IoT and SCADA	Security framework model	SCADA datasets	NA	No AI-based adaptive detection
[17]	AI-enhanced cloud threat recognition	DL methods	Edge-IIoTset dataset	Accuracy of 98.2%	Edge-layer integration was missing
[18]	ML-based IoT intrusion detection	Black Hole Algorithm (BHA) and ML	AWID3 dataset	Accuracy of 99.63%	No deep ensemble modeling.
[19]	Adaptive IoT attack recognition	CNN, GRU, XGBoost, and Prairie Dog Optimization	CIC-IDS 2018 and LANL Cybersecurity datasets	F1 score of 99.1%	Energy efficiency at the edge was not studied
[20]	Secure mobile edge computing	AE and MLP methods	NF-UQ-NIDS-V2 dataset	High accuracy of 99.98%	Limited Cloud-Edge scalability analysis
[21]	Efficient IoT intrusion detection	SSAE and TCN	CIC-IDS-2017 dataset	Attained better performance	Ensemble DL approaches were not explored
[22]	IoT-edge smart microgrid security	Variational encoder NNs.	Smart grid dataset	Accuracy of 98%	Focused on the energy domain only
[23]	Identify network anomaly traffic in cloud-edge collaborative networks	BiLSTM, CNN, and WGAN	NSL-KDD, UNSW-NB15, and CIC-ISD2018	Accuracy of 0.974, 0.925, and 0.953.	Maximum computational cost and restricted real-time adaptability
[24]	Detect malicious traffic in cloud-edge-end environments	DL and CNN models	Network traffic dataset	Accuracy of 93.89%	Lacked explainability and struggled with unseen threats.
[25]	Design a robust intrusion detection system for IoT in Cloud-Edge network	Dual Attention Mechanism	IoT intrusion datasets	Accuracy of 98.4%	Increased model complexity and resource consumption.
[26]	Identify DDoS threats in industrial control systems utilizing Cloud-Edge collaboration	Spatiotemporal DL model	CICDDoS2019 and Edge-IIoTset	Achieved effective attack detection	Restricted scalability and required large labeled datasets
[27]	Allow effectual intrusion detection utilizing collaborative inference	DNN	Network intrusion dataset	Reduced latency	The trade-off between accuracy and latency was not fully optimized.
[28]	Enhance IoT intrusion detection utilizing TL	CNN and GRU models	IoT intrusion and BoT-IoT	Accuracy of 0.99	Transferability through a heterogeneous network remained challenging

III. RESULT ANALYSIS

Table II presents a comparative analysis of existing approaches across different measures [12, 29-31]. The Rule-Based IDS model demonstrated the least performance with $accur_y$ of 89.90%, $prec_n$ of 85.40%, $reca_l$ of 79.10%, and $F1_{score}$ of 72.80%. The voting classifier exhibited slightly better results with $accur_y$ of 89.95%, $prec_n$ of 94.67%, $reca_l$ of 92.50%, and $F1_{score}$ of 92.95%. The EDLM-PSOFS and AE+LSTM approaches showed moderate performances with $accur_y$ of 94.06% and 94.24%, respectively. The GA-LSTM, CNN-RNNs, TabPFN, and TabNet approaches achieved better results, with $accur_y$ of 95.39%, 96.00%, 96.86%, and 97.00%, respectively. The FNN-CNN-Focal loss approach achieved $accur_y$ of 98.03%, $prec_n$ of 89.27%, $reca_l$ of 90.59%, and $F1_{score}$ of 89.04%. The CNN-GRU method demonstrated better results, with $accur_y$ of 98.07%, $prec_n$ of 90.81%, $reca_l$ of 91.55%, and $F1_{score}$ of 90.06%. Many approaches attain better performance due to their ability to automatically extract features from network traffic. DL methods can learn hidden patterns efficiently, while ensemble methods integrate multiple models to enhance detection accuracy and overall robustness.

TABLE II. COMPARATIVE ANALYSIS OF EXISTING METHODS

Method	$Accur_y$	$Preci_n$	$Recal_l$	$F1_{Score}$
VAE [12]	91.61	91.69	91.61	91.60
Rule-Based IDS [12]	89.00	85.40	79.10	72.80
AE+LSTM [12]	94.24	93.30	91.20	92.20
CNN-RNNs [12]	96.00	93.21	94.95	92.89
EDLM-PSOFS [29]	94.06	92.76	92.13	93.96
GA-LSTM [29]	95.39	95.61	93.48	89.79
LightGBM [29]	93.02	89.73	90.69	92.32
TabPFN [29]	96.86	92.35	89.95	90.63
Voting classifier [29]	89.95	94.67	92.50	92.95
VGGIncepNet [30]	92.00	93.00	92.00	92.00
CNN-GRU [30]	98.07	90.81	91.55	90.06
FNN-CNN-Focal Loss [31]	98.03	89.27	90.59	89.04
TabNet [31]	97.00	91.23	91.29	90.16
XGBoost [31]	93.37	91.39	89.54	91.86
GB machines [12]	91.45	93.43	89.12	91.22

IV. CONCLUSION

This survey reviewed emerging cybersecurity threats in Cloud-Edge IoT systems and analyzed AI-driven DL algorithms for intrusion detection. It summarized key concepts of Cloud, Edge, and IoT architectures, and examined ML- and DL-based IDS algorithms. A comparative evaluation of recent studies was conducted based on datasets, performance metrics, scalability, efficiency, and robustness. Unlike existing surveys, this work offers a unified perspective by integrating Cloud, Edge, and IoT security considerations within a single analytical framework. In addition, it critically identifies key limitations in existing methods, such as scalability challenges, computational overhead, and lack of explainability. Despite satisfactory outcomes, challenges such as increased computational complexity, limited dataset variety, and scalability problems in large-scale IoT networks are major concerns for IDS utilization. This survey highlights research gaps, implementation issues, and future directions for developing secure and resilient Cloud-Edge IoT networks. Future research directions should focus on federated and decentralized learning methods, explainable AI (XAI) for transparent decision-making, and adaptive ensemble methods to detect emerging attacks. Overcoming these challenges is vital for building protected, intelligent, and resilient Cloud-Edge IoT environments.

DECLARATION OF COMPETING INTERESTS

Not applicable to this work.

ACKNOWLEDGMENT

The author extends his appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/ 2025/01/37460).

DATA AVAILABILITY

Not applicable to this work.

REFERENCES

[1] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-Computing Architectures for Internet of Things Applications: A Survey," *Sensors*, vol. 20, no. 22, Nov. 2020, Art. no. 6441, https://doi.org/10.3390/s20226441.

[2] A. S. Anshad *et al.*, "Intelligent Anomaly Detection for Secure Data Transmission in Cloud Computing Systems over 6G Networks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 6, pp. 30349–30355, Dec. 2025, https://doi.org/10.48084/etasr.14022.

[3] S. A. Alshaya, "IoT Device Identification and Cybersecurity: Advancements, Challenges, and an LSTM-MLP Solution," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 11992–12000, Dec. 2023, https://doi.org/10.48084/etasr.6295.

[4] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Computers & Electrical Engineering*, vol. 59, pp. 126–140, Apr. 2017, https://doi.org/10.1016/j.compeleceng.2016.03.004.

[5] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences*, vol. 9, no. 20, Oct. 2019, Art. no. 4396, https://doi.org/10.3390/app9204396.

[6] A. T. Azar, S. U. Amin, M. A. Majeed, Ahmed Al-Khayyat, and I. Kasim, "Cloud-Cyber Physical Systems: Enhanced Metaheuristics with Hierarchical Deep Learning-based Cyberattack Detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 17572–17583, Dec. 2024, https://doi.org/10.48084/etasr.8286.

[7] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, vol. 10, pp. 121173–121192, 2022, https://doi.org/10.1109/ACCESS.2022.3220622.

[8] B. Vijetha, "Agentic Intelligence for Unified Cyber Defense: A Self-Adaptive Framework for Threat Detection Across Cloud, Edge, and IoT Systems," *IEEE Access*, vol. 14, pp. 5104–5118, 2026, https://doi.org/10.1109/ACCESS.2026.3650833.

[9] D. Darmin, W. Wahyudi, I. Taufik, A. Yusup, and A. H. Maulana, "Evaluation of Machine Learning Implementation for Network Intrusion Detection in Distributed IoT Systems," *Riwayat: Educational Journal of History and Humanities*, vol. 9, no. 1, pp. 1639–1653, Feb. 2026, https://doi.org/10.24815/riwayat.v9i1.472.

[10] P. Laiu, M. Li, J. A. Nichols, M. Huettel, I. Sikkema, and M. Mathur, "Designing resilient IoT and Edge Computing with federated tinyML," *Journal of Systems Architecture*, vol. 174, May 2026, Art. no. 103709, https://doi.org/10.1016/j.sysarc.2026.103709.

[11] B. A. Agbor, B. U. A. Stephen, P. Asuquo, U. O. Luke, and V. Anaga, "Hybrid CNN–BiLSTM–DNN Approach for Detecting Cybersecurity Threats in IoT Networks," *Computers*, vol. 14, no. 2, Feb. 2025, Art. no. 58, https://doi.org/10.3390/computers14020058.

[12] K. A. Alattas, "Advancing artificial intelligence-enabled cybersecurity framework using ensemble deep representation learning for intelligent cybersecurity in cloud-edge-IoT environments," *AIMS Mathematics*, vol. 10, no. 12, pp. 28981–29011, 2025, https://doi.org/10.3934/math.20251275.

[13] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, Y. Mardenov, and D. Satybaldina, "Penetration Testing and Machine Learning-Driven Cybersecurity Framework for IoT and Smart City Wireless Networks," *IEEE Access*, vol. 13, pp. 86144–86166, 2025, https://doi.org/10.1109/ACCESS.2025.3569965.

[14] Y. Xu, Y. Li, and Z. Sun, "IoT Intrusion Detection Using SDN Cloud-Edge Collaboration and Ensemble Deep Learning," in *2024 IEEE Cyber Science and Technology Congress (CyberSciTech)*, Nov. 2024, pp. 195–200, https://doi.org/10.1109/CyberSciTech64112.2024.00039.

[15] M. F. Saiyedand and I. Al-Anbagi, "Deep Ensemble Learning With Pruning for DDoS Attack Detection in IoT Networks," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 596–616, 2024, https://doi.org/10.1109/TMLCN.2024.3395419.

[16] A. Enemosah and O. G. Ifeanyi, "Cloud security frameworks for protecting IoT devices and SCADA systems in automated environments," *World Journal of Advanced Research and Reviews*, vol. 22, no. 3, pp. 2232–2252, June 2024, https://doi.org/10.30574/wjarr.2024.22.3.1485.

[17] A. Gogineni, "AI-Enhanced Threat Detection and Response in Cloud Infrastructure Using Deep Learning Techniques," *Journal of Artificial Intelligence & Cloud Computing*, vol. 3, no. 1, pp. 1–7, Mar. 2024, https://doi.org/10.47363/JAICC/2024(3)427.

[18] N. Kumar, J. P. Singh, and P. Kumar, "Machine learning-enhanced IoT network security: a Black Hole Algorithm-based feature selection approach for intrusion detection," *Journal of Cyber Security Technology*, vol. 10, no. 1, pp. 1–19, Dec. 2026, https://doi.org/10.1080/23742917.2025.2542995.

[19] C. Han, F. M. Alserhani, T. A. Ahanger, N. K. Almazmomi, and A. Hashmi, "Adaptive cyber threat detection in internet of things environment using deep learning and metaheuristic optimization," *Peer-to-Peer Networking and Applications*, vol. 19, no. 1, Jan. 2026, Art. no. 38, https://doi.org/10.1007/s12083-025-02130-5.

[20] O. Adeniyi, A. S. Sadiq, P. Pillai, M. Aljaidi, and O. Kaiwartya, "Securing Mobile Edge Computing Using Hybrid Deep Learning Method," *Computers*, vol. 13, no. 1, Jan. 2024, Art. no. 25, https://doi.org/10.3390/computers13010025.

[21] R. Yang *et al.*, "Efficient intrusion detection toward IoT networks using cloud–edge collaboration," *Computer Networks*, vol. 228, June 2023, Art. no. 109724, https://doi.org/10.1016/j.comnet.2023.109724.

[22] U. Arul, R. Gnanajeyaraman, A. Selvakumar, S. Ramesh, T. Manikandan, and G. Michael, "Integration of IoT and edge cloud computing for smart microgrid energy management in VANET using machine learning," *Computers and Electrical Engineering*, vol. 110, Sept. 2023, Art. no. 108905, https://doi.org/10.1016/j.compeleceng.2023.108905.

[23] Y, Wang, "Network Anomaly Traffic Detection Using WGAN-CNN-BiLSTM in Big Data Cloud–Edge Collaborative Computing Environment," *JIPS(Journal of Information Processing Systems)*, vol. 20, no. 3, pp. 375–390, June 2024, https://doi.org/10.3745/JIPS.01.0105.

[24] H. Liu, F. Han, and Y. Zhang, "Malicious traffic detection for cloud-edge-end networks: A deep learning approach," *Computer Communications*, vol. 215, pp. 150–156, Feb. 2024, https://doi.org/10.1016/j.comcom.2023.12.024.

[25] L. Zhou *et al.*, "AI-driven robust dual attention-enhanced intrusion detection framework for IoT devices in edge-cloud computing networks," *Future Generation Computer Systems*, vol. 176, Mar. 2026, Art. no. 108110, https://doi.org/10.1016/j.future.2025.108110.

[26] Z. Cao, B. Liu, D. Gao, D. Zhou, X. Han, and J. Cao, "A Dynamic Spatiotemporal Deep Learning Solution for Cloud–Edge Collaborative Industrial Control System Distributed Denial of Service Attack Detection," *Electronics*, vol. 14, no. 9, Apr. 2025, https://doi.org/10.3390/electronics14091843.

[27] J. Zhou *et al.*, "CECN-DNN: A Cloud-Edge Collaborative Inference Approach to Intrusion Detection," *Computer Networks*, Feb. 2026, Art. no. 112127, https://doi.org/10.1016/j.comnet.2026.112127.

[28] A. Gamlo, S. Sharaf, and R. Molla, "Efficient CNN–GRU Transfer Learning for Edge IoT Intrusion Detection," *Electronics*, vol. 15, no. 5, Feb. 2026, https://doi.org/10.3390/electronics15050981.

[29] H. Alamro *et al.*, "An intelligent deep representation learning with enhanced feature selection approach for cyberattack detection in internet of things enabled cloud environment," *Scientific Reports*, vol. 15, no. 1, Sept. 2025, Art. no. 34013, https://doi.org/10.1038/s41598-025-13457-7.

[30] A. Bensaoud and J. Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models," *Ad Hoc Networks*, vol. 170, Apr. 2025, Art. no. 103770, https://doi.org/10.1016/j.adhoc.2025.103770.

[31] F. Albalwy and M. Almohaimeed, "Advancing Artificial Intelligence of Things Security: Integrating Feature Selection and Deep Learning for Real-Time Intrusion Detection," *Systems*, vol. 13, no. 4, Mar. 2025, Art. no. 231, https://doi.org/10.3390/systems13040231.