A Comprehensive Review of DDoS Attack Detection in IoT using Deep Learning and Intelligence Techniques

M.I.Thariq Hussan[1], Dr.Shish Ahmad[2]
[1]Postdoctoral Researcher, Lincoln University, Malaysia
Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, India.
[2]Head of the Department, Department of Computer Science and Engineering, Integral University, Lucknow,
Uttar Pradesh, India.
[1]thariqhussain@rediffmail.com, [2]drshishahmad@gmail.com

Abstract: The rapid growth of the Internet of Things (IoT) has expanded connectivity and automation but also increased vulnerability to cyberattacks, especially Distributed Denial of Service (DDoS) attacks. Detecting such attacks in IoT environments is challenging due to large data volumes, device heterogeneity, and limited resources. Recently, machine learning and deep learning techniques have been widely adopted to improve intrusion detection performance. This paper reviews state-of-the-art IoT DDoS detection methods, classifying them into hybrid deep learning models, federated learning frameworks, optimization and feature selection techniques, machine learning and ensemble methods, SDN/edge-based architectures, and blockchain-enabled solutions. These approaches are evaluated based on architecture, datasets, performance metrics, advantages, and limitations. The review finds that hybrid deep learning models achieve high detection accuracy, while federated learning and blockchain approaches enhance privacy and security. Machine learning models are lightweight and efficient, especially when combined with optimized feature selection. However, challenges remain, including high computational complexity, poor generalization, limited explainability, and difficulty detecting zero-day attacks. Finally, the paper identifies research gaps and highlights the need for lightweight, scalable, and adaptive intrusion detection systems suitable for dynamic IoT environments.

Keywords: Deep learning; Internet of Things; Distributed Denial of Service; Recurrent Neural Network.

INTRODUCTION

The rapid growth of the Internet of Things (IoT) has transformed modern computing by connecting smart devices in applications such as healthcare, smart cities, industrial automation, and transportation. However, the large-scale deployment of IoT devices, combined with their limited resources and heterogeneity, has increased vulnerability to cyber threats, particularly Distributed Denial of Service (DDoS) attacks that disrupt network availability through malicious traffic [1].

To address these challenges, researchers have explored machine learning and deep learning-based detection methods. Various approaches, ranging from traditional machine learning models to advanced hybrid deep learning architectures, have been proposed. However, differences in methodologies, datasets, and evaluation metrics make systematic comparison difficult [2]. Therefore, classifying existing studies is essential to better understand the research landscape.

This review categorizes recent DDoS detection approaches based on their methodologies and functional characteristics [3]. Hybrid deep learning models combining CNN [4], RNN [5], and attention mechanisms have shown strong performance in capturing spatial and temporal traffic patterns. Federated learning has emerged as a privacy-preserving solution for distributed intrusion detection, while optimization and feature selection methods improve efficiency and reduce computational cost. Traditional machine learning and ensemble models remain useful for lightweight and real-time applications. In addition, SDN, fog computing, edge computing, and blockchain technologies have been integrated to improve scalability, latency, security, and decentralized trust in IoT environments.

Despite these advancements, existing methods still face challenges such as high computational complexity, poor generalization to real-world scenarios, lack of interpretability, and limited capability in

handling zero-day attacks. This review therefore provides a systematic and comparative analysis of state-of-the-art IoT-based DDoS detection methods, highlighting current trends, limitations, and future research directions for developing scalable, adaptive, and efficient intrusion detection systems.

HYBRID DEEP LEARNING-BASED DDOS DETECTION

Karamollaoglu et al. [6] suggested a CNNBiLSTM model with multi-head attention, which attains good spatial and temporal feature extraction and focuses on important traffic patterns with the highest accuracy of 99.93%. Equally, a light hybrid CNN-BiLSTM with attention mechanism that balances between the performance of detection and the computational efficiency was proposed by Najar et al. [7] and it is applicable in real-time deployment. Al-Eryani et al. [8] created a GRU-BiLSTM network, which maximizes the learning of the temporal dependency and has the highest accuracy rate of 99.99 with minimum false positives, but still cannot be interpreted. In general, hybrid architectures are very effective in increasing the precision of detection, but their processing power is a limiting factor.

Table 1 : Comparisons of Hybrid Deep Learning-based DDoS Detection

	Method	Key Contributions	Dataset	Merits	Demerits
	CNN + BiLSTM + Attention	Multi-level feature extraction with attention prioritization	CICDDoS 2019	Very high accuracy (99.93%), robust detection	High computational complexity
	CNN + BiLSTM + Attention	Lightweight hybrid model for real-time detection	CICDDoS 2019 Edge-IIoT	Efficient and scalable	Limited large-scale validation
	GRU + BiLSTM	Deep temporal learning with low false positives	CICDDoS 2019	Extremely high accuracy (99.99%)	Lack of interpretability

FEDERATED LEARNING AND PRIVACY-PRESERVING APPROACHES

Alsarhan et al. [9] adopted a federated deep learning system that allows collaborative learning to be held with decentralized devices and preserve data privacy with 98% accuracy and lower false positives. Alshdadi et al. [10] introduced a ResVGG-SwinNet architecture in an FL environment, which is a joint of CNN and transformer networks to enhance feature representation and scalability in heterogeneous IoT networks. Likewise, Alhasawi et al. [11] showed the efficiency of FL with CNN models to perform decentralized detection, but the performance is determined by the distribution of data over the nodes. These investigations point out that FL-based systems are privacy-assured and scalable, but need optimization to minimize overhead and enhance training performance.

Table 2 : Comparisons of Federated and privacy-preserving Learning-based DDoS Detection

	Method	Key Contributions	Dataset	Merits	Demerits
	Federated Deep Learning	Privacy-preserving distributed learning	CICDDoS2019	Reduced false positives, privacy protection	Communication overhead

	FL + ResVGG-SwinNet	CNN + Transformer hybrid in FL	CIC-DDoS 2019, UNSW-NB 15	High scalability, strong feature extraction	High training complexity
	FL + CNN	Decentralized DDoS detection	CICIDS2017	Data privacy, distributed learning	Sensitive to data imbalance

OPTIMIZATION AND FEATURE SELECTION-BASED APPROACHES

Yang et al. [12] used pelican optimization with sparse denoising autoencoder to pick the best features with a 99.80% accuracy and reduce redundancy. The Aboalela et al. [13] used Siberian tiger optimization and artificial protozoa optimizer to select features and parameter tuning in the hybrid deep learning structure, which led to a high level of detection (99.52%). To effectively detect in real-time, Arya et al. [14] employed the PCA and adaptive sliding window methods with LightGBM. In general, optimization is much better at enhancing feature relevance and performance, at the cost of increasing computational complexity and design overhead.

Table 3 : Optimization and feature selection-based DDoS Detection

	Method	**Key Contributions**	**Dataset**	**Merits**	**Demerits**
	IPOA + SDAE	Optimal feature pruning	BoT-IoT	High accuracy (99.80%)	High computational cost
	STO + APO + BiGRU	Optimized feature selection & tuning	IoT datasets	Improved performance	Complex optimization pipeline
	PCA + LightGBM	Real-time efficient classification	IoT datasets	Fast and lightweight	Limited adaptability

LIGHTWEIGHT MODELS, ENSEMBLE, AND MACHINE LEARNING

In [15], Shukla et al. suggested a distributed ensemble with H2O.ai and Apache Storm allowing the detection of multi-class attacks in real-time and with a high success rate and low latency. Al-Fayoumi et al. [16] created a lightweight decision tree-based IDS, which has an accuracy of 99.5 with a small number of features, thus being suitable in resource-constrained settings. As Belachew et al. [17] showed, XGBoost is the best compared to the other models of ML in terms of accuracy and execution time, which suggests its applicability to real-time systems. These research findings suggest that ML-based solutions are effective and can be scaled but might not be able to cope with complicated attack patterns.

Table 4 : Comparisons of Lightweight Models, Ensemble, and Machine Learning -based DDoS Detection

	Method	**Key Contributions**	**Dataset**	**Merits**	**Demerits**
	Ensemble (H2O + Storm)	Real-time multi-class detection	IoT datasets	High accuracy,	Complex deployment

				fast processing	
	Decision Tree	Lightweight IDS with minimal features	MQTT dataset	Fast and efficient	Limited complexity handling
	XGBoost	High-performance ML detection	CICIDS2017, Edge-IIoT	Fast and accurate	Requires feature engineering

SDN, FOG AND EDGE-BASED SECURITY FRAMEWORKS

An SDN-based fog-enabled architecture that is proposed by Chaudhary et al. [18] integrates entropy-based detection with machine learning, which allows cutting the response time by a significant factor and enhancing the accuracy of detection. Rajan et al. [19] adopted a CNN-LSTM model in an SDN setting to detect and mitigate anomalies in traffic, which is successful in detecting abnormal traffic patterns. These frameworks are more scalable and perform better, however, with a cost to the security of the controller and complexity of the system.

Table 5 : Comparisons of SDN, Fog and Edge-Based Security Frameworks-based DDoS Detection

	Method	**Key Contributions**	**Dataset**	**Merits**	**Demerits**
	SDN + Fog + ML	Reduced latency detection	BoT-IoT	Scalable, fast response	Controller dependency
	CNN + LSTM	Anomaly detection in SDN	IoT datasets	Effective pattern recognition	Limited real-time validation

ADVANCED SECURITY MECHANISMS AND BLOCKCHAIN

Villegas et al. [20] suggested a hybrid framework using blockchain and AI, which can guarantee data integrity and real-time detection, although scalability is an issue. Abi Sen et al. [21] proposed a dual-chain blockchain framework that had deep learning-based adaptive and resilient attack detection with moderate performance but did not compromise the efficiency of the system. These strategies emphasize the significance of safe and decentralized models, but they usually lack in-latency and resource limitations.

Table 6 : Comparisons of Advanced Security Mechanisms and Blockchain-based DDoS Detection

	Method	**Key Contributions**	**Dataset**	**Merits**	**Demerits**
	Blockchain + AI	Data integrity + detection	IoT datasets	Secure and reliable	Scalability issues

	Dual-chain + DL	Adaptive detection system	IoT-23	Handles unseen attacks	Moderate accuracy

CHALLENGES OF EXISTING WORK

Although significant progress has been made in IoT-based DDoS detection, several challenges remain.

- High computational complexity in hybrid deep learning models (CNN, LSTM, GRU, attention) limits deployment on resource-constrained IoT devices.
- Most models are tested only on benchmark datasets such as CICDDoS2019 and BoT-IoT, reducing their effectiveness in real-time and dynamic network environments.
- Heavy dependence on limited public datasets causes overfitting and weak generalization to unseen or zero-day attacks. Dataset imbalance also affects prediction accuracy despite techniques like SMOTE and ADASYN.
- Deep learning models often lack explainability and transparency, making it difficult for administrators to trust detection decisions, even though methods like SHAP and LIME have been explored.
- Federated learning and blockchain-based solutions introduce communication overhead, latency, and synchronization issues, reducing suitability for real-time detection.
- Current systems have limited capability in detecting zero-day and adaptive attacks, while energy efficiency and scalability are often overlooked in large-scale IoT environments with constrained resources.

FUTURE IMPROVEMENTS AND FUTURE RESEARCH

This review provides a comprehensive overview of recent IoT-based DDoS detection approaches and highlights several future research directions to address current limitations.

- Develop lightweight and energy-efficient models with high detection accuracy for deployment on edge and IoT devices using techniques such as model compression, pruning, and knowledge distillation.
- Focus on real-time and adaptive learning frameworks capable of handling dynamic network conditions through online learning, continual learning, and reinforcement learning.
- Build generalized models trained on diverse real-world datasets containing multiple attack types and realistic traffic scenarios to improve robustness and generalization.
- Enhance explainability and transparency by integrating explainable AI methods that provide clear reasons for detection decisions, especially in critical domains such as smart cities and healthcare.
- Improve hybrid architectures combining deep learning, federated learning, and blockchain to balance accuracy, privacy, and efficiency while reducing communication overhead and improving blockchain consensus mechanisms.
- Advance zero-day attack detection and anomaly-based systems using unsupervised and self-supervised learning techniques that do not rely heavily on labeled data.
- Ensure scalability and compatibility with emerging technologies such as 5G/6G, edge computing, and software-defined networking (SDN) to support robust and real-time intrusion detection in next-generation IoT environments.

CONCLUSION

This review provides a comprehensive overview of recent DDoS detection approaches in IoT by classifying existing solutions based on methodology and architecture. The study shows that hybrid deep

learning models, particularly those combining CNN, LSTM/GRU, and attention mechanisms, achieve high performance by capturing both spatial and temporal traffic features. Federated learning and blockchain-based approaches enhance privacy, security, and decentralized learning in distributed IoT environments. Optimization and feature selection methods improve detection accuracy while reducing computational cost, whereas traditional machine learning and ensemble techniques offer lightweight and real-time solutions. In addition, SDN, fog, and edge-based architectures help reduce latency and improve scalability in large-scale IoT networks. Despite these advances, several challenges remain, including high computational complexity, dependence on benchmark datasets, poor generalization to real-world scenarios, limited explainability, and difficulty detecting zero-day attacks. These issues highlight the need for more adaptive, efficient, and robust detection systems.

Future research should focus on lightweight and energy-efficient models for resource-constrained IoT devices. Incorporating continuous and adaptive learning can improve zero-day attack detection, while using diverse real-world datasets can enhance model robustness and generalization. Furthermore, integrating explainable AI (XAI) can improve transparency and trust. Optimizing federated learning and blockchain frameworks may reduce communication overhead and latency. Finally, combining deep learning with edge computing, SDN, and 5G/6G technologies can enable scalable, secure, and real-time intrusion detection systems.

REFERENCES

[1] E. Osei Owusu, I. Danlard, G. Opoku, A. Dede, G. Klogo, K. Osei Boateng and E. Kofi Akowuah, "A Systematic Review of Machine Learning and Deep Learning Techniques for DDoS Attack Mitigation in IoT and Edge Computing Systems", Security and Privacy, vol. 9, no. 1, pp. e70147, 2026.

[2] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. Marghalani, O. B. Alotaibi and S. A. Bajandouh, "DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions", Electronics, vol. 12, no. 14, pp. 3103, 2023.

[3] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things", Future Generation Computer Systems, vol. 82, pp. 761-768, 2018.

[4] M. Belhaj Mohamed, D. Bouzidi, M. Khalid Ibraheem, A. Al-Abadi and A. Fakhfakh, "Cyber Approach for DDoS Attack Detection Using Hybrid CNN-LSTM Model in IoT-Based Healthcare", Future Internet, vol. 18, no. 1, pp. 52, 2026.

[5] A. OK Al-Hasani, I. R Abdelmaksoud and A. Rezk, "A Novel Hybrid CNN-LSTM Framework for Robust DDoS Attack Detection and Classification", Journal of Cybersecurity & Information Management, vol. 17, no. 1, 2026.

[6] H. Karamollaoglu, İ. Yucedag, İ. A. Dogru, S. Toklu and İ. Atacak, "CBM-IDS: An Advanced Hybrid Deep Learning Model for DDoS Attack Detection in IoT Networks", Journal of Universal Computer Science, vol. 32, no. 1, pp. 108, 2026.

[7] A. A. Najar and S. M. Naik, "DDoS attack detection using CNN-BiLSTM with attention mechanism", Telematics and Informatics Reports, vol. 18, pp. 100211, 2025.

[8] A. M. Al-Eryani, F. A. Omara and E. Hossny, "A deep learning GRU-BiLSTM for DDoS attack detection", SN Computer Science, vol. 6, no. 6, pp. 605, 2025.

[9] A. Alsarhan, M. Barhoush, B. Khassawneh, M. Al-Essa, M. Aljaidi and Q. Al-Naamneh, "Deep Learning Utilization for DDoS Attack Detection with Federated Learning: A Case Study on the CICDDoS2019 Dataset", Engineering, Technology & Applied Science Research, vol. 16, no. 1, pp. 31203-31208, 2026.

[10] A. A. Alshdadi, A. Ali Almazroi, N. Ayub, M. D. Lytras, E. Alsolami, F. S. Alsubaei and R. Alharbey, "Federated deep learning for scalable and privacy-preserving distributed denial-of-service attack detection in internet of things networks", Future Internet, vol. 17, no. 2, pp. 88, 2025.

[11] Y. Alhasawi and S. Alghamdi, "Federated learning for decentralized DDoS attack detection in IoT networks", IEEE Access, vol. 12, pp. 42357-42368, 2024.

[12] E. Yang, S. Jeong and C. Seo, "Harnessing feature pruning with optimal deep learning based DDoS cyberattack detection on IoT environment", Scientific Reports, vol. 15, no. 1, pp. 17516, 2025.

[13] R. A. Aboalela, K. H. Allehaibi, N. Alsaadi, A. S. Alorfi, L. A. Maghrabi, B. Ashary, W. Alghamdi and M. Ragab, "Harnessing feature pruning with optimal deep learning-based distributed denial of service cyberattack detection on IoT environment", Alexandria Engineering Journal, vol. 120, pp. 584-597, 2025.

[14] H. Arya, N. Kandhoul, S. K. Dhurandher and I. Woungang, "Adaptive sliding window and LightGBM-based DDoS attack detection framework for IoT networks", Peer-to-Peer Networking and Applications, vol. 19, no. 1, pp. 16, 2026.

[15] P. Shukla, C. R. Krishna and N. V. Patil, "Distributed ensemble method using deep learning to detect DDoS attacks in IoT networks", Arabian Journal for Science and Engineering, vol. 50, no. 2, pp. 1143-1168, 2025.

[16] M. Al-Fayoumi and Q. A. Al-Haija, "Capturing low-rate DDoS attack based on MQTT protocol in software Defined-IoT environment", Array, vol. 19, pp. 100316, 2023.

[17] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa and A. J. Muhammed, "Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning", IEEE Access, 2025.

[18] P. Chaudhary, A. K. Singh and B. B. Gupta, "Dynamic multiphase DDoS attack identification and mitigation framework to secure SDN-based fog-empowered consumer IoT networks", Computers and Electrical Engineering, vol. 123, pp. 110226, 2025.

[19] D. M. Rajan and D. J. Aravindhar, "Detection and mitigation of DDOS attack in SDN environment using hybrid CNN-LSTM", Migration Letters, vol. 20, pp. 407-419, 2023.

[20] W. Villegas, J. Govea, R. Gurierrez and A. Mera-Navarrete, "Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection", IEEE Access, 2025.

[21] A. A. Abi Sen, A. B. Mnaouer, O. Tayan and N. M. Bahbouh, "A Hybrid Framework for IoT Attacks Detection Combining Blockchain and Deep Learning", Ad Hoc Networks, pp. 104197, 2026.