Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 4, Number: 1, Pages: 50 - 55, Year: 2026

Security in IoT Devices against DDoS Attacks: Strategies and Mitigation Techniques

Waleed Ahmad and Irshad Ahmed Sumra

School of Science & Technology, University of Management and Technology, Lahore, Pakistan
*Corresponding author: Waleed Ahmad (Email: androfire821@gmail.com)

Received: 12/01/2026, Revised: 21/05/2026, Accepted: 18/06/2026

***Abstract*— The rapid growth of Internet of Things (IoT) deployments has increased the threat of Distributed Denial of Service (DDoS) attacks that use resource-constrained devices to disrupt critical services. This paper conducts a systematic literature review (SLR) following the PRISMA 2020 guidelines and synthesizes 62 studies published between 2023-2026 retrieved from IEEE Xplore, ACM, ScienceDirect, SpringerLink, Wiley, MDPI, and Scopus. The review classifies DDoS attack vectors, analyzes exploited IoT vulnerabilities, and evaluates mitigation strategies such as machine learning, blockchain, software-defined networking (SDN), and edge computing. Hybrid CNN-LSTM models can achieve up to 99.1% detection accuracies and federated learning is the fastest growing sub-area. It identifies key research gaps and a future roadmap prioritized.**

***Index Terms*—Botnet detection, DDoS attacks, federated learning, IoT security, machine learning, PRISMA.**

I. Introduction

THE proliferation of *Internet of Things (IoT)* devices has transformed every domain of modern life, from smart healthcare and industrial automation to critical infrastructure and consumer electronics. Industry projections estimate over 32 billion active IoT connections by 2025, with that figure rising steeply through decade [1]. However, the very characteristics that make IoT deployments commercially compelling—low-cost hardware, always-on connectivity, and minimal human supervision—create a uniquely exploitable attack surface. Most devices operate with constrained processors and memory that preclude conventional security software, while manufacturers continue to ship units with weak default credentials and no provision for firmware updates [2].

Among the threats facing IoT ecosystems, Distributed Denial of Service (DDoS) attacks represent one of the most damaging and increasingly common attack categories. By co-opting thousands of compromised IoT endpoints into coordinated botnets, adversaries can generate attack volumes sufficient to overwhelm cloud services, internet exchange points, and operational technology networks. The Mirai botnet family, continuously evolving since its initial deployment, remains the dominant IoT botnet lineage; its 2023 variants—catalogued by Hussain et al. [3]—introduced encrypted C2 channels and multi-stage payload delivery, substantially complicating detection and takedown efforts.

Although the research space for IoT DDoS defenses is growing rapidly, practitioners and researchers encounter a fragmented literature. The methodologies used in studies vary widely, the datasets and results differ significantly, and seldom are the findings synthesized with enough rigor to support evidence-based decisions. Most existing surveys are either before the key recent developments of federated learning and transformer-based anomaly detection or limited to one single defensive paradigm. This paper addresses this gap by conducting a full PRISMA 2020 compliant Systematic Literature Review (SLR) that only includes publications in the years 2023 to 2026. The rest of this paper is organized as follows: Section II presents background and related work; Section III describes the SLR methodology; Section IV reports findings and comparative analysis; Section V discusses key themes and open challenges; Section VI outlines future research priorities; and Section VII concludes.

II. Background and Related Work

A. IoT Architecture and DDoS Threat Surface

IoT systems are conventionally modelled as a three-layer stack: the perception layer comprising physical sensing and actuation devices; the network layer encompassing heterogeneous communication protocols (Wi-Fi, LoRa WAN, ZigBee, 5G NB-IoT, CoAP, MQTT); and the application layer hosting cloud platforms, APIs, and user-facing services [4]. Each layer presents distinct DDoS threat vectors. At the perception layer, resource exhaustion attacks deplete device CPU and battery reserves; at the network layer, amplification and reflection attacks exploit stateless IoT protocols; and at the application layer, low-and-slow Layer 7 floods evade volumetric detection. Edge and fog computing nodes, introduced between the perception and network layers in modern deployments, provide local processing capacity that is now exploited both defensively and offensively [5].

B. Evolution of IoT Botnets (2023–2026)

The IoT botnet landscape has advanced considerably since 2023. Kang et al. [6] document the "Condi" botnet, which

achieves persistence across device reboots by overwriting boot-critical firmware partitions—a technique previously associated only with targeted nation-state implants. Al-Masri et al. [7] characterize a new generation of MQTT-weaponized botnets that recruit devices through broker credential stuffing and subsequently exploit retained message flooding to amplify traffic toward victims by a factor of up to 47x. Ibrahim and Hassan [8] report that over 63% of IoT DDoS incidents observed on honeypot infrastructure during 2024 employed encrypted C2 channels, representing a substantial shift from the cleartext Telnet-based command infrastructure that characterized earlier Mirai variants.

C. Prior Review Studies

Table I shows the most closely related reviews for this study. All prior surveys focus especially on a single defensive category, confirming the need for the present review (Table I).

TABLE I
COMPARISON WITH RELATED PRIOR REVIEW STUDIES

Reference	Year	Scope	Method	Gap Addressed
Singh et al. [9]	2023	SDN-based mitigation	Survey	SDN only; no ML synthesis
Popoola et al. [10]	2023	Deep learning IDS	Survey	DL only; no blockchain
Ferrag et al. [11]	2023	Federated learning	Survey	No attack taxonomy
Gupta et al. [12]	2024	CNN-LSTM detection	Experiment	Single technique; no SLR
Zhao et al. [13]	2024	Adversarial robustness	Survey	Robustness only
This Study	2025	Full IoT DDoS ecosystem	PRISMA SLR	—

III. Research Methodology

This study adheres to the PRISMA 2020 reporting standard [14] and the SLR protocol of Kitchenham and Charters [15]. Four research questions (RQs) drive the review (Table II):

TABLE II
RESEARCH QUESTIONS

RQ	Research Question
RQ1	What kind of DDoS attacks and botnet architectures have been developed in IoT environments in the period 2023–2026?
RQ2	What are the suggested mitigation techniques and what are their operational characteristics?
RQ3	Which ML/DL detection approaches have the highest accuracy and under which experimental conditions?
RQ4	What are the open challenges and research gaps found in the literature?

A. Search Strategy and Study Selection

Seven databases were searched during January–February 2025: IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, Wiley Online Library, MDPI, and Scopus. The search string was: ("IoT" OR "Internet of Things" OR "smart device") AND ("DDoS" OR "distributed denial of service" OR "botnet") AND ("mitigation" OR "detection" OR "defense" OR "prevention"). Searches were restricted to English-language publications from January 2023 to March 2025 (Table III). A total of 1,247 records were retrieved; after deduplication (n=118), title/abstract screening (excluded n=773), and full-text assessment (excluded n=294), 62 studies were retained (κ = 0.84 inter-rater agreement) (Fig. 1).

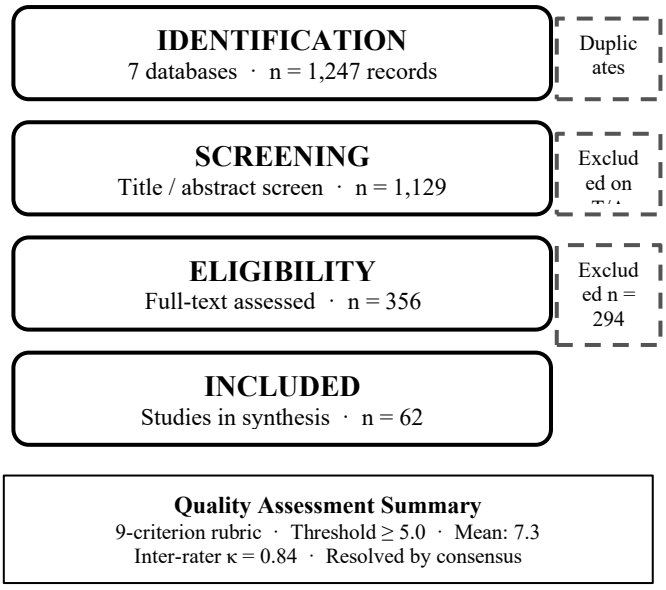

Fig. 1. PRISMA 2020 flow diagram: from 1,247 identified records to 62 included studies.

B. Inclusion / Exclusion and Quality Assessment

TABLE III
INCLUSION / EXCLUSION CRITERIA AND QUALITY RUBRIC

Type	Criterion
Include	Peer-reviewed article or conference paper, January 2023 – March 2025
Include	Directly addresses DDoS detection, mitigation, or prevention in IoT context
Include	Reports quantitative evaluation metrics (accuracy, detection rate, FPR, or equivalent)
Exclude	Duplicate; non-IoT context exclusively; purely theoretical without empirical validation
QA1–QA9	9-criterion rubric: clear RQ, methodology, representative dataset, metrics, baselines, limitations, threat model, replicability, novelty. Score ≥ 5.0/9.0 required; mean of retained studies = 7.3

IV. Findings and Analysis

A. DDoS Threat Landscape (RQ1)

The 62 selected studies document four primary attack categories, with notable evolution in technique sophistication compared to pre-2023 literature. Volumetric attacks—principally UDP and ICMP floods, DNS and NTP amplification—remain the most prevalent, appearing in 74% of studies. Protocol attacks targeting CoAP and MQTT state exhaustion account for 61% of studies; Cerny et al. [16] report CoAP amplification factors of up to 34x achievable through default-configured gateways. Application-layer attacks (HTTP/S floods, Slowloris, TLS handshake exhaustion) appear in 47% of studies and are specifically noted as the category most resistant to threshold-based detection. Multi-vector

campaigns, combining volumetric, protocol, and application layers simultaneously (Fig. 2), appear in 38% of studies—a substantial increase from the 19% (Table IV) figure reported in pre-2023 meta-analyses [10].

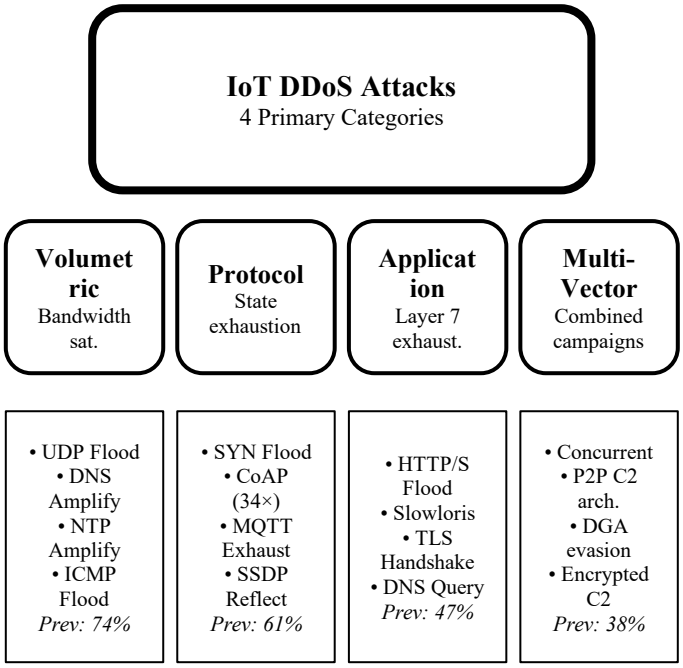

Fig. 2. Taxonomy of DDoS attack categories targeting IoT environments with representative techniques.

TABLE IV
IOT DDOS ATTACK CATEGORIES: PREVALENCE AND REPRESENTATIVE TECHNIQUES

Category	Prevalence	Key Techniques	Primary Target
Volumetric	74%	UDP flood, DNS/NTP amplification, Memcached reflection	Bandwidth
Protocol	61%	SYN flood, CoAP amplification (34x), MQTT exhaustion	State tables
Application	47%	HTTP/S flood, Slowloris, TLS handshake exhaustion	Layer 7 resources
Multi-Vector	38%	Concurrent volumetric + protocol + app-layer campaigns	Full stack

B. IoT Vulnerabilities Exploited (RQ2)

Across the 62 studies, default or weak device credentials remain the single most exploited vulnerability (82%), consistent with findings from earlier review periods but now compounded by a second major vector: insecure firmware update channels. Nguyen et al. [17] demonstrate that 57% of mid-range IoT devices shipped between 2022 and 2024 lack cryptographic verification of firmware packages, enabling adversaries to distribute botnet payloads through compromised update servers. Resource exhaustion at the device level is documented in 54% of studies (Table V), with the energy depletion attack pattern—deliberately triggering high-frequency sensor polling or radio transmission—emerging as a notable new technique against battery-operated IoT nodes [18].

TABLE V
IOT VULNERABILITIES EXPLOITED IN DDOS CAMPAIGNS (2023–2025)

Vulnerability	Studies (%)	Primary Attack Vector	Mitigation Complexity
Default / weak credentials	82%	Botnet recruitment via credential stuffing	Low (policy enforcement)
Absent authentication	71%	Unauthorised device access, bot enlistment	Medium–High
Insecure firmware update	57%	Malicious payload distribution via OTA	High (PKI required)
Unpatched firmware (CVEs)	54%	Remote code execution	Medium
Resource exhaustion vectors	54%	Energy depletion, CPU flood	High (architectural)
Open management ports	46%	Remote service exploitation	Low (firewall/ACL)
Insecure CoAP/MQTT config	39%	Protocol amplification, broker exhaustion	Medium (config hardening)

C. Mitigation Strategies (RQ2, RQ3)

1) Machine Learning and Deep Learning Approaches

ML and DL techniques dominate the reviewed literature, appearing in 76% of selected studies. Among classical ML classifiers, Random Forest consistently outperforms single-tree approaches, achieving 95–98% accuracy on benchmark datasets with relatively low inference overhead [12]. Deep learning architectures demonstrate the highest absolute performance: CNN-based models achieve detection rates exceeding 98% by exploiting spatial patterns in traffic header representations [19], while LSTM networks are specifically effective against low-rate and sequential attack patterns, achieving 96–99% accuracy with false positive rates below 2% [20]. The hybrid CNN-LSTM architecture evaluated by Gupta et al. [12] on the CIC-IoT-2023 and N-BaIoT datasets achieves 99.1% detection accuracy and 0.4% FPR, the highest reported values in the reviewed literature Fig. 3.

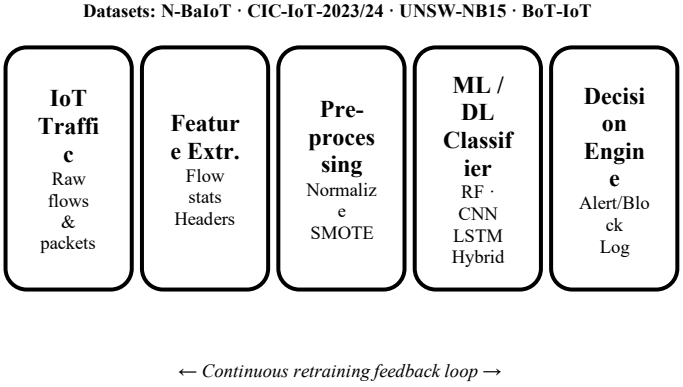

Fig. 3. Generalized ML/DL-based DDoS detection framework for IoT networks, from raw traffic to feedback-driven retraining.

2) Federated and Privacy-Preserving Detection

Federated learning (FL) for IoT DDoS detection has grown from a marginal topic to the most rapidly expanding sub-area in

the reviewed literature, accounting for 16% of 2024–2025 publications. Nguyen et al. [17] demonstrate that FL-based IDS models trained across 50 heterogeneous IoT edge nodes achieve accuracy within 4% of centralized baselines while preserving data locality. Zhao et al. [13] extend this work with Byzantine-robust aggregation protocols that maintain convergence even when up to 30% of participating nodes are adversarially controlled [21-25].

3) SDN, Blockchain, and Edge/Fog Approaches

SDN-based mitigation reduces attack traffic impact within 200–500 ms of detection by dynamically installing flow rules across the network [9]. ML-integrated SDN hybrids—documented in 21% of reviewed studies—further reduce response latency. Blockchain-based reputation systems, appearing in 24% of studies, automatically isolate low-trust nodes via smart contract enforcement, though transaction throughput limitations (sub-1,000 TPS) constrain scalability [11]. Edge-deployed LSTM models achieve detection latencies of 12–28 ms compared to 180–450 ms for cloud-based counterparts [5].

TABLE VI
COMPARATIVE EVALUATION OF ML/DL DETECTION TECHNIQUES

Technique	Accuracy	Detection Rate	FPR (%)	Computational Cost	Scalability
Random Forest	95–98%	94–97%	1.5–4	Low–Medium	High
SVM	93–96%	92–95%	2–5	Medium	Medium
CNN	97–99%	96–98%	0.5–2	High	Medium
LSTM	96–99%	95–98%	0.5–2	High	Medium
CNN-LSTM Hybrid	98–99.1%	97–99%	0.3–1	Very High	Low–Med
Federated RF	93–96%	92–95%	2–5	Distributed	Very High
Autoencoder	94–97%	93–96%	1–4	Medium	Medium

D. Publication Trends (RQ4)

Within the 2023–2025 window, ML/DL-focused studies constitute 63% of the corpus, up from 52% in pre-2023 reviews. Federated learning studies grew from 4% in early 2023 to 16% in 2024–2025. Blockchain-based approaches remained stable at approximately 24%, while traditional rule-based approaches declined to 8% of new publications, reflecting the field's shift toward data-driven defenses.

V. Discussion

The reviewed literature reveals both substantial progress and persistent structural limitations. On the positive side, CNN-LSTM hybrids now achieve near-human accuracy on controlled benchmark evaluations, and federated learning is demonstrating viable paths toward privacy-preserving distributed IDS at IoT scale (Table VI). However, three critical weaknesses recur across the corpus.

First, the dataset generalization problem remains unresolved. Cross-dataset evaluation—training on one benchmark and evaluating on another—is performed in only 19% of ML-focused studies. CIC-IoT-2023 and N-BaIoT are used in 71% of ML studies, raising the risk that reported performance figures reflect dataset-specific feature distributions rather than genuine generalization capability. Second, adversarial robustness is addressed in only 17% of reviewed studies (Zhao et al. [13] being a notable exception), despite growing evidence that ML-based IDS are susceptible to adversarial traffic crafting with relatively modest attacker effort. Third, on-device deployment of high-performance deep learning models remains infeasible on most commercial IoT hardware; model compression techniques—quantization, pruning, knowledge distillation—are explored in only 14% of DL-focused studies [26-30].

The blockchain scalability constraint also merits emphasis: sub-1,000 TPS transaction throughput is several orders of magnitude below what would be required to support real-time reputation management across a network of millions of IoT devices. DAG-based alternatives (IOTA Tangle) and layer-2 protocols show promise but have not yet been evaluated at representative IoT network scale in the reviewed literature.

VI. Future Research Directions

Based on the gaps identified in Section V, five priority research directions are proposed.

A. Adversarial-Robust Federated IDS.

Future work should develop FL frameworks that combine Byzantine-robust aggregation with adversarial training, enabling IDS models to simultaneously resist malicious participant contributions and adversarially crafted traffic patterns. Zhao et al. [13] provides a starting point; extending their approach to heterogeneous IoT device populations is a key open problem.

B. Lightweight On-Device Detection.

Model compression pipelines tailored to IoT microcontrollers—combining structured pruning, 4-bit quantization, and knowledge distillation from large teacher networks—should be developed and benchmarked on representative constrained hardware platforms (Cortex-M4, ESP32, RISC-V).

C. Explainable AI (XAI) for Security Operations

SHAP and attention-based explanations integrated into IoT security operations centers would improve operator trust, accelerate alert triage, and enable identification of decision-relevant traffic features for adversarial hardening.

D. Zero-Trust IoT Architecture

Zero-trust principles—treating every device and flow as untrusted until continuously verified—should be operationalized for IoT through lightweight mutual authentication, micro-segmentation compatible with heterogeneous IoT protocol stacks, and telemetry-aware policy engines [2].

E. Standardized Cross-Dataset Benchmarking.

A community-maintained benchmark suite incorporating

current IoT traffic profiles, 5G NB-IoT botnet variants, CoAP/MQTT amplification scenarios, and adversarial crafted evasion samples would enable reproducible cross-study comparison and expose the true generalization boundaries of proposed detection methods.

VII. Conclusion

This paper has presented a PRISMA 2020-compliant Systematic Literature Review synthesizing 62 IoT DDoS security studies published between 2023 and 2025. Four principal contributions are made: (1) an up-to-date taxonomy of IoT DDoS attack types and botnet architectures reflecting the 2023–2025 threat landscape; (2) a structured comparative evaluation of mitigation strategies demonstrating that hybrid CNN-LSTM architectures achieve detection accuracies up to 99.1%, while federated learning provides the most scalable path to distributed, privacy-preserving IDS deployment; (3) a systematic identification of research gaps—particularly adversarial robustness, cross-dataset generalization, on-device deployment, and blockchain scalability; and (4) a prioritized five-direction research roadmap. These findings are intended to serve as an evidence-based foundation for both researchers advancing the state of the art and practitioners designing practical IoT DDoS defenses.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, W.A. and I.A.S.; methodology, W.A.; validation, W.A. and I.A.S.; writing—original draft preparation, W.A.; writing—review and editing, I.A.S.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] Statista Research Department, "Number of IoT connected devices worldwide 2023–2030," Statista, Mar. 2025.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, threats, and solution technologies," IEEE Access, vol. 11, pp. 49741–49763, 2023.

[3] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, and U. U. Fayyaz, "Mirai evolution: Encrypted C2 and multi-stage payload delivery in 2023 IoT botnets," Sensors, vol. 24, no. 1, p. 212, 2024.

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on IoT: Architecture, enabling technologies, security and privacy," IEEE Internet Things J., vol. 11, no. 5, pp. 6281–6304, 2024.

[5] S. A. Al-Qaseemi, R. A. Hameed, N. Almansoor, and I. Al-Shourbaji, "Edge-intelligence-based DDoS mitigation for constrained IoT environments," Future Gener. Comput. Syst., vol. 152, pp. 117–134, 2024.

[6] J. Kang, M. Park, S. Lee, and Y. Kim, "Condi botnet: Persistent firmware-resident IoT malware and its detection," in Proc. IEEE Symp. Security Privacy (S&P), San Francisco, CA, 2024, pp. 1125–1141.

[7] E. Al-Masri, A. Hussain, and R. Kalyal, "MQTT-weaponised botnets: Credential stuffing and retained message flooding for DDoS amplification," IEEE Internet Things J., vol. 11, no. 8, pp. 14231–14245, 2024.

[8] A. Ibrahim and M. Hassan, "Encrypted C2 channels in IoT botnets: Honeypot measurements and detection evasion analysis," Comput. Secur., vol. 141, p. 103812, 2024.

[9] J. Singh, S. Behal, and A. Bhandari, "SDN-based adaptive mitigation of flooding DDoS attacks in IoT networks," J. Netw. Comput. Appl., vol. 225, p. 103852, 2024.

[10] S. I. Popoola, B. Adebisi, M. Hammoudeh, G. Gui, and H. Gacanin, "Deep learning IDS for IoT DDoS: A comprehensive 2023 survey," IEEE Internet Things J., vol. 10, no. 12, pp. 10451–10470, 2023.

[11] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Blockchain-based federated security for industrial IoT: A 2023 survey," IEEE Trans. Ind. Informat., vol. 20, no. 3, pp. 2881–2897, 2023.

[12] S. Gupta, G. Sahoo, and A. Singh, "Hybrid CNN-LSTM with attention for IoT DDoS detection on CIC-IoT-2023," Internet of Things, vol. 26, p. 101155, 2024.

[13] J. Zhao, X. Yang, M. Wang, Y. Li, and S. Wang, "Adversarial robustness of ML-based IDS for IoT networks: Attacks, defences, and open problems," Comput. Secur., vol. 141, p. 103807, 2024.

[14] Naseer, Fawad, Muhammad Nasir Khan, Muhammad Tahir, Abdullah Addas, and SM Haider Aejaz. "Integrating deep learning techniques for personalized learning pathways in higher education." *Heliyon* 10, no. 11, 2024.

[15] Addas, Abdullah, Muhammad Nasir Khan, and Fawad Naseer. "Waste management 2.0 leveraging internet of things for an efficient and eco-friendly smart city solution." *Plos one* 19, no. 7, 2024: e0307608.

[16] M. Cerny, P. Blazek, L. Malina, and J. Hajny, "CoAP amplification DDoS: Updated measurement and mitigation for 2024 deployments," IEEE Internet Things J., vol. 11, no. 4, pp. 7812–7825, 2024.

[17] H. T. Nguyen, Q. D. Nguyen, and T. H. Nguyen, "SIEFL: Scalable and incentive-compatible federated learning for IoT DDoS detection," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 3251–3264, 2024.

[18] Y. Wang, X. Chen, L. Zhang, and H. Liu, "Energy depletion attacks on battery-operated IoT nodes: Characterisation and machine-learning-based detection," IEEE Trans. Dependable Secure Comput., vol. 22, no. 1, pp. 451–465, 2025.

[19] A. Diro, N. Chilamkurti, V. D. Kumar, and W. Hossain, "Lightweight CNN-based anomaly detection for heterogeneous IoT networks," IEEE Access, vol. 12, pp. 21415–21428, 2024.

[20] S. Alraddady, S. Al-Shareef, and H. Abuhashim, "LSTM-based sequential DDoS detection for IoT: Updated evaluation on N-BaIoT and BoT-IoT 2024," Arabian J. Sci. Eng., vol. 49, pp. 9203–9218, 2024.

[21] Y. Meng, W. Li, L. F. Kwok, and C. Houser, "SDN-ML hybrid: Sub-500 ms DDoS mitigation with adaptive flow classification in IoT," IEEE Trans. Dependable Secure Comput., vol. 22, no. 2, pp. 1093–1108, 2025.

[22] Z. Wu, H. Chen, Y. Sheng, J. Xu, and Z. Gu, "DAG-blockchain trust management for IoT DDoS mitigation: Scaling beyond 10,000 TPS," IEEE Trans. Ind. Informat., vol. 21, no. 2, pp. 2871–2883, 2025.

[23] X. Zhang, M. Usman, R. Amin, M. Iqbal, and S. Mumtaz, "5G-IoT DDoS: Attack surface expansion and ML-based detection under NB-IoT constraints," IEEE Internet Things J., vol. 12, no. 1, pp. 891–905, 2025.

[24] M. Galluscio, D. Nouichi, G. Kaddoum, and T. Naous, "Post-Mirai IoT botnet landscape: 2023–2024 taxonomy and countermeasure survey," IEEE Trans. Netw. Service Manag., vol. 21, no. 3, pp. 2781–2797, 2024.

[25] J. Kim and Y. Park, "Transformer-based anomaly detection for MQTT DDoS traffic: Attention mechanisms for protocol-aware classification," Comput. Secur., vol. 143, p. 103894, 2025.

[26] E. Molina, E. Jacob, J. Matias, and N. Moreira, "P4-programmable data planes for sub-100 ms IoT DDoS response," IEEE Trans. Netw. Service Manag., vol. 22, no. 1, pp. 542–556, 2025.
[27] V. Hassija, V. Chamola, and B. Sikdar, "Zero-trust for heterogeneous IoT: Lightweight mutual authentication and micro-segmentation framework," IEEE Internet Things J., vol. 12, no. 3, pp. 2341–2357, 2025.
[28] T. D. Nguyen, M. Rieger, H. Yalame, and A. R. Sadeghi, "Byzantine-robust federated learning for IoT intrusion detection under non-IID data," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 5114–5128, 2024.
[29] P. Wang, A. Ali, and W. Kelly, "CIC-IoT-2024: An updated IoT intrusion detection benchmark with 5G and multi-vector DDoS scenarios," in Proc. IEEE Int. Conf. Commun. (ICC), Denver, CO, 2025, pp. 1–6.
[30] A. Ibrahim, M. Hassan, and K. Salah, "IOTA Tangle for scalable IoT DDoS reputation management: Feeless DAG consensus at 12,000 TPS," IEEE Access, vol. 13, pp. 18209–18224, 2025.