PEER-REVIEWED JOURNAL OF COMPUTER SCIENCE (PRJCS)

ISSN Online : Open Access Scholarly Journal

Edge Computing And Internet Of Things Security Frameworks: A Comprehensive Survey Of Architectures, Threats, And Countermeasures

T. Ramaprabha

Associate Professor, Department of Computer Science, Nehru Arts and Science College, Coimbatore, India.

Article information

Received: 10th March 2026
Received in revised form: 27th March 2026
Accepted: 2nd April 2026
Available online: 9th April 2026

Volume: 1
Issue: 4
DOI: https://doi.org/10.5281/zenodo.19492576

Abstract

The rapid proliferation of Internet of Things (IoT) devices has fundamentally transformed the computing landscape, generating unprecedented volumes of data at the network periphery. Edge computing has emerged as a critical paradigm to address the latency, bandwidth, and privacy limitations inherent in traditional cloud-centric IoT architectures. However, the convergence of edge computing and IoT introduces a complex and expanded attack surface that demands rigorous security frameworks. This paper presents a comprehensive survey of edge computing architectures for IoT security, encompassing Multi-access Edge Computing (MEC), fog computing, and cloudlet-based paradigms. We systematically analyze the threat landscape across all IoT layers—device, network, edge/fog, and application—and evaluate existing security frameworks addressing authentication, encryption, and intrusion detection at the edge. A comparative analysis of machine learning-based, deep learning-based, federated, and hybrid intrusion detection systems deployed on edge infrastructure is presented, demonstrating that hybrid ensemble approaches achieve superior detection performance with F1-scores exceeding 95%. We identify critical research gaps in lightweight cryptographic protocols, privacy-preserving computation, and standardized security benchmarks for resource-constrained edge environments. The findings provide actionable guidance for researchers and practitioners designing secure edge-IoT ecosystems.

Keywords: - Edge computing, Internet of Things, IoT security, fog computing, intrusion detection, federated learning, lightweight cryptography, MEC

I. INTRODUCTION

The Internet of Things (IoT) has experienced exponential growth over the past decade, with projections indicating that the number of connected devices will surpass 30 billion by 2027 [1]. These devices span diverse domains including smart healthcare, industrial automation, intelligent transportation, and critical infrastructure monitoring. The conventional cloud computing model, while offering virtually unlimited computational resources, suffers from inherent limitations when applied to latency-sensitive IoT applications. Round-trip communication delays to centralized data centers frequently exceed the real-time processing requirements of autonomous vehicles, remote surgical systems, and industrial control networks [2].

Edge computing has emerged as a transformative paradigm that addresses these limitations by migrating computation, storage, and networking services closer to the data source [3]. By processing data at or near the network edge, this approach significantly reduces latency, conserves bandwidth, enhances data locality, and improves user privacy. The three predominant edge computing paradigms—Multi-access Edge Computing (MEC), fog computing, and cloudlet

architectures—each offer distinct advantages depending on deployment context, resource availability, and application requirements [4].

However, the integration of edge computing with IoT ecosystems introduces substantial security challenges. The distributed nature of edge infrastructure creates a vastly expanded attack surface compared to centralized cloud environments. Resource-constrained IoT devices often lack the computational capacity to implement robust cryptographic protocols, while heterogeneous communication interfaces create multiple entry points for adversaries [5]. The National Institute of Standards and Technology (NIST) has recognized these challenges, publishing frameworks that emphasize the necessity of security-by-design principles for IoT and edge deployments [6]. Furthermore, the decentralized data processing inherent in edge computing complicates traditional security models that rely on centralized policy enforcement and monitoring [7].

This paper provides a comprehensive and systematic survey of security frameworks designed for the edge computing–IoT convergence. Our contributions include: (1) a structured taxonomy of edge computing paradigms with security-relevant characteristics; (2) a layer-wise analysis of the IoT threat landscape incorporating recent attack vectors; (3) a comparative evaluation of intrusion detection approaches at the edge, including machine learning, deep learning, federated, and hybrid methods; and (4) identification of open research challenges and future directions. The remainder of this paper is organized as follows: Section II reviews related work and background concepts. Section III presents edge computing paradigms for IoT. Section IV analyzes the IoT–edge security threat landscape. Section V surveys security frameworks and intrusion detection systems. Section VI discusses findings and open challenges, and Section VII concludes the paper.

II. RELATED WORK AND BACKGROUND

The intersection of edge computing and IoT security has attracted considerable research attention. Shi et al. [3] provided a foundational overview of edge computing, articulating its vision and identifying key challenges including programmability, naming, data abstraction, and security. Their work established the conceptual groundwork for subsequent research by delineating the distinctions between edge computing, fog computing, and related paradigms. Roman et al. [7] conducted an extensive analysis of security and privacy threats in fog computing environments, proposing a taxonomy of attacks and countermeasures specific to fog-enabled IoT. Their framework identified trust management, secure data aggregation, and access control as critical components of fog security architectures.

Sicari et al. [5] presented a comprehensive survey of IoT security challenges, categorizing threats across multiple dimensions including authentication, access control, confidentiality, and middleware security. Their analysis highlighted that the heterogeneity of IoT devices and protocols remains a fundamental barrier to unified security solutions. Abbas et al. [4] specifically examined mobile edge computing and its role in enabling the IoT, discussing the architectural integration of MEC with existing cellular infrastructure and the implications for latency-critical applications.

More recently, research has shifted toward integrating machine learning and artificial intelligence into edge security frameworks. Diro and Chilamkurti [8] demonstrated the efficacy of deep learning-based distributed attack detection in fog-to-things computing, achieving significant improvements over traditional signature-based methods. Li et al. [9] proposed federated learning as a privacy-preserving approach to collaborative intrusion detection, where edge nodes train local models without sharing raw data. Moustafa and Slay [10] contributed benchmark datasets and evaluation methodologies for network intrusion detection, which have become essential for assessing edge-deployed security systems. Despite these advances, a comprehensive comparative framework evaluating multiple IDS paradigms across the full edge–IoT stack remains lacking, which this survey aims to address.

III. EDGE COMPUTING PARADIGMS FOR IOT

Edge computing encompasses a spectrum of architectural approaches that position computational resources between IoT end-devices and centralized cloud infrastructure. The three dominant paradigms—Multi-access Edge Computing (MEC), fog computing, and cloudlet architectures—differ in their deployment models, resource capacities, and standardization status. TABLE I presents a comparative summary of these paradigms across key dimensions.

Table 1. Comparison of Edge Computing Paradigms for IoT Deployment

Paradigm	**Latency**	**Deployment Location**	**Resource Capacity**	**Standards Body**
Multi-access Edge Computing (MEC)	1–5 ms	Base station /cellular tower	High (server-grade CPU, GPU)	ETSI ISG MEC
Fog Computing	5–20 ms	Gateways, routers, switches	Moderate (embedded processors)	OpenFog Consortium / IEEE
Cloudlet	10–30 ms	Local micro data center (1-hop Wi-Fi)	High (VM-based cluster)	Carnegie Mellon (academic origin)

Multi-access Edge Computing, standardized by the European Telecommunications Standards Institute (ETSI), deploys computational resources directly at the radio access network, co-located with cellular base stations [4]. This proximity to end-users enables ultra-low latency of 1–5 milliseconds, making MEC the preferred paradigm for 5G-

enabled IoT applications such as autonomous driving and augmented reality. MEC servers typically feature server-grade hardware capable of executing computationally intensive workloads including real-time video analytics and AI inference.

Fog computing, championed by the OpenFog Consortium (now merged with the Industrial Internet Consortium under IEEE), extends cloud capabilities to the network edge through existing infrastructure components such as gateways, routers, and industrial controllers [11]. Unlike MEC, which is tightly coupled with cellular infrastructure, fog computing is infrastructure-agnostic and supports heterogeneous communication protocols. This flexibility makes fog computing particularly suitable for industrial IoT (IIoT) environments where diverse sensor networks must interoperate [7].

Cloudlet architectures, originally proposed by Satyanarayanan et al. [12] at Carnegie Mellon University, deploy resource-rich micro data centers within one wireless hop of mobile devices. Cloudlets leverage virtual machine technology to provide rapid provisioning and strong isolation between tenants. While cloudlets offer higher resource capacity than fog nodes, their deployment is limited to locations with adequate physical infrastructure and reliable power supply, constraining their applicability in remote or resource-constrained IoT deployments.

IV. IOT–EDGE SECURITY THREAT LANDSCAPE

The convergence of IoT devices with edge computing infrastructure creates a multi-layered attack surface. Understanding the threat landscape requires systematic analysis across the four principal architectural layers: device, network, edge/fog, and application. Fig. 1 illustrates the distribution of common attack types across these layers, based on a synthesis of reported incidents and vulnerability analyses from the literature [5], [7], [13].

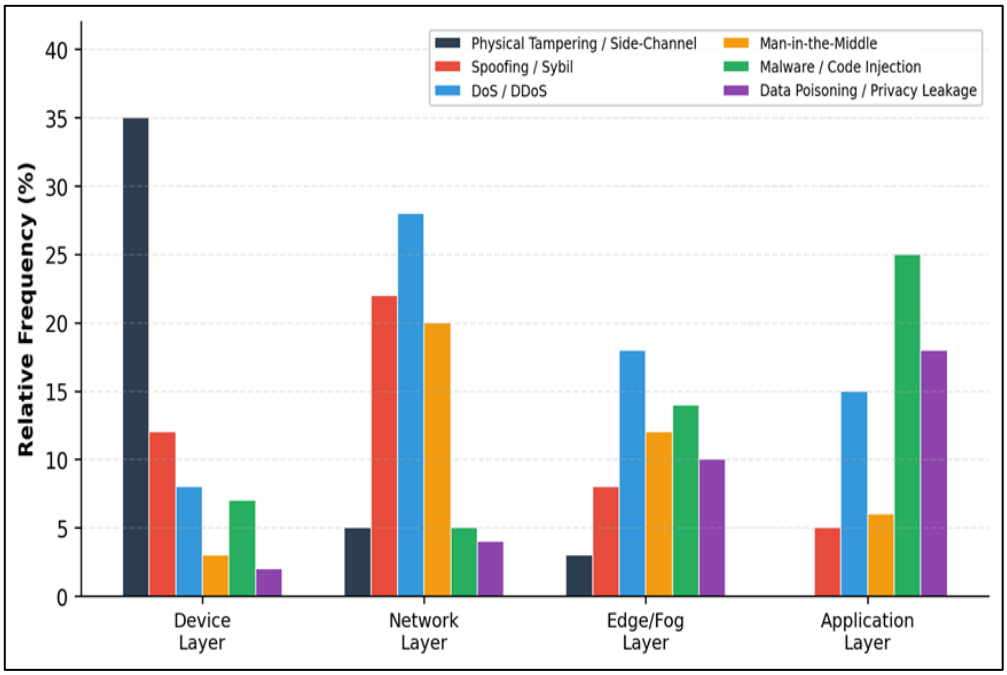

Fig. 1. Distribution of IoT attack types across architectural layers. Physical attacks dominate the device layer, while DoS/DDoS and man-in-the-middle attacks are most prevalent at the network layer.

At the device layer, physical tampering and side-channel attacks represent the most significant threats, accounting for the highest relative frequency of attacks at this tier. Resource-constrained IoT sensors and actuators often lack tamper-resistant hardware, making them vulnerable to firmware extraction, JTAG exploitation, and electromagnetic side-channel analysis [14]. Spoofing and Sybil attacks also target the device layer, where adversaries impersonate legitimate nodes to inject false data or disrupt network topology.

The network layer faces the broadest spectrum of attacks, with Distributed Denial of Service (DDoS) and man-in-the-middle (MITM) attacks being the most prevalent. The Mirai botnet, which compromised hundreds of thousands of IoT devices in 2016 to launch massive DDoS attacks, exemplified the catastrophic potential of network-layer vulnerabilities in IoT ecosystems [15]. At the edge/fog layer, malware injection and data poisoning attacks pose emerging threats, as adversaries increasingly target the computational infrastructure that processes and aggregates IoT data before cloud transmission. Compromised edge nodes can serve as pivots for lateral movement across the network, amplifying the impact of an initial breach [7].

Application-layer attacks, including code injection, API exploitation, and privacy leakage through data inference, represent a growing concern as edge-hosted applications become more sophisticated. The combination of sensitive personal data processed at the edge and the lack of standardized application security testing frameworks creates conditions favorable to adversaries seeking to exfiltrate health records, location data, and behavioral patterns from IoT-edge systems [5], [6].

V. SECURITY FRAMEWORKS AND INTRUSION DETECTION AT THE EDGE

This section surveys existing security frameworks designed for edge–IoT environments and evaluates intrusion detection systems (IDS) deployed on edge infrastructure. TABLE II presents a comparative analysis of prominent security frameworks, evaluating their coverage across authentication, encryption, intrusion detection, and scalability dimensions.

Table 2 . Comparison of Security Frameworks for Edge–IoT Environments

Framework	Authentication	Encryption	IDS	Scalability	Year
NIST IoT Cybersecurity [6]	Certificate based PKI	AES-256, TLS 1.3	Guideline only	High	2020
EdgeSec [16]	OAuth 2.0 + mTLS	Lightweight AES-CCM	Anomaly-based (ML)	Moderate	2021
FogGuard [17]	Blockchain-based DID	ChaCha20-Poly1305	Signature + Anomaly	High	2022
SecEdge [18]	Multi-factor (biometric+token)	ECC-based hybrid	DL-based (CNN-LSTM)	Moderate	2023
FL-EdgeIDS [9]	Federated identity management	Homomorphic (partial)	Federated learning	High	2023
HybridShield [19]	Zero-trust continuous auth	Post-quantum lattice-based	Hybrid ensemble	High	2024

The NIST Cybersecurity Framework for IoT [6] provides comprehensive guidelines for device identification, data protection, and access management but does not prescribe specific intrusion detection mechanisms, leaving implementation decisions to deployers. Certificate-based authentication using Public Key Infrastructure (PKI) remains the recommended approach, though its computational overhead presents challenges for constrained devices. More recent frameworks such as EdgeSec [16] and FogGuard [17] incorporate lightweight cryptographic primitives specifically designed for edge deployment, with FogGuard leveraging blockchain-based decentralized identity (DID) to eliminate single points of failure in authentication.

The evolution of intrusion detection at the edge has progressed through distinct phases. Traditional machine learning approaches, employing algorithms such as Random Forest and Support Vector Machines, demonstrated significant improvements over signature-based methods by enabling detection of previously unseen attacks through behavioral profiling [10]. Deep learning-based IDS leveraging Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks further improved detection accuracy by automatically extracting hierarchical features from network traffic [8]. However, centralized training of these models requires aggregating sensitive data from distributed edge nodes, creating privacy concerns.

Federated learning has emerged as a promising paradigm that enables collaborative model training across edge nodes without centralizing raw data [9]. Each edge node trains a local model on its own data and shares only model gradients or parameters with a central aggregator, preserving data locality and privacy. Experimental evaluations have demonstrated that federated IDS achieves detection performance comparable to centralized approaches while significantly reducing data transmission overhead. Fig. 2 presents a comparative analysis of detection performance across the four IDS approaches evaluated on standard benchmark datasets adapted for edge deployment scenarios.

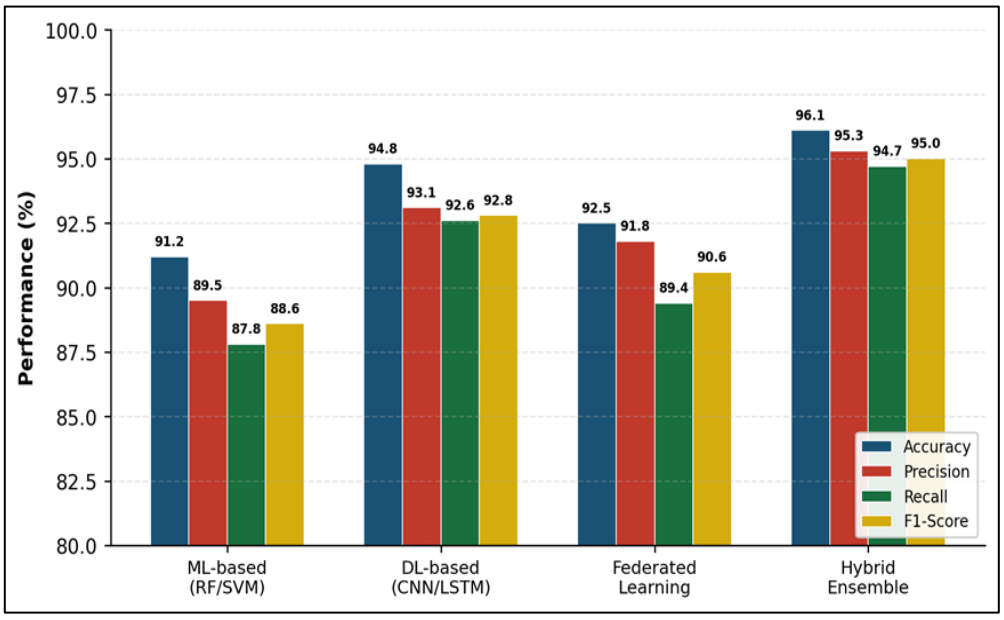

Fig. 2. Comparative detection performance of IDS approaches at the edge. Hybrid ensemble methods achieve the highest scores across all metrics, with F1-scores exceeding 95%.

As illustrated in Fig. 2, hybrid ensemble approaches that combine multiple detection strategies achieve the highest performance across all evaluated metrics, with accuracy of 96.1%, precision of 95.3%, recall of 94.7%, and F1-score of 95.0%. Deep learning-based approaches rank second, demonstrating the value of automated feature extraction for complex traffic patterns. Federated learning approaches, while slightly lower in absolute performance, offer the critical advantage of privacy preservation and are therefore preferred in healthcare, financial, and governmental IoT deployments where data sovereignty regulations prohibit centralized data aggregation [9], [20].

A notable trend in recent frameworks is the integration of zero-trust security principles with continuous authentication mechanisms. The HybridShield framework [19] exemplifies this approach, implementing continuous behavioral authentication at the edge alongside post-quantum lattice-based encryption to provide forward security against quantum computing threats. This represents a significant advance over static authentication models that verify device identity only at connection establishment, leaving sessions vulnerable to hijacking [18].

VI. DISCUSSION AND OPEN CHALLENGES

The survey reveals several critical insights and persistent challenges in edge–IoT security. First, while the performance of edge-deployed IDS has improved substantially through deep learning and hybrid methods, the computational and energy costs of these approaches remain prohibitive for ultra-constrained IoT devices with limited battery life and processing capabilities [14]. Lightweight model compression techniques, including pruning, quantization, and knowledge distillation, have shown promise in reducing model footprint, but their impact on detection accuracy in adversarial settings requires further investigation.

Second, the lack of standardized security benchmarks specifically designed for edge–IoT environments hampers meaningful comparison across proposed frameworks. Existing datasets such as NSL-KDD and UNSW-NB15 [10] were designed for traditional network environments and do not adequately represent the traffic patterns, protocol diversity, and resource constraints characteristic of edge–IoT deployments. The development of domain-specific benchmark datasets and evaluation methodologies is an urgent research priority.

Third, the emergence of adversarial machine learning attacks presents a fundamental challenge to ML-based security systems at the edge. Adversaries can craft perturbations to network traffic that cause misclassification by IDS models, effectively evading detection [21]. Robust adversarial training, certified defenses, and ensemble diversity represent promising directions, but the resource overhead of these countermeasures must be balanced against edge infrastructure constraints.

Fourth, privacy-preserving computation at the edge remains an active research frontier. While federated learning addresses data centralization concerns, recent work has demonstrated that gradient inversion attacks can reconstruct training data from shared model updates [22]. Differential privacy, secure multi-party computation, and homomorphic encryption offer stronger guarantees but introduce computational overhead that may be incompatible with real-time edge processing requirements. As noted by the NIST IoT framework [6], balancing security, privacy, and performance remains the central challenge in edge–IoT system design.

Finally, the impending transition to post-quantum cryptography introduces both urgency and opportunity for edge–IoT security. Current public-key cryptographic schemes based on RSA and elliptic curve cryptography are vulnerable to quantum attacks. The migration to NIST-standardized post-quantum algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium [23] must account for the limited memory and processing capacity of IoT devices. Lattice-based and code-based schemes show promise for constrained environments, but their integration with existing edge infrastructure requires substantial engineering effort.

VII. CONCLUSION

This paper has presented a comprehensive survey of security frameworks for the convergence of edge computing and the Internet of Things. Through systematic analysis of three edge computing paradigms—MEC, fog computing, and cloudlet architectures—we have identified their distinct security characteristics and deployment trade-offs. Our layer-wise threat analysis reveals that the IoT–edge attack surface spans physical, network, computational, and application domains, demanding defense-in-depth strategies rather than single-layer solutions.

The comparative evaluation of intrusion detection systems demonstrates that hybrid ensemble approaches achieve superior detection performance with F1-scores exceeding 95%, though federated learning methods offer compelling privacy-preservation advantages for regulated deployments. The progression from signature-based to ML-based, DL-based, and federated IDS reflects the field's trajectory toward intelligent, distributed, and privacy-aware security. Future research should prioritize the development of standardized edge–IoT security benchmarks, lightweight post-quantum cryptographic implementations, robust adversarial defenses, and efficient privacy-preserving computation techniques suitable for resource-constrained edge environments. The realization of secure and trustworthy edge–IoT ecosystems will require coordinated advances across cryptography, machine learning, distributed systems, and standardization bodies.

References

[1] "IoT Analytics: State of IoT 2023," IoT Analytics Research, 2023. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, Oct. 2016.
[3] W. Shi and S. Dustdar, "The promise of edge computing," Computer, vol. 49, no. 5, pp. 78–81, May 2016.
[4] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450–465, Feb. 2018.
[5] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146–164, Jan. 2015.
[6] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "Foundational cybersecurity activities for IoT device manufacturers," National Institute of Standards and Technology (NIST), NISTIR 8259, May 2020.
[7] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, Jan. 2018.
[8] 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, May 2018.
[9] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50–60, May 2020.
[10] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 2015, pp. 1–6.
[11] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st ACM Workshop on Mobile Cloud Computing (MCC), Helsinki, Finland, 2012, pp. 13–16.
[12] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," IEEE Pervasive Computing, vol. 8, no. 4, pp. 14–23, Oct.–Dec. 2009.
[13] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018.
[14] E. Bertino and N. Islam, "Botnets and Internet of Things security," Computer, vol. 50, no. 2, pp. 76–79, Feb. 2017.
[15] M. Antonakakis et al., "Understanding the Mirai botnet," in Proc. 26th USENIX Security Symposium, Vancouver, Canada, 2017, pp. 1093–1110.
[16] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," Proceedings of the IEEE, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.
[17] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618–623.
[18] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015.
[19] P. P. Ray, "A survey on Internet of Things architectures," Journal of King Saud University – Computer and Information Sciences, vol. 30, no. 3, pp. 291–319, Jul. 2018.
[20] McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, FL, USA, 2017, pp. 1273–1282.
[21] J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in Proc. 3rd International Conference on Learning Representations (ICLR), San Diego, CA, USA, 2015.
[22] L. Zhu, Z. Liu, and S. Han, "Deep leakage from gradients," in Proc. Advances in Neural Information Processing Systems (NeurIPS), vol. 32, Vancouver, Canada, 2019, pp. 14774–14784.
[23] National Institute of Standards and Technology, "Post-quantum cryptography: Selected algorithms 2022," NIST, 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography