



Science Forum (Journal of Pure and Applied Sciences)

Journal Homepage: <https://atbuscienceforum.com.ng/index.php/jpas>



Internet of Things (IoT) and Artificial Intelligence of Things (AIoT): A Comprehensive Systematic Review of Architectures, Edge Protocols, Applications, and Open Security Challenges

Dalal Adnan Abbas

Diyala Directorate of Education, Diyala, Iraq

Abstract

The Artificial Intelligence of Things (AIoT) is a new paradigm that emerged from the quick convergence of artificial intelligence (AI) and the Internet of Things (IoT). This development marks a shift of networks from merely enabling basic connectivity to being capable of making independent intelligent decisions at the network edge. While the core mission of previous networks was simply to connect devices and transmit data, this transformation is different: at edge locations close to various terminal devices and far from the core network, the network can make its own intelligent judgments and decisions, eliminating the need to send all data back to the core network for processing, which has fundamentally changed the way modern distributed systems process data and take actions. Additionally, it offers a comparative analysis of application-layer protocols including MQTT, CoAP, and AMQP, as well as upcoming standards like Matter and 6G-enabled Ambient IoT. The evaluation highlights the significance of Edge AI in enhancing real-time responsiveness while safeguarding data privacy. Finally, it categorizes the many security risks, including malware, phishing, and data spoofing, and takes into account cutting-edge solutions like blockchain, federated learning, and zero-trust architectures. For academics and professionals studying the intricate relationship between intelligence and connectivity in the contemporary digital age, this book is meant to be a vital resource.

Keywords

Artificial Intelligence of Things AIoT,
Internet of Things (IoT),
Edge Protocols,
System Architectures,
Edge AI,
Open Security Challenges



1. Introduction

From a theoretical network of interconnected items, the Internet of Things (IoT) has developed into a pervasive infrastructure that sustains modern society. IoT has revolutionized a variety of industries, including smart manufacturing and healthcare, by enabling billions of different devices to sense, communicate, and act [6], [16]. The ability of IoT to link the digital and physical realms to create a "smart" environment that adapts to changing environmental circumstances is at its core [47], [51]. Nevertheless, traditional cloud-centered designs face significant latency, bandwidth, and privacy limitations as the datasets generated by these devices reach exabytes [3], [18].

The AIoT is the result of artificial intelligence being integrated into IoT due to the need for localized, real-time intelligence. [37]. AIoT reduces dependency on centralized servers by processing data at the edge using the analytical powers of machine learning (ML) and deep learning (DL)[5], [18], [33]. Because sensitive data may be reviewed without leaving the local area, this combination allows for autonomous decision-making, quicker response times, and stronger privacy guarantees [15], [22], [34]. Despite these benefits, integrating AI into IoT devices with limited resources adds new protocol needs and increases architectural complexity [4], [19].

Furthermore, the increased attack surface of AIoT systems introduces serious security risks. Due to their dynamic and varied characteristics, these networks are vulnerable to a wide range of cyberattacks, such as sophisticated phishing campaigns, distributed denial-of-service (DDoS) attacks, and virus compromise [1], [2], [46]. To solve these issues, a thorough grasp of contemporary

architectural methodologies, communication standards, and security frameworks is required. This paper provides a systematic evaluation of these important components, highlighting important trends and unfilled research gaps, in order to provide a comprehensive assessment of the state of the art in IoT and AIoT research.

2. Methodology

In this systematic review, the corpus of existing literature on the Internet of Things and AIoT was found, assessed, and integrated using a methodical approach. The method was intended to enable a thorough analysis that was sufficiently concentrated on the technological developments influencing the sector.

2.1 Literature Search and Selection

Several academic databases, such as ArXiv and Google Scholar, were used in a comprehensive search. "IoT architectures," "AIoT edge protocols," "AI-driven IoT security," and "edge-cloud orchestration" were the most popular search terms. From an initial batch of 237 distinct papers, the findings were narrowed down to 223 highly relevant articles, with focus on work published between 2019 and 2025. This period has seen the biggest developments in Edge AI, SDN-enabled IoT, and contemporary cybersecurity frameworks.

2.2 Inclusion and Exclusion Criteria

Studies that provided technical information regarding IoT/AIoT architecture layers, presented real-world applications (such healthcare and smart cities), compared communication protocols using empirical or theoretical data, or suggested novel security methods were included. Technically shallow general overview papers were not included. Systematic reviews, mapping studies, and

experimental articles that offered particular insights into SDN, federated learning, and zero-trust models were prioritized during the selection process.

2.3 Synthesis and Analysis

Studies that offered technical information concerning IoT/AIoT architecture layers, illustrated real-world applications (such as healthcare and smart cities), compared communication protocols using theoretical or empirical data, or suggested novel security measures were all included. Technically shallow general overview papers did not exist. Systematic reviews, mapping studies, and experimental works that offered particular insights into SDN, federated learning, and zero-trust models were prioritized during the selection process.

3. Architecture Analysis

The architecture of IoT and AIoT systems include the blueprint for connectivity, data processing, and service delivery. Research indicates that from simple layered models, complex distributed and software-defined frameworks have developed.

3.1 Progression of Layered Models

The Perception, Network, and Application layers make up the fundamental three-layer architecture, which has long been the accepted baseline [6], [11], [21]. However, as IoT systems have grown more intricate, scholars have put out more intricate models, as illustrated in Figure 1

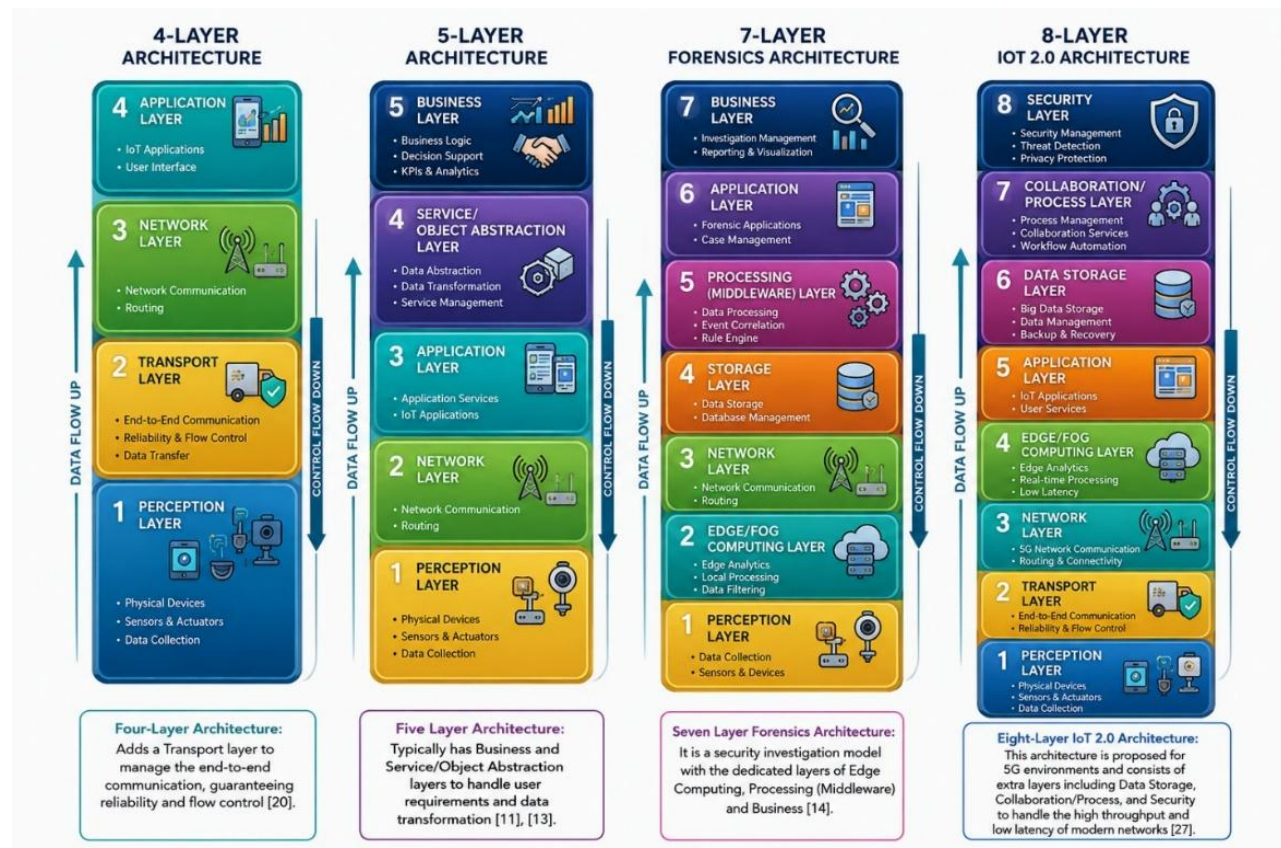


Figure 1: Evolution of IOT Architecture

- **Four-Layer Architecture:** Adds a Transport layer to manage the end-to-end communication, guaranteeing reliability and flow control [20].
- **Five Layer Architecture:** Typically has Business and Service/Object Abstraction layers to handle user requirements and data transformation [11], [13].
- **Seven Layer Forensics Architecture:** It is a security investigation model with the dedicated layers of Edge Computing, Processing (Middleware) and Business [14].
- **Eight-Layer IoT 2.0 Architecture:** This architecture is proposed for 5G environments and consists of extra layers including Data Storage, Collaboration/Process, and Security to handle the high throughput and low latency of modern networks [27].

3.2 Edge-Cloud Orchestration and Hybrid Paradigms

One major change in the AIoT architecture is the transition from centralized cloud processing to the edge-cloud orchestration. This involves a trade-off between the computational power of the cloud and the low-latency agility of the edge nodes [12], [40]. Figure 2 illustrate architectural patterns of Edge-Cloud Data Flow in AIoT. Three major architectural patterns have emerged:

- **Hierarchical Edge-Cloud:** Data is processed in different levels starting from local devices to regional edge gateways and then to the central cloud [8], [9], [12].
- **Collaborative (Split) Inference:** AI model workloads are split between the edge and cloud to optimize resource usage and latency [8], [12].
- **Cloud Backed On-Device Inference:** The device executes critical tasks, while the cloud performs complex historical analysis or model retraining [8], [12].

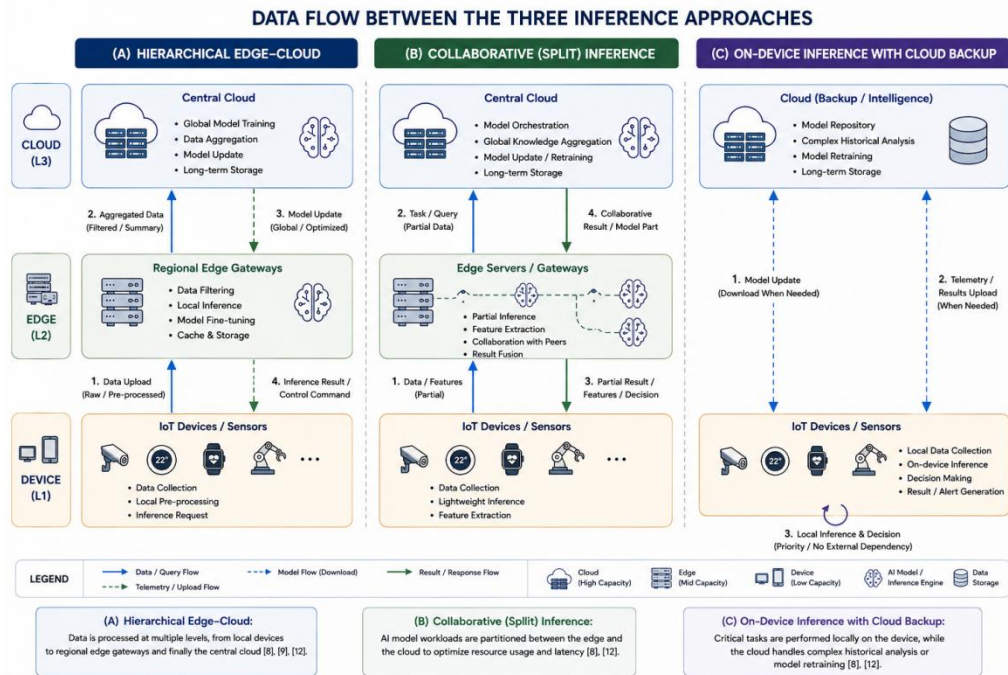


Figure 2: Architectural Patterns of Edge-Cloud Data Flow in AIoT

3.3 Software Defined Networking (SDN) and Network Function Virtualization (NFV)

The advent of SDN-EC-IoT, i.e., Software Defined Networking for Edge Computing, is a great step ahead. This paradigm combines Edge Computing for IoT (EC-IoT) with Software Defined IoT (SDIoT) to resolve the challenges of network management, scalability and heterogeneity [3], [28]. The control plane is decoupled from the data plane in SDN, which can provide more flexible and programmable network configurations. This is critical to handle the huge amount of data in AIoT systems [3], [27]. NFV further enhances this by enabling the deployment of virtualized network functions (VNFs) across the infrastructure, enabling services to be scaled and managed as software [27].

3.4 Cognitive and Modular Hardware

Emerging platforms like VEDLIoT propose a comprehensive strategy using modular and

scalable cognitive hardware [17], [23]. These platforms use microserver technology and are composed of heterogeneous computing elements including special ASICs and FPGAs for hardware acceleration [17], [23]. This modularity supports collaborative solutions of complex deep learning applications on distributed systems, allowing the hardware to be adapted to specific IoT use cases such as automotive or industrial control [17], [23].

3.5 Agentic IoT and Digital Twins

Studies these days are eliminating the limits of the conventional theories in technology to encompass the notion of Agentic IoT, which implies that devices will be hosting autonomous agents capable of making decisions on-site and exchanging data with other agents on the so-called Internet of Agents (IoA) [44]. In addition to this, the integration of the technology of Digital Twins, which creates virtual reality showing the physical property,

together with Multimodal Generative AI contributes to the creation of the most precise simulation processes from AIoT perspective [50].

4. Edge Protocols Comparison

Data exchange in IoT/AIoT networks is largely determined by communication protocols. The protocol may differ based on its bandwidth efficiency, latency, reliability, and resources used by edge devices [4], [11].

4.1 Comparative Analysis of Application Layer Protocols

The following are some leading application layer protocols, which involve different trade-offs:

- **MQTT (Message Queuing Telemetry Transport):** MQTT is a lightweight publish-subscribe messaging protocol. It is well-suited for devices with limited resources due to its low bandwidth usage and small memory requirements [11]. It provides three levels of Quality of Service for reliable communication [4], [13].
- **CoAP (Constrained Application Protocol):** CoAP protocol is based on the client-server request-response model and is optimized for communication in constrained networks and devices [13], [14]. Its use is recommended for stateless environments, where UDP connection will increase efficiency [13].
- **AMQP (Advanced Message Queuing Protocol):** AMQP is a TCP-based protocol providing numerous messaging capabilities, such as messaging queuing and routing; therefore, it is ideal for

complex industrial applications [4], [13].

- **DDS (Data Distribution Service):** DDS is a middleware protocol designed to be data-centric. It enables low-latency communication over peer-to-peer networks, making it perfect for real-time applications, such as healthcare [4], [13], [20].
- **Matter:** An emerging standard designed to overcome different types of devices by implementing a consolidated strategy that operates over Thread, Wi-Fi, and Ethernet.

4.2. Network and Link Layer Protocol Evaluation

To ensure that various physical mediums can communicate, several low-power protocols have been devised.

- **6LoWPAN:** Offers an opportunity to transmit IPv6 packets through low-power wireless networks, thus connecting small sensors to the web. [13], [20].
- **ZigBee and Bluetooth Low Energy (BLE):** Are probably the most used short-range protocol in smart homes and healthcare systems due to their low energy consumption. [11], [20].
- **LoRaWAN and SigFox:** Have been made for long-range communication (with a few kilometers of transmission) with a very low data rate, suitable for smart city sensors and agricultural applications. [11], [13].

- **Ambient IoT and 6G:** This emerging area deals with the use of 6G technology in Ambient IoT. In particular, this technology will enable communication between a huge number of passive or zero-energy sensors. [41].

A comprehensive comparative analysis of application-layer and network-layer edge protocols, detailing their operational characteristics and primary use cases, is summarized in Table 1.

Table 1: Comparative Analysis of Edge Communication Protocols Across Architectural Layers, Energy Efficiency, and Use Cases.

Protocol	Protocol Layer	Transport Protocol	Bandwidth & Overhead	Energy Efficiency	Best Use-Case Scenario
MQTT	Application	TCP	Low / Low	Moderate	Real-time telemetry & pub/sub messaging
CoAP	Application	UDP	Very Low / Minimal	High (Resource-constrained)	Battery-operated IoT & constrained nodes
AMQP	Application	TCP	Medium / High	Low	Enterprise messaging & queuing systems
DDS	Application	UDP / IP	High / Dynamic	Moderate	High-performance, real-time autonomous systems
Matter	Application	Thread / Wi-Fi / Ethernet	Low to Medium	High (over Thread)	Smart home & inter-vendor interoperability
6LoWPAN	Network / Adaptation	IEEE 802.15.4	Low / Minimal	Very High	IPv6 connectivity for low-power wireless networks
BLE	Physical / Link	Short-Range RF	Low / Minimal	Very High (BLE Mesh)	Short-range personal networks & wearables
LoRaWAN	Link / Network	Sub-GHz LPWAN	Very Low / Very Low	Ultra-High	Long-range, low-power remote monitoring

4.3 Protocol Performance and Security Considerations

When deciding on the choice of protocol, one should take into account the specifics of the environment. For instance, MQTT is perfect for many-to-one telemetry systems. At the same time, DDS is better suited for one-to-many and many-to-many real-time data transmissions [4]. The issue of security is also compounded; although it is possible to use TLS to protect MQTT, such a method is impractical for very small sensors, necessitating DTLS for CoAP or some form of specialized lightweight encryption for LoRaWAN [20], [32], [35].

5. Applications of IoT and AIoT

IoT and AIoT are versatile technologies that find applications in a wide variety of areas, all of which benefit from localized intelligence and pervasive connectivity.

5.1 Smart Cities and Public Safety

AIoT plays an essential role in creating smart cities and facilitating the real-time monitoring of cities. It finds application in smart parking, traffic management, and energy efficiency [13], [42]. Edge AI can be applied to public safety activities, which would help detect potential threats such as suspicious behaviors and armed individuals based on sensor and video information [15]. In the realm of disaster relief, IoT applications must work effectively in order to support emergency operations and public safety [13].

5.2 Healthcare and Patient Monitoring

In the healthcare area, IoT devices enable constant patient monitoring and personalized care delivery [9], [12], [43]. AIoT makes these systems better by using real-time analytics for anomaly detection (e.g., detection of irregular heartbeats) and emergency

assistance. Edge AI is useful in terms of preserving privacy since the data is processed locally and therefore not transmitted to the cloud [7], [15]. Research emphasizes the importance of the federated learning as a way of training medical AI applications in various hospitals without transmitting the data [7], [9], [48].

5.3 Industrial IoT (IIoT) and Smart Manufacturing

The main emphasis of the Industrial Internet of Things (IIoT) is to boost efficacy and determination-making in manufacturing systems (Industry 4.0) [4], [38]. The applications of Artificial Intelligence of Things (AIoT) in this area cover predictive maintenance whereby algorithms analyze machinery sensor data and predict breakdowns in advance [4], [15]. In this regard, edge computing is indispensable as it guarantees the necessary reaction time in milliseconds in safety-critical industrial control systems [4], [24]. The marriage between IoT and Programmable Logic Controllers (PLCs) allows for increased automation [53].

5.4 Precision Agriculture and Sustainability

Smart farming is about benefiting from IoT to monitor soil humidity, atmospheric conditions, and crop condition [11], [31]. AIoT adds thinking capacity giving way to creating smart irrigation solutions and models that forecast crop diseases with the help of AI [49]. Distributed computing systems make it possible for farmers to create smart technologies which provide for the necessary work efficiency on farmlands [11], [19]. Green IoT (GIoT) aims at improving energy efficiency and employing energy harvesting solutions [29], [36].

5.5 Autonomous Systems and Smart Transportation

When it comes to autonomous vehicles, the ability to make instantaneous decisions is critical. The role of AIoT is to collect, analyze, and use data from multiple sources like LIDAR, radars, and cameras to help the vehicle make decisions to avoid obstacles while driving [15], [17]. Communication technologies, such as vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication, are an important subject of study that supports the

safe and reliable transmission of information in different environments [16], [39]. Edge AI is responsible for maintaining the security and privacy of information in the Internet of Vehicles (IoV) by focusing on safe communication within this area [15]. To provide a consolidated mapping of real-world deployments, Table 2 synthesizes the core AIoT application domains, highlighting their primary algorithms, edge-value propositions, and optimal communication protocols.

Table 2: Strategic Synthesis of AIoT Application Domains, Underlying Algorithms, Edge Value Propositions, and Optimal Protocols.

Application Domain	Key AI/ML Algorithms	Edge AI Value Proposition	Optimal Protocol
Smart Cities	CNNs, Graph Neural Networks (GNNs), Spatial-Temporal Models	Low-latency traffic orchestration, localized anomaly detection, reduced backhaul bandwidth	MQTT / CoAP
Healthcare (IoMT)	XGBoost, Random Forest, Lightweight Deep Neural Networks	Real-time patient monitoring, zero-latency critical alerts, strict data privacy compliance	CoAP / BLE
Industrial IoT (IIoT)	Autoencoders, LSTM Networks, Reinforcement Learning	Predictive maintenance, ultra-reliable low-latency control, fault isolation	DDS / AMQP
Precision Agriculture	Computer Vision (OpenCV), Decision Trees, Support Vector Machines	Edge-based crop health assessment, automated irrigation, operation in disconnected environments	LoRaWAN / 6LoWPAN
Autonomous Systems	Deep Reinforcement Learning, YOLO, Sensor Fusion Algorithms	Millisecond-level obstacle detection, dynamic path planning, deterministic safety guarantees	DDS / Matter

As demonstrated in Table 2, matching specific algorithmic complexity with appropriate network protocols is critical for maximizing system performance across domain-specific operational constraints.

6. Security Challenges and Defensive Strategies

However, the AIoT ecosystem is threatened by many security challenges. The combination of devices with limited resources, varied devices, and sensitive data makes AIoT very appealing to cybercriminals.

6.1 Categorization of Security Threats

The key threats in IoT and AIoT include:

1. **Distributed Denial-of-Service (DDoS) attack:** Attackers generate excessive traffic that affects the devices or network [1].
2. **Phishing and Malware attacks:** Both phishing and malware can attack the IoT network through various ways [1], [2].
3. **Data Spoofing and Integrity attacks:** Making changes to the data supplied by the sensors, which affects the decision-making process in AI [1], [25].
4. **Phishing Targeting Edge Nodes:** New threats consist of advanced forms of fishing that aim to breach edge nodes and enter the network. [2]
5. **Forensics Dilemmas:** They make probing hacks in IoT a daunting task due to the various machines, devices, and formats involved [14], [20].

6.2 AI-Driven Security Advancements

Artificial Intelligence is regarded as a powerful defense technology. AI systems that are capable of detecting anomalies and prevent intrusions using machine learning algorithms can spot possible threats and prevent them in real time [1], [45]. Edge AIs are capable of becoming local phishing detectors, spotting these online scams right at their source [2]. Also, federated learning allows for creating joint security models without resorting to sharing of sensitive locals' data [1], [9]. XAIoT technologies are on the rise, as they can increase transparency and trust towards the security decision-making processes [35].

6.3 Zero-Trust and Blockchain Integration

Researchers are looking into Zero-Trust Architectures (ZTA) as a means to advance beyond conventional security. ZTA makes use of the "never trust, always verify" principle, continuously verifying every device and user of the network. Additionally, blockchain technology provides a decentralized registry of all communications and transactions, further fortifying ZTA, while guaranteeing the integrity of the data exchanged [26], [52]. The structured taxonomy mapping these major cyber-security threats including DDoS, phishing, and data spoofing to their corresponding AI-driven, federated, and zero-trust defensive frameworks is comprehensively illustrated in Figure 3.

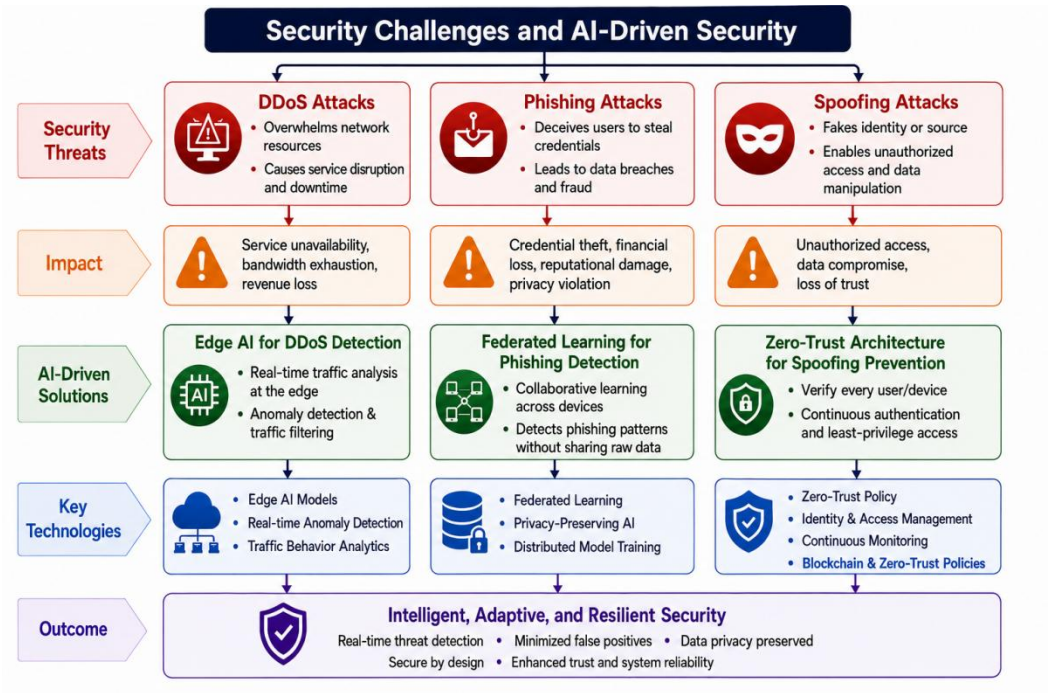


Figure 3: AIoT security threat taxonomy and AI-driven defense framework

6.4 Hardware-Based Security and Trusted Computing

In host security, trusted computing, remote attestation, and secure execution environment techniques are deployed in AIoT hardware platforms like VEDLIoT [17]. These methods allow the device to work with only authorized software code and ensure that the hardware itself has not been modified.

A structured taxonomy of the security landscape is presented in Table 3, which maps primary AIoT threat vectors to their targeted architectural layers and corresponding AI-driven or cryptographic countermeasures.

Table 3: Threat Matrix Mapping AIoT Attack Vectors, Targeted Architectural Layers, and AI-Driven Defensive Mechanisms.

Attack Vector / Threat	Targeted Layer	Primary Impact / Risk	Defensive Mechanism & Technology
DDoS Attacks	Network & Transport Layer	Service disruption, resource exhaustion, bandwidth flooding	Edge AI Anomaly Detection: Real-time traffic filtering and localized intrusion prevention systems (IPS).
Phishing & Credentials Theft	Application & Edge User Layer	Unauthorized system access, credential leakage, fraud	Federated Learning & XAIoT: Localized phishing pattern detection without raw data exposure.
Data & Identity Spoofing	Perception & Physical Layer	Sensor data manipulation, identity impersonation, false injection	Zero-Trust Architecture: Continuous identity verification and least-privilege access policies.
Data Tampering & Integrity	Storage & Communication Layer	Man-in-the-Middle (MitM) attacks, data corruption	Blockchain Integration: Cryptographic immutability and tamper-proof distributed ledgers.
Model Poisoning Attacks	AI/ML Pipeline Layer	Degradation of global AI inference, malicious bias injection	Secure Aggregation & Robust FL: Anomaly-aware model updates and hardware-based Enclaves (TEEs).

This threat matrix underscores the necessity of a multi-layered, defense-in-depth strategy that combines decentralized machine learning with continuous cryptographic verification.

7. Research Gaps and Future Directions

In spite of the notable developments recorded, various challenges are still encountered in the IoT and AIoT environment:

1. **Standardized interoperability:** In relation to the installation of AI models and cross-platform compatibility, the absence of commonly agreed standards, such as Matter protocol opens the way for future expansion of its applicability [2], [10].

2. **Resource-sparing AI:** A major challenge remains to be the creation of lightweight AI models that can function effectively on devices that do not use much energy and openness to the possibility of weak performance [7], [18].

3. **Adaptive security:** Future work must be guided by the development of adaptive AI models that will have the ability to overcome any threats that may arise after the operation of the system has already begun [16].

4. Energy-aware privacy: In order to preserve the information safely, it is essential to ensure energy efficiency as well as safety [7].

5. Zero trust scalability: Bringing together AI, blockchain, as well as zero-trust architectures on a global scale in trillions of devices would create plenty of problems concerning the compatibility [26].

8. Conclusion

The AIoT paradigm, which combines the Internet of Things and artificial intelligence, has opened up countless opportunities for advancement in industries, smart cities, and healthcare. The need for low latency and co-localized intelligence is met by the shift to edge-centric architectures, which is facilitated by Software Defined Networks and modular hardware. The required connectivity is provided via communication protocols like MQTT and CoAP, but the development of some standards, like Matter, has made it possible to achieve interoperability, which has always been a problem.

But the rapid advancement of AIoT technology has surpassed that of security technologies. For these dispersed and diverse networks, the conventional perimeter-based defense techniques are ineffective. The effective implementation of blockchain-based integrity assurance, zero-trust networks, and AI-based threat detection is critical to the future of AIoT. In order to keep the AIoT ecosystem robust and reliable, the research community is expected to address the outstanding problems in the fields of adaptive security and energy-efficient AI.

References

- [1] Q. Chen, L. Tan, J. Tang, and X. Qu, "AI-Enabled IoT Security: A Survey on Advances, Challenges, and Cross-Domain Collaborative Frameworks," *Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence*, Sept. 2025, doi: 10.1145/3773365.3773619.
- [2] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," *IEEE Access*, vol. 11, pp. 36805-36822, 2023, doi: 10.1109/ACCESS.2023.3252366.
- [3] I. E. Kamarudin, M. A. Ameen, M. F. A. Razak, and A. Zabidi, "Integrating Edge Computing and Software Defined Networking in Internet of Things: A Systematic Review," *Iraqi journal for computer science and mathematics*, Nov. 2023, doi: 10.52866/ijcsm.2023.04.04.011.
- [4] R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 503-514, May 2023, doi: 10.48175/ijarsct-11979b.
- [5] A. G. Christou, C. L. Stergiou, V. A. Memos, Y. Ishibashi, and K. E. Psannis, "Revolutionizing Connectivity: The Power of AI, IoT, and Edge Computing for Smart and Autonomous Systems," in *Proc. 2023 6th World Symposium on Communication Engineering (WSCE)*, Thessaloniki, Greece, 2023, pp. 24-29, doi: 10.1109/WSCE59557.2023.10365771.

- [6] S. Kraijak and P. Tuwanut, "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends," pp. 1-6, Jan. 2015, doi: 10.1049/CP.2015.0714.
- [7] P. V. S. Kumar and N. Velmurugan, "From Sensors to Edge Intelligence: A Critical Review of AI-Enabled IoT for Healthcare," *6th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 1098-1103, Sept. 2025, doi: 10.1109/icesc65114.2025.11212327.
- [8] S. Jonnakuti, "Intelligent edge architectures: ai at the boundary of cloud and device," *International Journal of Engineering Technology Research & Management*, 2022, doi:10.5281/zenodo.15455791.
- [9] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan and X. Chen, "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869-904, Secondquarter 2020, doi: 10.1109/COMST.2020.2970550.
- [10] A. Dwarampudi and M. K. Yogi, "Novel Perspectives in Artificial IoT: Current Trends, Research Directions," *Journal of Cyber Security, Privacy Issues and Challenges*, Apr. 2024, doi: 10.46610/jcspic.2024.v03i01.004.
- [11] F. J. Ferrandez-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, and J. Mora-Martínez, "Precision Agriculture Design Method Using a Distributed Computing Architecture on Internet of Things Context.," *Sensors*, vol. 18, no. 6, p. 1731, May 2018, doi: 10.3390/S18061731.
- [12] V. Ramamoorthi, "Exploring AI-Driven Cloud-Edge Orchestration for IoT Applications," *International journal of scientific research in computer science, engineering and information technology*, pp. 385-393, Oct. 2023, doi: 10.32628/cseit239072.
- [13] M. Pradhan, "Interoperability for Disaster Relief Operations in Smart City Environments," *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, 2019, pp. 711-714, doi: 10.1109/WF-IoT.2019.8767169.
- [14] D. Avila, J. P. Miller, and S. S. Iyengar, "Current Challenges in IoT Security and Forensics: Strategies for a Secure Connected Future," Nov. 2024, doi: 10.5772/intechopen.1007766.
- [15] S. S. Gill et al., "Edge AI: A Taxonomy, Systematic Review and Future Directions," July 2024, doi: 10.48550/arxiv.2407.04053.
- [16] F. Alwahedi et al., "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167-185, 2024, doi: 10.1016/j.iotcps.2023.12.003.
- [17] M. Kevin et al., "VEDLIoT -- Next generation accelerated AIoT systems and applications," May 2023, doi: 10.48550/arxiv.2305.05388.
- [18] K. K. Vaigandla, "AI and Edge Analytics for Real-Time IoT Decision-Making in SMAC Environments: A Comprehensive Review," *Journal of Sensors, IoT and Health Sciences*, Dec. 2025, doi: 10.69996/jsihs.2025016.

- [19] A. Z. Miran et al., "The Investigation and Challenges of Advanced Applications Using Artificial IoT on Edge Computing," *QALAAI ZANISTSCIENTIFIC JOURNAL*, vol. 8, no. 2, Apr. 2023, doi: 10.25212/lfu.qzj.8.2.55.
- [20] S. Rani et al., "Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey," *Wireless Communications and Mobile Computing*, vol. 2021, p. 5579148, Apr. 2021, doi: 10.1155/2021/5579148.
- [21] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," *Sensors*, vol. 23, no. 8, Art. no. 4117, Apr. 2023, doi: 10.3390/s23084117..
- [22] M. K. Pasupuleti, "AI in Edge Computing for IoT Optimization," *International Journal of Academic and Industrial Research Innovations*, Nov. 2024, doi: 10.62311/nesx/rb978-81-981466-8-7.
- [23] M. Kaiser et al., "VEDLIoT: Very Efficient Deep Learning in IoT," *Conference: Automation & Test in Europe Conference & Exhibition (DATE)*, July 01, 2022. doi: 10.23919/DATE54114.2022.9774653.
- [24] J. Xiong and H. Chen, "Challenges for building a cloud native scalable and trustable multi-tenant AIoT platform," Nov. 2020, doi: 10.1145/3400302.3415756.
- [25] L. Gupta and G. Yao, "Enhancing Critical Infrastructure Cybersecurity: Collaborative DNN Synthesis in the Cloud Continuum," May 2024, doi: 10.48550/arxiv.2405.14074.
- [26] I. U. Khan*, F. M. Khan, Z. A. Haider, and F. Alturise, "Integrating AI, Blockchain, and Edge Computing for Zero-Trust IoT Security: A Comprehensive Review of Advanced Cybersecurity Framework," *Cmc-computers Materials & Continua*, vol. 85, no. 3, pp. 4307-4344, Jan. 2025, doi: 10.32604/cmc.2025.070189.
- [27] I. Zhou et al., "Internet of Things 2.0: Concepts, Applications, and Future Directions," *IEEE Access*, vol. 9, pp. 70961-71012, May 2021, doi: 10.1109/ACCESS.2021.3078549.
- [28] J. Li et al., "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," *IEEE Access*, vol. 8, pp. 135479-135490, July 2020, doi: 10.1109/ACCESS.2020.3011503.
- [29] M. A. M. Albreem, A. M. Sheikh, M. H. Alsharif, M. Jusoh, and M. N. M. Yasin, "Green Internet of Things (GIoT): Applications, Practices, Awareness, and Challenges," *IEEE Access*, vol. 9, pp. 38833-38858, Feb. 2021, doi: 10.1109/ACCESS.2021.3061697.
- [30] H. Eren, Ö. Karaduman, and M. T. Gençoğlu, "Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions," *Applied Sciences*, vol. 15, no. 15, pp. 8704-8704, Aug. 2025, doi: 10.3390/app15158704.
- [31] D. Muhammed, E. Ahvar, S. Ahvar, M. Trocan, M. Montpetit, and R. Ehsani, "Artificial Intelligence of Things (AIoT) for smart agriculture: A review of architectures, technologies and solutions," *Journal of Network and Computer Applications*, vol. 228, pp. 103905-103905, Aug. 2024, doi: 10.1016/j.jnca.2024.103905.
- [32] E. Toé, F. Jaafar, and L. Ferrier, "Securing LoRaWAN in the AIoT Era: A Systematic Mapping Study and an MITRE-Based Threat

Matrix," *IEEE Internet of Things Journal*, vol. 13, no. 3, pp. 3827-3849, Nov. 2025, doi: 10.1109/jiot.2025.3633940.

[33] J. Zhang and D. Tao, "Empowering Things With Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7789-7817, 15 May 2021, doi: 10.1109/JIOT.2020.3039359.

[34] S. Chinta, "Edge AI for Real-Time Decision Making in IOT Networks," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, no. 09, pp. 11293-11309, Sept. 2024, doi: 10.15680/ijirccce.2024.1209044.

[35] V. E. Quincozes, S. E. Quincozes, J. F. Kazienko, S. Gama, O. Cheikhrouhou, and A. Koubaa, "A survey on IoT application layer protocols, security challenges, and the role of explainable AI in IoT (XAIoT)," *International Journal of Information Security*, Mar. 2024, doi: 10.1007/s10207-024-00828-w.

[36] A. Ouadah and L. Zemmouchi-Ghomari, "Artificial Intelligence of Things: A review of its potential for sustainability," Oct. 2025, doi: 10.1386/tmsd_00110_1.

[37] H. K. Adli et al., "AIoT: bridging the gap between artificial intelligence and the internet of things", *JOURNAL OF ARTIFICIAL INTELLIGENCE AND ROBOTICS*, vol.1, issue1, 2023, doi: 10.61577/jaiar.2023.100001.

[38] D. Rahmayanti, "Artificial Intelligence of Things (AIoT) To Improve Efficiency and Automation in Industrial 4.0," *Sci-tech Journal*, vol. 3, no. 3, pp. 255-270, Dec. 2024, doi: 10.56709/stj.v3i3.656.

[39] S. F. Ahmed, S. Shuravi, S. Afrin, S. J. Rafa, M. Hoque, and A. H. Gandomi, "The Power of Internet of Things (IoT): Connecting the Dots with Cloud, Edge, and Fog Computing," *arXiv.org*, vol. abs/2309.03420, Sept. 2023, doi: 10.48550/arxiv.2309.03420.

[40] H. Gill and K. Kaur, "Hybrid Edge-Cloud Models for IoT: A Systematic Review," *International Journal For Multidisciplinary Research*, Dec. 2025, doi: 10.36948/ijfmr.2025.v07i06.63015.

[41] K. Zheng, R. Xu, J. Mei, H. Yang, L. Lei, and X. Wang, "Ambient IoT towards 6G: Standardization, Potentials, and Challenges," Dec. 2024, doi: 10.48550/arxiv.2412.12519.

[42] D. Bogićević, "Improving internet of things parking systems," vol. 19, no. 3, pp. 163-174, Jan. 2021, doi: 10.22190/FUACR2003163B.

[43] Md. Milon Islam et al., "Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3611-3641, Feb. 2023, doi: 10.1109/jiot.2022.3228795.

[44] R. H. Sevinç, B. Türkoğlu, and İ. Kök, "Agentic IoT: Architectures, Applications, and Challenges Toward the Internet of Agents," July 05, 2026. [Online]. Available: <https://arxiv.org/abs/2607.04219v1>

[45] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey," *Security and Communication Networks*, vol. 2020, pp. 1-13, Sept. 2020, doi: 10.1155/2020/8872586.

- [46] A. Srhir, T. Mazri, and M. Benbrahim, "Security in the IoT: State-of-the-Art, Issues, Solutions, and Challenges," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, Jan. 2023, doi: 10.14569/ijacsa.2023.0140507.
- [47] P. Deshpande, A. Damkonde, and V. Chavan, "The Internet of Things: Vision, Architecture and Applications," *International Journal of Computer Applications*, vol. 178, no. 2, pp. 1-14, Nov. 2017, doi: 10.5120/IJCA2017915722.
- [48] C. Anagnostopoulos et al., "Multimodal Federated Learning in AIoT Systems: Existing Solutions, Applications, and Challenges," *IEEE Access*, vol. 12, pp. 180864-180902, Jan. 2024, doi: 10.1109/access.2024.3508030.
- [49] M. B. Kusharki, M. M. Liman, B. L. Muhammad-Bello, and M. Timothy, "Artificial Intelligence of Things Technologies for Predictive Crop Disease Models in Precision Agriculture: A Systematic Review," Sept. 2025, doi: 10.47852/bonviewaia52024321.
- [50] X. Luo et al., "Toward Intelligent AIoT: A Comprehensive Survey on Digital Twin and Multimodal Generative AI Integration," *Mathematics*, vol. 13, no. 21, pp. 3382-3382, Oct. 2025, doi: 10.3390/math13213382.
- [51] J. P. Gupta, Ms. Shikha, and P. Gupta, "Demystifying the Internet of Things: A Deep Dive into Protocols, Architectures, Technologies, and Beyond," pp. 155-168, Mar. 2024, doi: 10.58532/nbennurch76.
- [52] M. Wazid, A. K. Das, and Y.-H. Park, "Blockchain-Envisioned Secure Authentication Approach in AIoT: Applications, Challenges, and Future Research," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-19, Oct. 2021, doi: 10.1155/2021/3866006.
- [53] J. Wei, "Convergence of IoT and PLC in Industrial Automation: A Systematic Review of Emerging Trends, Technical Challenges, and Prospects," *Applied and Computational Engineering*, vol. 145, no. 1, pp. 221-226, Apr. 2025, doi: 10.54254/2755-2721/2025.22249.