International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct-2026, PP 01-6

Artificial Intelligence Of Things (Aiot): A Review Of Architectures, Learning Techniques And Applications Of Iot With AI

Buchake Rameshwari Hanumant[1] Prof. M. A. Auti[2] Prof. M. C. Kolse[3] Prof. S. K. Said[3]
Department of Artificial Intelligence and Data Science
Jaihind College of Engineering
Pune, Maharashtra, India

Abstract—The Internet of Things (IoT) connects sensors, cameras, smartphones and machines to the internet so that they can collect and exchange data, while Artificial Intelligence (AI) analyses that data to recognize patterns and make decisions. Their combination, often called the Artificial Intelligence of Things (AIoT), enables systems that monitor, control and manage activities with minimal human involvement. This paper reviews AIoT from the perspectives of architecture, intelligence and application. It explains layered IoT architectures, communication protocols and context-aware computing, then surveys machine learning and deep learning for IoT data analytics, including streaming analytics, anomaly detection and edge-based inference, as well as federated learning for privacy. Applications in smart homes, smart cities, healthcare, agriculture and industrial IoT are reviewed. Security threats such as large IoT botnets are discussed as a key concern. A five-layer AIoT architecture comprising perception, connectivity, edge intelligence, cloud analytics and application layers is proposed, along with research gaps, objectives, a comparison of learning approaches and an analysis of challenges in interoperability, energy, privacy and security. The review concludes that AIoT can greatly improve automation, accuracy and productivity when built with security and privacy in mind.

Index Terms—Internet of Things, artificial intelligence, AIoT, machine learning, edge computing, smart cities, industrial IoT, IoT security

I. Introduction

1.1 Motivation

The IoT turns ordinary objects into data sources. Atzori *et al.* [1] described the IoT as a paradigm in which things interact and cooperate through unique addressing, and Gubbi *et al.* [2] envisioned ubiquitous sensing that feeds cloud-based analytics. By itself, however, IoT mostly collects data; value arises when that data is interpreted and acted upon.

AI provides this interpretation. Machine learning recognizes patterns in sensor streams, predicts future states and triggers actions automatically. Together, IoT and AI enable smart homes that adjust energy use, cities that manage traffic, hospitals that monitor patients remotely and factories that predict machine failures.

This paper reviews the combination of IoT and AI, proposes a layered architecture and discusses challenges and future directions.

1.2 Objectives of the Review

- 1. To review IoT architectures, protocols and the role of AI.
- 2. To examine machine learning and deep learning methods for IoT data.
- 3. To propose a five-layer AIoT architecture.

- 4. To compare learning approaches for IoT.
- 5. To discuss applications, challenges and future directions.

II. Overview of Key Concepts

2.1 IoT Architecture and Protocols

IoT systems are commonly described in layers: perception (sensors and actuators), network (communication), and application (services). Lin *et al.* [3] surveyed these layers and their enabling technologies. Protocols such as MQTT [4] and low-power wide-area networks [5] connect constrained devices.

2.2 Types of Intelligence

Fig. 1 summarizes the intelligence functions AI adds to IoT: sensing and recognition, prediction, anomaly detection, optimization and autonomous control.

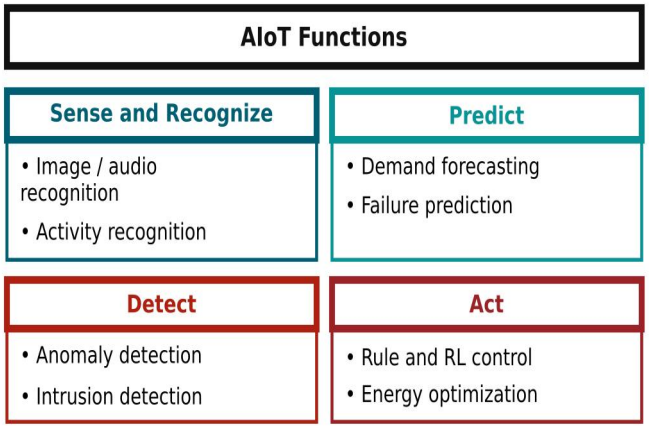


Fig. 1. Intelligence functions added by AI to IoT systems.

III. Review of Existing Work

Al-Fuqaha *et al.* [6] surveyed IoT enabling technologies and protocols and noted that analytics and intelligence were key open areas. Perera *et al.* [7] reviewed context-aware computing for IoT, explaining how sensor data can be turned into context that drives adaptive behaviour.

Mahdavinejad *et al.* [8] reviewed machine learning algorithms for IoT data analysis and matched them to data characteristics such as volume, velocity and noise. Mohammadi *et al.* [9] surveyed deep learning for IoT big data and streaming analytics, discussing models suited to time series, images and sequences, and the need to run them on resource-constrained devices.

In application domains, Zanella *et al.* [10] described an urban IoT deployment for smart city services, Islam *et al.* [11] surveyed IoT for healthcare, and Sisinni *et al.* [12] analysed the industrial IoT and its reliability and real-time requirements.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct-2026, PP 01-6

Security is a critical concern: Kolias *et al.* [13] analysed the Mirai botnet, which hijacked large numbers of poorly secured IoT devices to launch massive denial-of-service attacks. McMahan *et al.* [14] introduced federated learning, which allows devices to learn collaboratively without sharing raw data. Table I summarizes these works.

Sr. No.	Ref.	Year	Methodology	Findings	Research Gap
1	[7]	2014	Context-aware computing for IoT	Context lifecycle model	Pre-deep-learning
2	[10]	2014	Urban IoT for smart cities	Real deployment architecture	Limited intelligence
3	[6]	2015	Survey of IoT technologies and protocols	Comprehensive protocol overview	Limited AI coverage
4	[11]	2015	IoT for healthcare survey	Architectures and applications	Security challenges open
5	[13]	2017	Mirai botnet analysis	Exposed IoT security weaknesses	Attack analysis only
6	[8]	2018	ML for IoT data analysis	Matched algorithms to data traits	Survey only
7	[9]	2018	Deep learning for IoT streaming	Models for big and streaming data	Resource limits noted
8	[12]	2018	Industrial IoT analysis	Requirements and directions	Conceptual

TABLE I Summary of Literature Survey

IV. Identified Research Gaps

G1: Devices from different vendors use incompatible protocols and data formats.

G2: Many IoT devices lack the computing and energy resources to run AI models.

G3: Security practices such as strong passwords and updates are often missing on consumer devices.

G4: Continuous collection of personal data raises privacy concerns.

G5: Few deployments measure the long-term reliability and benefit of AIoT systems.

V. System Architecture

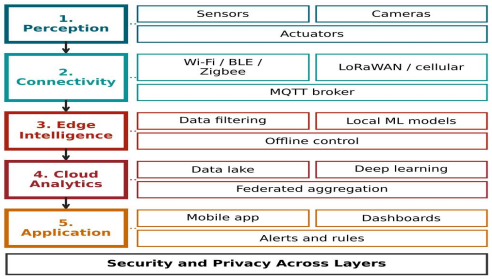


Fig. 2 shows the proposed architecture.

Fig. 2. Proposed five-layer AIoT architecture.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct-2026, PP 01-6

5.1 Perception Layer

Sensors measure temperature, motion, light, air quality, power consumption and other quantities; actuators control lights, motors and valves.

5.2 Connectivity Layer

Wi-Fi, Bluetooth Low Energy, Zigbee, LoRaWAN and cellular links carry data; MQTT brokers distribute messages.

5.3 Edge Intelligence Layer

Gateways filter data, run lightweight models for anomaly detection and local control, and continue operating when the internet is unavailable.

5.4 Cloud Analytics Layer

Large datasets are stored and analysed, deep models are trained, and federated learning aggregates updates from many sites.

5.5 Application Layer

Mobile apps and dashboards display insights, send alerts and allow users to set rules or goals.

VI. Implementation Methodology

Fig. 3 describes the AIoT operating loop. A simple anomaly score for a sensor reading x_t compares it with a rolling mean μ and standard deviation σ:

$$z_t = |x_t - \mu| / \sigma \quad (1)$$

and readings with z_t above a threshold are flagged. More complex patterns are learned by models such as LSTM autoencoders, which flag sequences with high reconstruction error.

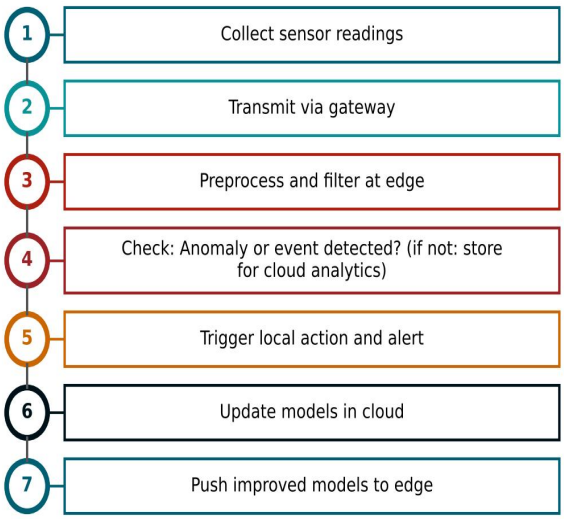


Fig. 3. Operating loop of an AIoT system.

International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 5
Sep-Oct-2026, PP 01-6

VII. Performance Comparison

Table II compares learning approaches. Classical machine learning is lightweight, deep learning handles images and complex sequences, and federated learning protects privacy across many devices.

Approach	Compute Need	Data Type	Privacy
Classical ML (RF, SVM)	Low	Tabular sensor data	Medium
Deep learning (CNN, LSTM)	High	Images, sequences	Medium
TinyML	Very low	Simple signals	High
Federated learning	Medium	Distributed data	High
Reinforcement learning	Medium–High	Control decisions	Medium

TABLE II Comparison of Learning Approaches for IoT

VIII. Open Issues and Future Directions

Table III summarizes challenges. Future AIoT systems will use tiny ML on microcontrollers, digital twins of buildings and cities, 5G connectivity and standards for interoperability and security labelling of consumer devices.

Challenge	Mitigation
Interoperability	Open standards; common data models
Energy limits	Low-power radios; duty cycling; TinyML
Security	Unique credentials; updates; network segmentation
Privacy	Edge processing; federated learning
Scalability	Edge filtering; cloud elasticity

TABLE III Challenges and Mitigation

IX. Conclusion

IoT gives machines the ability to sense, and AI gives them the ability to understand and act. The reviewed literature shows mature architectures and protocols for connectivity, a broad range of learning methods for IoT data, and successful applications across homes, cities, healthcare and industry. Interoperability, energy constraints, privacy and especially security must be addressed for AIoT to deliver its full benefits safely.

9.1 Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

References

1. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

2. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.
3. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, 2017.
4. OASIS, MQTT Version 5.0, OASIS Standard, Mar. 2019.
5. U. Raza, P. Kulkarni, and M. Sooriyabandara, “Low power wide area networks: An overview,” IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 855–873, 2017.
6. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015.
7. C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, “Context aware computing for the Internet of Things: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 414–454, 2014.
8. M. S. Mahdavinejad et al., “Machine learning for Internet of Things data analysis: A survey,” Digit. Commun. Netw., vol. 4, no. 3, pp. 161–175, 2018.
9. M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deep learning for IoT big data and streaming analytics: A survey,” IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 2923–2960, 2018.
10. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.
11. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, “The Internet of Things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.
12. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, opportunities, and directions,” IEEE Trans. Ind. Informat., vol. 14, no. 11, pp. 4724–4734, 2018.
13. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, vol. 50, no. 7, pp. 80–84, 2017.
14. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proc. AISTATS, 2017, pp. 1273–1282.