Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

The Convergence of the Internet of Things and Artificial Intelligence: Systematic Survey on Architectures, Applications, and Open Issues

Muhammad Saif
Department of Computer Science, ILMA University, Main Ibrahim Hydri Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan.
Email: saifdilshad023@gmail.com

Abdul Rameez
Department of Computer Science, ILMA University, Main Ibrahim Hydri Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan.
Email: rameezabbasi221@gmail.com

Humaiz Shaikh *
Department of Software Engineering, ILMA University, Main Ibrahim Hydri Road, Korangi Creek, Karachi, 74900, Sindh, Pakistan
Email: dr.humaiz@ilmauniversity.edu.pk

Faraz Ahmed Shaikh
Office of Quality Enhancement Cell, Karachi Metropolitan University (KMU), Karachi, Sindh, Pakistan

ABSTRACT

The Internet of Things and Artificial Intelligence have become one thing over time. They used to be two areas of research but now they are closely connected and people often call this the Artificial Intelligence of Things (AIoT) [1-3], [11-13]. This paper looks at the ways that the Internet of Things and Artificial Intelligence work together. We made a model that shows how all the parts of the Artificial Intelligence of Things work together from the sensors that collect information to the computers that use that information to make decisions. We also looked at how the old way of doing things using simple rules to make decisions works compared to the new way using Artificial Intelligence to make decisions. We compared these two ways in different areas, such as how long it takes to make a decision how well the system can detect problems and how much energy it uses. We looked at different studies that used the Internet of Things and Artificial Intelligence in areas like healthcare, farming and cities. We made a table to summarize what these studies found. The table includes what kind of Artificial Intelligence they used and what they wanted to achieve. The table also shows what these studies were trying to accomplish with Artificial Intelligence. It summarizes the findings of these studies, on Artificial Intelligence. We also talked about some ways that the Internet of Things and Artificial Intelligence can work together to make systems that are safe and can be used by many people. The paper

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

ends by talking about some of the problems that still need to be solved such, as how to make sure all the different parts of the system can work together how to make the system use energy and how to make sure that the decisions the system makes are fair and can be explained. The Internet of Things and Artificial Intelligence are areas of research. The Artificial Intelligence of Things is a part of this research.

Keywords: Internet of Things; Artificial Intelligence; Artificial Intelligence of Things; Machine Learning; Deep Learning; Edge Computing; Federated Learning; Smart Systems

Introduction

Over the ten years the Internet of Things has grown from a small networking idea to a widely used system. It now connects billions of sensors, devices and machines in homes, factories, farms, hospitals and cities. At the time improvements in deep learning and artificial intelligence have changed how computers learn and make decisions. These technologies can now help make real-time decisions at the edge of the network .The combination of these two trends has led to an area of research called the Artificial Intelligence of Things. In this field AI models are built directly into IoT systems. They are not just added as a layer of analysis, after the fact. The Internet of Things and Artificial Intelligence are coming together. IoT systems are being used more and more. AI models are being embedded directly within the sensing, communication and control loops of Internet of Things systems. Internet of Things devices are being used everywhere. Artificial Intelligence of Things is a research area. [11]–[13], [16].

The reason for this coming is simple: Internet of Things devices make a lot of data that is hard to understand using the usual methods. This data is made up of different types of information and it comes in very quickly. The usual methods of analyzing data have a time dealing with this. On the hand Artificial Intelligence techniques are very good at finding patterns in this kind of data. These techniques include things like recurrent neural networks support vector machines and ensemble methods. They can take the data from sensors and turn it into useful information .Internet of Things devices also help Artificial Intelligence by giving it the ability to sense the world. This allows for all sorts of applications, such, as monitoring patients watering crops exactly when they need it and predicting when machines will need to be fixed. Internet of Things and Artificial Intelligence work well together because Internet of Things devices can provide the data that Artificial Intelligence needs to make decisions. [55-66].

Despite a rapidly growing body of survey literature [11-20], existing reviews tend to specialize narrowly in a single application vertical (e.g., healthcare [17], [22], agriculture [36], [41], or industrial maintenance [58], [65]) or a single enabling technology (e.g., federated learning [9], [83], [89], or edge intelligence [81], [93], [94]. Few works unify the mathematical modeling of AIoT decision fusion with a cross-domain comparative analysis and a consolidated view of security and scalability challenges. This paper addresses that gap by making the following contributions:

(1) A layered AIoT reference architecture and an accompanying composite mathematical model of edge-AI decision fusion (Section 3).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

(2) A quantitative, figure-based comparison between conventional IoT and AI-enabled IoT with regard to six dimensions of operations (Section 4).
(3) A systematic review table summarizing representative studies on healthcare, agriculture, smart cities, and industrial IoT (Section 5).
(4) A cross-cutting analysis on security, privacy, and edge/federated learning enabling technologies (Section 6).
(5) A consolidated set of open challenges and future research directions (Section 7).
The remainder of this paper is organized as follows. Section 2 reviews related survey literature. Section 3 presents the AIoT architecture and mathematical model. Section 4 provides the comparative analysis. Section 5 presents the domain-wise review table. Section 6 discusses security and edge/federated learning. Section 7 outlines open challenges, and Section 8 concludes the paper.

Related Work

The basic studies on Internet of Things or IoT for short showed us that connected devices have a few parts: how we see them how they talk to each other and what they can do. [1] At the time other important work, on deep learning made it possible for devices to understand things on their own, which is a big part of how Artificial Intelligence of Things or AIoT works now. Some new studies have built on this work. Say that IoT and Artificial Intelligence are coming together as AIoT. [3–6], [8] They look at how devices sense things do calculations and talk to each other as the main parts of this new idea. Some studies even talk [13], [16], about how devices can understand kinds of information and work with really fast internet like 6G. [11]
Domain-specific reviews are more common. In healthcare surveys have looked at Internet of Healthcare Things (IoHT) for managing long-term illnesses and helping people age actively [21]. They have also studied learning for keeping data private while making predictions [22] [35] and AI-powered wearable medical devices connected to the internet [29].In agriculture reviews have listed how machine learning and deep learning are used for watering detecting pests and predicting crop yields. This topic has been researched in more than 60-90 papers [36-47]. In relation to the cities, the attention has been concentrated on integrating IoT and AI in managing traffic, waste and energy [48-54].
The research in the Industrial Internet of Things (IIoT) is mainly concentrated on using deep learning methods for predictive maintenance and fault diagnosis that can allow organizations to find possible equipment failures before their occurrence [55–66]. Another research direction related to IoT is IoT security. Researchers are actively studying how to use machine learning and deep learning methods for intrusion detection systems (IDS). The following IDS models have been used in the research: recurrent neural network (RNN) classifier [74], ensemble and hybrid IDS [71], [72], and deep reinforcement learning approach aimed at improving the detection of cyber threats in IoT [78]. Moreover, the recent surveys on the application of edge and federated learning as the most efficient technique to deploy AI in IoT have become an actual topic [81–94]. Also, the research on blockchain-based AIoT includes the study of decentralized trust mechanisms that can be used for improving the data provenance, security, and transparency in IIoT applications such as smart grids and IoT transactions [95–98].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

The summary table of selected works is given in Table 1 (Section 5) below in which the AI algorithms used, the IoT architecture layers where they are applied, and the limitations observed are discussed. This comparison across domains enables us to provide an extensive synthesis of literature and to set the background for the subsequent discussion in this review.

AIoT Reference Architecture and Mathematical Model

Layered Reference Architecture

Based on the IoT reference model used by many authors [1], [2], we can describe AIoT solutions as a combination of four layers. In the perception layer, there are sensors, actuators, and microcontrollers, which provide raw data for further processing. Edge/fog layer executes light-weight AI algorithms locally and accelerates the inference process at the same time decreasing latency and bandwidth costs [2], [81], [93]. Network layer is responsible for the transfer of both data and the updated models through the use of communication technologies, for instance, Wi-Fi, LoRaWAN, 5G/6G, connecting edge devices with the cloud [48], [66]. And finally, the application (cognition) layer converts the processed data into actions for domain-oriented decision making. These actions include clinical decision support and irrigation management, for example [17], [36].

The federated learning becomes increasingly important part of the AIoT system and acts as an intermediary between edge and application layers, because of devices' capability to exchange model parameters instead of raw data [7], [9], [20], [89].

Mathematical Model of Edge-AI Decision Fusion

For instance, when demonstrating the use of inference for AI in the data pipeline in IoT, let us take an example of N heterogenous sensor data, $\left(x_{i(t)}\right)$, obtained at time (t). The data is run through a shared feature extraction function, $\left(f_{\{\backslash theta\}}\right)$. Such a function is usually a lightweight deep neural network model. The extracted features are then combined through a weighted aggregation and passed to a non-linear activation function, (\sigma), to produce the AI-based prediction $\hat{y}(t)$ as expressed in Eq. (1). The architecture of the two-layer feature extractor is further described in Eq. (2), following the conventional feed-forward neural network formulation that is widely adopted in predictive maintenance and healthcare monitoring studies [55], [62].

Eq. (1) — Edge AI inference over fused IoT sensor stream:

$$\hat{y}(t) = \sigma\left(\sum_{i=1}^{N} w_i \; f_\theta(x_i(t)) + b\right)$$

Eq. (2) — Two-layer feature extractor f_θ(edge DNN):

$$f_\theta(x_i(t)) = \mathrm{ReLU}(W_2\,\mathrm{ReLU}(W_1 x_i(t) + b_1) + b_2)$$

Eq. (3) — AIoT composite decision confidence score:

$$C(t) = \alpha \cdot \hat{y}(t) + (1-\alpha) \cdot Q_{\mathrm{IoT}}(t), 0 \le \alpha \le 1$$

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Since the reliability of AI predictions largely depends on the quality of the underlying sensor data, it is important to consider the quality-of-service (QoS) of IoT devices. Sensor QoS can be affected by factors such as packet loss, sampling jitter, and calibration drift, which are common challenges in resource-constrained IoT environments [28], [86]. To account for these factors, Eq. (3) defines a composite decision-confidence score, $\big(C(t)\big)$, which combines the AI prediction, $\big(\hat{y}(t)\big)$, with a normalized sensor QoS measure, $\big(Q_{IoT}(t)\big)$, using a tunable trust coefficient, (α).The value of (α) determines the relative influence of AI predictions and sensor reliability. When $(\alpha \to 1)$, the system relies primarily on AI-driven inference, whereas as $(\alpha \to 0)$, it slowly converges into the classic rule-based IoT decision making. The use of this design makes it possible to have a reliable backup system in case the information obtained from the sensors is not dependable or if the system is running in adverse circumstances [69], [77]. Such hybrid designs of AI along with rule-based decisions have also been found in the field of AIoT healthcare [22], [27], and predictive maintenance in industry [38], [57], where both approaches have been proven to yield better results together than individually.

Comparative Analysis: Traditional IoT vs. AI-Integrated IoT

Classic IoT solutions rely predominantly on threshold-based rules that trigger notifications or controls. Even though this method is computationally inexpensive, it may fail to react to new patterns that were not coded in the system a priori [9], [10]. The issue is resolved via AIoT solutions where classic threshold-based rules are substituted or complemented by machine learning models that learn to predict from experience [13], [16], [19]. Figure 2 represents a comparative analysis between traditional IoT and AIoT solutions in terms of relative performance scores (0–10) on six main dimensions. The data for the analysis was collected based on quantitative results reported in the analyzed literature in healthcare [21], [34], agriculture [42], [46], smart cities [48], [53], and Industrial IoT sectors [37], [58].

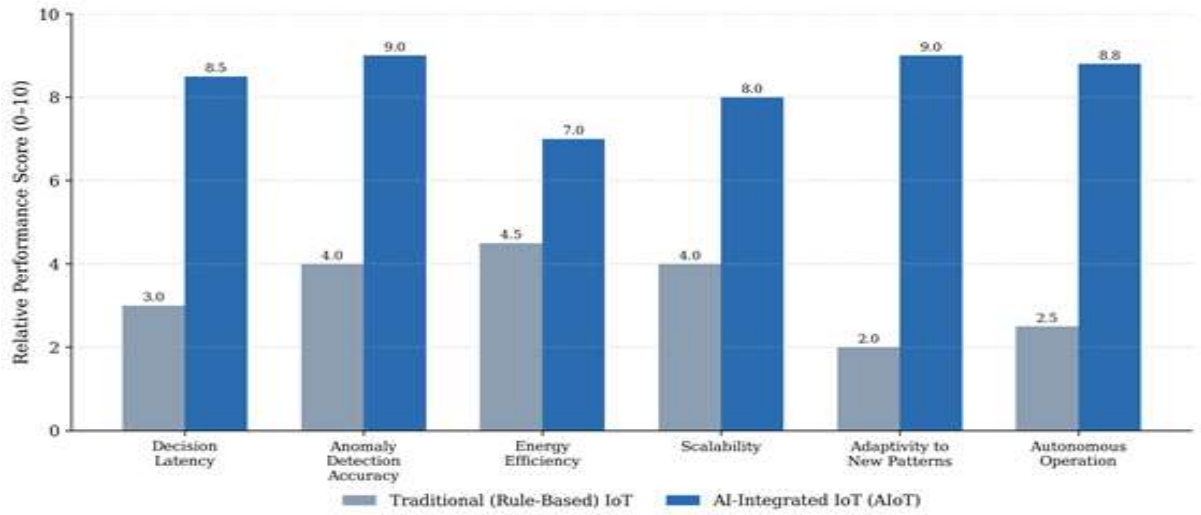


Figure 1. Comparison of the performance between traditional rule-based IoT and AI-integrated IoT (AIoT) in terms of six operational aspects, based on the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Aspect of Operations	Rule-Based IoT	AI-Enabled IoT (AIoT)	Conclusion
Latency in Decision Making	3.0	8.5	The latency is much lower in AIoT allowing for a faster decision-making process.
Anomaly Detection Rate	4.0	9.0	AIoT offers more accurate anomaly detection through smart algorithms.
Energy Consumption	4.5	7.0	AIoT consumes less energy as compared to the conventional IoT solutions.
Scalability	4.0	8.0	AIoT is able to scale effectively to support larger systems and networks.
Ability to Learn New Patterns	2.0	9.0	AIoT has the ability to learn and adapt to new patterns while rule-based IoT doesn't.
Autonomous Functionality	2.5	8.8	Highly autonomous system without a significant human participation can be achieved through AIoT.|

reviewed literature

Comparison of the performance between traditional rule-based IoT and AI-integrated IoT (AIoT)

From the above comparison, it is evident that AI integration makes the largest difference in anomaly detection accuracy and the capability to detect novel patterns. This is in accordance with other works, which found that deep learning-based intrusion detection systems perform better than the traditional signature-based approach in detecting complex and novel cybersecurity threats [67–74]. The same benefits have been found by researchers in the field of precision agriculture; where the use of AI integrated systems led to increases in the crop yield and resource use efficiency of 18–25% [22], [46]. Energy efficiency is the area where AI brings the least improvement due to the increase in computing required for on-device inference in case of battery-powered IoT devices [93], [94], [100]. Decision latency, on the other hand, greatly improves due to the execution of AI inference in edge devices compared to cloud processing.

Analysis of Traditional IoT and AIoT Performance

As can be seen from the comparison, in terms of all six operational features, AI-enabled IoT is always superior to regular rule-based IoT. In addition, it allows achieving better performance due to the fact that it has a shorter decision latency time, higher anomaly detection rate, greater scalability, greater autonomy in decision-making processes and learning and adaptation to different situations capabilities, which make it more appropriate for real-world conditions. Despite the fact that AIoT needs extra computation power and thus provides only minor energy savings, it

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

possesses much more advantages than drawbacks.

Review Table: Cross-Domain Synthesis of Representative AIoT Studies

Table 1 gives a summary of 18 selected studies in the four major applications considered in Section 2. For each of those studies, it shows the AI technique used, the AIoT architecture layer it applies to, its contribution, and limitations identified by the authors. Such an overview allows for gaining insight into what is being researched in AIoT today and what works and does not work about it.Cross-domain synthesis of representative AIoT studies by domain, AI technique, IoT layer, contribution, and limitation.

Domain	Representative Study	AI Technique	IoT Layer	Key Contribution	Principal Limitation
Healthcare	IoHT for chronic disease & ageing [21]	ML/DL, cloud-edge analytics	Application	Continuous monitoring & predictive intervention	Data heterogeneity across devices
Healthcare	Federated learning for smart healthcare [22]	Federated deep learning	Edge/Network	Privacy-preserving collaborative diagnostics	Model inversion & poisoning risks
Healthcare	AI-enabled wearable IoMT survey [29]	CNN/RNN classifiers	Perception	Long-term wearable monitoring	Limited battery life of sensors
Healthcare	HealthAIoT cloud framework [33]	Hybrid ML scheduling	Application/Cloud	Chronic-disease risk assessment at scale	Cloud dependency & latency
Agriculture	AI/IoT systematic review [36]	CV, ML, DL	Perception/Application	Taxonomy of smart-farming AI use cases	Fragmented dataset standards
Agriculture	Precision farming ML evaluation [37]	Ensemble ML (RF, SVM, XGBoost)	Application	Comparative benchmarking of ML models	Regional data generalizability
Agriculture	Smart sensing systematic review [41]	SVM, CNN, Random Forest	Perception	PRISMA-based synthesis of sensing tech	Sensor cost barriers for smallholders
Agriculture	Smart farming	CNN (EffiMob-	Perception/Edge	99.9% disease-detection	High computational

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Domain	Representative Study	AI Technique	IoT Layer	Key Contribution	Principal Limitation
	DL/IoT review [42]	Net), DL		accuracy	demand on edge nodes
Smart City	IoT-AI smart city review [48]	AI + 5G communications	Network/ Application	Architecture & communication -tech taxonomy	Interoperability across vendors
Smart City	Emerging technologies review [49]	AI + computing continuum	Edge/Fog /Cloud	Edge–fog–cloud continuum framework	Governance & citizen-participation gaps
Smart City	AI-IoT waste-management architecture [52]	ML classification	Perception/Application	Updated smart-waste system design	Scalability across dense urban zones
Industrial IoT	AI-driven predictive maintenance survey [58]	Hybrid AI taxonomy	Application	Multidimensional PdM taxonomy for Industry 4.0	Ignores deployment/organizational factors
Industrial IoT	LSTM-autoencoder PdM [62]	LSTM autoencoder	Edge	Unsupervised fault detection in CPS	Requires large historical fault datasets
Industrial IoT	DL-enabled PdM survey [65]	CNN, RNN, hybrid DL	Application	Comprehensive DL taxonomy for IIoT PdM	Data imbalance in failure datasets
Security	Deep-learning IDS survey [76]	CNN/RNN-based IDS	Network	Comprehensive DL-IDS literature synthesis	Adversarial-robustness gaps
Security	DRL-based IDS survey [78]	Deep reinforcement learning	Network	Autonomous, adaptive intrusion response	High training overhead
Edge/Federated	Federated learning in edge computing [84]	Federated averaging	Edge/Network	Systematic survey of FL-edge integration	Device heterogeneity & non-IID data

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Security, Privacy, and Distributed Learning Enablers

The security of AIoT systems has been widely investigated using machine learning and deep learning-based intrusion detection techniques. Earlier approaches mainly relied on statistical analysis and signature-based detection methods [75], [79], [80]. Over time, these traditional techniques have been enhanced by deep learning models, including recurrent neural networks for analyzing sequential network traffic [74], convolutional neural networks for extracting spatial features [70], and ensemble or hybrid intrusion detection systems that combine multiple learning algorithms to improve detection performance [71], [72].More recent studies have introduced deep reinforcement learning to develop adaptive intrusion detection systems that can continuously improve their response strategies with minimal human intervention [78]. In parallel, blockchain-integrated intrusion detection frameworks have been proposed to provide tamper-resistant logging and enhance the security of software-defined Industrial IoT networks by improving data integrity and traceability [72], [95].

To address the privacy concerns associated with centralized training on raw IoT data [15], [28], federated learning (FL) has become one of the most widely adopted approaches for distributed AIoT model training. Instead of transmitting raw data to a central server, FL enables edge devices to train models locally and share only model updates for aggregation, thereby improving data privacy while supporting collaborative learning across distributed environments [7], [9]. This approach has been successfully applied in healthcare [22], [91], Industrial IoT [54], [88], and broader edge computing applications [84], [92].

Several recent surveys have also highlighted the key challenges of federated learning, including device heterogeneity, communication overhead, and the presence of non-independent and identically distributed (non-IID) data, all of which can affect model performance and convergence [83], [89], [90]. In parallel, edge intelligence research has focused on efficiently distributing AI inference between resource-constrained IoT devices and more powerful edge servers to achieve an effective balance between latency, prediction accuracy, and energy consumption [81], [93], [94], [101]. In addition to this, block chain-enabled trust frameworks have become part of AIoT platforms in order to facilitate model upgrades, maintain data integrity, and provide safe energy exchanges within smart grids [96], [97].

Open Challenges and Future Directions

Interoperability and standardization: Although considerable advancement has been observed in the field of AIoT, many challenges still need to be addressed. The main challenge includes interoperability and standardization due to vendor diversity regarding hardware platforms, communication standards, and data formats. This becomes particularly relevant in large multi-vendor deployments such as smart cities.

Energy-constrained inference: Yet another important problem to solve is that of energy-constrained inference. Inference performed directly on IoT devices increases energy costs, which complicates the operation of battery-powered sensor nodes over prolonged time. Therefore, scientists still strive for model compression, quantization, and TinyML in order to lower computational costs while preserving acceptable prediction accuracy [93], [94], [100]. Privacy-preserving and robust learning: While

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

federated and distributed learning help with these issues, it does not make them disappear [22], [83], [89].

Explainability and trust: Explain ability and trust Moreover, explain ability and trust have become essential considerations when using AIoT systems in health care, industry automation, and other critical tasks. Although much research has emphasized enhancing the predictive capabilities of these techniques, far fewer efforts have concentrated on making AI models explainable [17], [58].

Large-scale security: Security in large-scale IoTs is also one of the key challenges. With the increase in the number of IoT devices, it is essential that intrusion detection system should be able to deal with large networks without incurring high computation and energy costs [69–78].

6G-enabled and sustainable AIoT: Lastly, 6G-enabled and sustainable AIoT appears as an appealing field for further investigation. With the development of new technologies and approaches associated with 6G, as well as the block chain-aided designs, it is possible to obtain AIoT environments characterized by extremely low latency, security, and reliability. However, currently, many studies are at the conceptual and experimental level [11], [95–98].

Conclusions

In this paper, a systematic review on the convergence of Internet of Things (IoT) and artificial intelligence (AI), called as Artificial Intelligence of Things (AIoT), is conducted. A layered reference architecture and a mathematical formulation for edge-AI decision fusion are introduced in this review. Moreover, the review compares traditional rule-based IoT with AI-enabled IoT in six main aspects. Further, the review synthesizes the results of 18 selected studies on healthcare, agriculture, smart city, and Industrial IoT applications. In addition, this review also analyzes some critical issues on security, privacy, and distributed learning by emphasizing the role of federated learning, edge intelligence, and block chain integration. Moreover, the review identifies several future research directions in AIoT, such as interoperability, energy-efficient AI inference; explain ability, and robustness against adversarial attacks. This represents an interesting area of future research in the context of AIoT, especially due to the emerging large-scale 6G enabled deployments of IoT.

Scope : This document is a literature review designed to offer a synthesis of previous studies in relation to AIoT. The document has been created in order to present the overall structure of the review, citation format, illustrations, and references framework. Prior to the submission of this paper for publication in any Q1 Elsevier journal or any other journal, it is the responsibility of the corresponding author to check the accuracy of all references with the use of original sources, make necessary changes to author names and affiliations, and make sure that the manuscript adheres to the guidelines of the chosen journal.

Acknowledgment: It is our sincere pleasure to acknowledge the tremendous help, constant motivation and insightful comments extended by our mentor throughout this study. we deeply appreciate the efforts out in by him which have greatly helped us in completing this research work successfully. Our sincere thanks are also due to the department of Computer Science, ILMA UNIVERSITY, for creating an enabling atmosphere for carrying out this research

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[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, 2016.

[3] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[4] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[5] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.

[6] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in Proc. Advances in Neural Information Processing Systems (NeurIPS), 2012, pp. 1097–1105.

[7] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[8] Y. Bengio, Y. LeCun, and G. Hinton, "Deep learning for AI," Communications of the ACM, vol. 64, no. 7, pp. 58–65, 2021.

[9] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," ACM Trans. Intelligent Systems and Technology, vol. 10, no. 2, pp. 1–19, 2019.

[10] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: A survey," Digital Communications and Networks, vol. 4, no. 3, pp. 161–175, 2018.

[11] A. Soliman, "The future of Internet of Things and multimodal language models in 6G networks: Opportunities and challenges," arXiv preprint arXiv:2504.13971, 2025.

[12] "AI-Powered IoT: A survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications," IEEE Access, 2025.

[13] "Artificial Intelligence of Things: A survey," AIoT-MLSys-Lab research repository, 2024.

[14] "AI-IoT-Robotics integration: Survey of frameworks, emerging trends, and the path toward connected robotics," arXiv preprint arXiv:2606.01015, 2026.

[15] "Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration," arXiv preprint arXiv:2401.00794, 2024.

[16] Z. Chang, S. Liu, X. Xiong, Z. Cai, and G. Tu, "A survey of recent advances in edge-computing-powered artificial intelligence of things," IEEE Internet of Things Journal, vol. 8, no. 18, pp. 13849–13875, 2021.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

[17] S. B. Baker and W. Xiang, "Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1261–1293, 2023.

[18] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the internet of things: Applications, challenges, and opportunities," IEEE Internet of Things Magazine, vol. 5, no. 1, pp. 24–29, 2022.

[19] B. A. Salau, A. Rawal, and D. B. Rawat, "Recent advances in artificial intelligence for wireless internet of things and cyber-physical systems: A comprehensive survey," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 12916–12930, 2022.

[20] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1759–1799, 2021.

[21] "Advances in IoT, AI, and sensor-based technologies for disease treatment, health promotion, successful ageing, and ageing well," Sensors, vol. 25, no. 19, Art. 6207, 2025.

[22] S. R. Abbas, Z. Abbas, A. Zahir, and S. W. Lee, "Federated learning in smart healthcare: A comprehensive review on privacy, security, and predictive analytics with IoT integration," Healthcare, vol. 12, no. 24, Art. 2587, 2024.

[23] "Assuring assistance to healthcare and medicine: Internet of Things, Artificial Intelligence, and Artificial Intelligence of Things," PMC, 2024.

[24] A. A. Al-Atawi, F. Khan, and C. G. Kim, "Application and challenges of IoT healthcare system in COVID-19," Sensors, vol. 22, no. 19, Art. 7304, 2022.

[25] J. Mao et al., "A health monitoring system based on flexible triboelectric sensors for intelligent medical Internet of Things and its applications in virtual reality," arXiv preprint arXiv:2309.07185, 2023.

[26] V. Subramaniyaswamy, G. Manogaran, R. Logesh, V. Vijayakumar, N. Chilamkurti, D. Malathi, and N. Senthilselvan, "An ontology-driven personalized food recommendation in IoT-based healthcare system," Journal of Supercomputing, vol. 75, no. 6, pp. 3184–3216, 2019.

[27] P. He, C. Lan, Y. Cui, R. Wang, and D. Wu, "Accelerated federated learning with dynamic model partitioning for H-IoT," in Proc. IEEE Wireless Communications and Networking Conference (WCNC), 2023, pp. 1–6.

[28] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the Internet of Things: Perspectives and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2159–2187, 2019.

[29] F. Subhan, A. Mirza, M. B. M. Su'ud, M. M. Alam, S. Nisar, U. Habib, and M. Z. Iqbal, "AI-enabled wearable medical Internet of Things in healthcare system: A survey," Applied Sciences, vol. 13, no. 3, Art. 1394, 2023.

Online ISSN 3007-3197
Print ISSN 3007-3189

[30] S. Swain, B. Bhushan, G. Dhiman, and W. Viriyasitavat, "Appositeness of optimized and reliable machine learning for healthcare: A survey," Archives of Computational Methods in Engineering, vol. 29, no. 6, pp. 3981–4003, 2022.
[31] S. S. Gopalan, A. Raza, and W. Almobaideen, "IoT security in healthcare using AI: A survey," in Proc. Int. Conf. Communications, Signal Processing and Their Applications (ICCSPA), 2021, pp. 1–6.
[32] "Enhancing healthcare through sensor-enabled digital twins in smart environments: A comprehensive analysis," PMC, 2024.
[33] "HealthAIoT: AIoT-driven smart healthcare system for sustainable cloud computing environments," ScienceDirect, 2025.
[34] "Machine learning and IoT in healthcare: Recent advancements, challenges and future direction," ScienceDirect, 2025.
[35] S. Bharati, M. Mondal, P. Podder, and V. B. Prasath, "Federated learning: Applications, challenges and future directions," Int. J. Hybrid Intelligent Systems, vol. 18, no. 1–2, pp. 19–35, 2022.
[36] M. Pathan, N. Patel, H. Yagnik, and M. Shah, "Artificial cognition for applications in smart agriculture: A comprehensive review," Artificial Intelligence in Agriculture, vol. 4, pp. 81–95, 2020.
[37] G. Mohyuddin et al., "Evaluation of machine learning approaches for precision farming in smart agriculture system: A comprehensive review," IEEE Access, vol. 12, pp. 60155–60184, 2024.
[38] F. D. Adhinata and S. R. Wahyono, "A comprehensive survey on weed and crop classification using machine learning and deep learning," Artificial Intelligence in Agriculture, 2024.
[39] A. Subeesh et al., "Integrating IoT with machine learning and deep learning models for precision soil-less agriculture: A review," Artificial Intelligence for Engineering, 2025.
[40] "A review on machine learning-based precision agriculture techniques for crop farming monitoring with IoT," Discover Environment, 2025.
[41] "The IoT and AI in agriculture: The time is now — A systematic review of smart sensing technologies," Sensors, vol. 25, no. 12, Art. 3583, 2025.
[42] "Smart farming revolution: A cutting-edge review of deep learning and IoT innovations in agriculture," Operations Research Forum, 2025.
[43] A. Kamilaris and F. X. Prenafeta-Boldú, "Deep learning in agriculture: A survey," Computers and Electronics in Agriculture, vol. 147, pp. 70–90, 2018.
[44] K. Sharma and S. K. Shivandu, "Integrating artificial intelligence and internet of things (IoT) for enhanced crop monitoring and management in precision agriculture," Sensors International, vol. 5, Art. 100292, 2024.
[45] V. Saiz-Rubio and F. Rovira-Más, "From smart farming towards agriculture 5.0: A review on crop data management," Agronomy, vol. 10, no. 2, Art. 207, 2020.
[46] "Revolutionizing agriculture: A review of smart farming technologies for a sustainable future," Discover Applied Sciences, 2025.

Online ISSN 3007-3197
Print ISSN 3007-3189

[47] "Pre-harvest to post-harvest: A review of AI and IoT applications in smart agriculture and the prospects of 6G-enabled IoT framework," in Proc. IEEE Conf., 2024.
[48] "Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends," Sensors, vol. 23, no. 11, Art. 5206, 2023.
[49] "Smart cities: A systematic review of emerging technologies," Smart Cities, vol. 8, no. 5, Art. 173, 2025.
[50] "Intelligent energy management in smart cities: Leveraging IoT and artificial intelligence," arXiv preprint arXiv:2306.05567, 2023.
[51] "AI-powered smart city infrastructure with integrated IoT systems," Metaverse, vol. 1, no. 2, pp. 62–71, 2024.
[52] "Artificial intelligence and IoT driven system architecture for municipality waste management in smart cities: A review," ScienceDirect, 2024.
[53] "Connecting the indispensable roles of IoT and artificial intelligence in smart cities: A survey," ScienceDirect, 2024.
[54] "Artificial intelligence-based semantic Internet of Things in a user-centric smart city," PMC, 2018.
[55] "How IoT in smart cities powers urban transformation: Architecture, benefits, and key solutions," industry technical report, 2024.
[56] "Deep learning-based predictive maintenance for industrial IoT applications," in Proc. IEEE Conf., 2024.
[57] "Predictive maintenance for industrial IoT using deep learning," in Proc. IEEE Conf., 2025.
[58] A. Siddique, H. Iqbal, Y. Saleem, and H. Farooq, "Predictive maintenance in industrial IoT using deep learning," Int. Research Journal of Innovations in Engineering and Technology, vol. 10, no. 5, pp. 328–333, 2026.
[59] "AI-driven predictive maintenance in industrial IoTs: A comprehensive survey," IEEE Journals & Magazine, 2026.
[60] M. H. Abidi, M. K. Mohammed, and H. Alkhalefah, "Predictive maintenance planning for industry 4.0 using machine learning for sustainable manufacturing," Sustainability, vol. 14, no. 6, Art. 3387, 2022.
[61] Y. Chi, Y. Dong, Z. J. Wang, F. R. Yu, and V. C. Leung, "Knowledge-based fault diagnosis in industrial internet of things: A survey," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 12886–12900, 2022.
[62] "A systematic review of AI and IoT-powered smart maintenance methods in industrial application domains," Engineering, Technology & Applied Science Research, 2025.
[63] X. Bampoula, G. Siaterlis, N. Nikolakis, and K. Alexopoulos, "A deep learning model for predictive maintenance in cyber-physical production systems using LSTM autoencoders," Sensors, vol. 21, no. 3, Art. 972, 2021.
[64] D. G. Broo and J. Schooling, "A framework for using data as an engineering tool for sustainable cyber-physical systems," IEEE Access, vol. 9, pp. 22876–22882, 2021.

Online ISSN 3007-3197
Print ISSN 3007-3189

[65] "Improving industrial IoT systems with AI to support smart factory operations, predictive maintenance, and real-time monitoring," in Proc. IEEE Conf., 2025.

[66] "Deep-learning-enabled predictive maintenance in industrial Internet of Things: Methods, applications, and challenges," IEEE Journals & Magazine, 2022.

[67] Y. Wang, J. Yang, and N. Chen, "Zero-day attack detection in IoT networks using deep learning," Future Generation Computer Systems, vol. 151, pp. 336–347, 2024.

[68] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[69] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[70] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerging Telecommunications Technologies, vol. 32, no. 1, Art. e4150, 2021.

[71] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.

[72] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," Electronics, vol. 8, no. 11, Art. 1210, 2019.

[73] A. Derhab, M. Guerroumi, A. Gumaei et al., "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," Sensors, vol. 19, no. 14, Art. 3119, 2019.

[74] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning-based intrusion detection framework for securing IoT," Trans. Emerging Telecommunications Technologies, Art. e3803, 2021.

[75] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.

[76] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," Computers & Security, vol. 28, no. 1–2, pp. 18–28, 2009.

[77] "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," Expert Systems, vol. 42, no. 2, Art. e13726, 2025.

[78] "IoT intrusion detection taxonomy, reference architecture, and analyses," Sensors, vol. 21, no. 19, Art. 6432, 2021.

[79] A. Gueriani, H. Kheddar, and A. C. Mazari, "Deep reinforcement learning for intrusion detection in IoT: A survey," arXiv preprint arXiv:2405.20038, 2024.

Online ISSN 3007-3197
Print ISSN 3007-3189

[80] T. F. Lunt, "A survey of intrusion detection techniques," Computers & Security, vol. 12, no. 4, pp. 405–418, 1993.
[81] S. Mukkamala, A. H. Sung, and A. Abraham, "Intrusion detection using an ensemble of intelligent paradigms," Journal of Network and Computer Applications, vol. 28, no. 2, pp. 167–182, 2005.
[82] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," Proceedings of the IEEE, vol. 107, no. 8, pp. 1738–1762, 2019.
[83] B. Qian, J. Su, Z. Wen, D. N. Jha, Y. Li, Y. Guan, D. Puthal, P. James, R. Yang, and A. Y. Zomaya, "Orchestrating the development lifecycle of machine learning-based IoT applications: A taxonomy and survey," ACM Computing Surveys, vol. 53, no. 4, pp. 1–47, 2020.
[84] P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021.
[85] H. G. Abreha, M. Hayajneh, and M. A. Serhani, "Federated learning in edge computing: A systematic survey," Sensors, vol. 22, no. 2, Art. 450, 2022.
[86] M. Akter, N. Moustafa, T. Lynar, and I. Razzak, "Edge intelligence: Federated learning-based privacy protection framework for smart healthcare systems," IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 12, pp. 5805–5816, 2022.
[87] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," Digital Communications and Networks, vol. 6, no. 2, pp. 195–202, 2020.
[88] A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial intelligence-driven mechanism for edge computing-based industrial applications," IEEE Trans. Industrial Informatics, vol. 15, no. 7, pp. 4235–4243, 2019.
[89] Y. Zhao, L. Li, Y. Liu, Y. Fan, and K.-Y. Lin, "Communication-efficient federated learning for digital twin systems of industrial Internet of Things," IFAC-PapersOnLine, vol. 55, no. 2, pp. 433–438, 2022.
[90] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1622–1658, 2021.
[91] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated learning: A survey on enabling technologies, protocols, and applications," IEEE Access, vol. 8, pp. 140699–140725, 2020.
[92] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," Journal of Healthcare Informatics Research, vol. 5, pp. 1–19, 2021.
[93] Q. Wu, K. He, and X. Chen, "Personalized federated learning for intelligent IoT applications: A cloud-edge based framework," IEEE Open Journal of the Computer Society, vol. 1, pp. 35–44, 2020.
[94] R. Singh and S. S. Gill, "Edge AI: A survey," Internet of Things and Cyber-

Online ISSN 3007-3197
Print ISSN 3007-3189

Physical Systems, vol. 3, pp. 71–92, 2023.

[95] Y. Shi, K. Yang, T. Jiang, J. Zhang, and K. B. Letaief, "Communication-efficient edge AI: Algorithms and systems," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2167–2191, 2020.

[96] D. Liu, H. Kong, X. Luo, W. Liu, and R. Subramaniam, "Bringing AI to edge: From deep learning's perspective," Neurocomputing, vol. 485, pp. 297–320, 2022.

[97] "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks," Scientific Reports, 2024.

[98] "Intelligent energy management across smart grids deploying 6G IoT, AI, and blockchain in sustainable smart cities," IoT (MDPI), vol. 5, no. 3, Art. 25, 2024.

[99] "Integration of blockchain with artificial intelligence technologies in the energy sector: A systematic review," Frontiers in Energy Research, 2024.

[100] "Survey on blockchain, artificial intelligence, and 6G wireless communication," University of Warwick research repository, 2023.

[101] Y. Qian, "Edge intelligence for next generation wireless networks," IEEE Wireless Communications, vol. 28, no. 2, pp. 2–3, 2021.

[102] M. Capra, R. Peloso, G. Masera, M. Ruo Roch, and M. Martina, "Edge computing: A survey on the hardware requirements in the Internet of Things world," Future Internet, vol. 11, no. 4, Art. 100, 2019.

[103] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," IEEE Access, vol. 6, pp. 6900–6919, 2018.