International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Review of Artificial Intelligence and Machine Learning Applications in the Internet of Things

Mathew Wintters[1], Viswanath Kapoor[2]

[1]Senior Systems Engineer, Eero LLC, SFO, CA, USA
[2]Systems Engineer, Eero LLC., SFO, CA, USA;

Abstract
The Internet of Things (IoT) generates vast amounts of data from billions of connected devices, and artificial intelligence (AI), particularly machine learning (ML), has become the primary means of turning that data into useful action. This review surveys how AI and ML are applied across the IoT. The main families of learning techniques used in IoT settings are first outlined, including supervised, unsupervised, and reinforcement learning, deep learning, federated learning, and the on-device methods grouped under TinyML. The application of these techniques is then reviewed across several domains. Data analytics and predictive maintenance are considered first, where ML is used to forecast equipment failures and reduce downtime. Applications in healthcare, smart cities, and industry are then surveyed. The use of AI for IoT security, especially for intrusion and anomaly detection, is examined next, followed by the more recent use of AI, including large language model (LLM) based and agentic systems, for managing IoT networks. The main challenges are identified, including data quality, limited device resources, privacy, and the reliability of autonomous systems, and directions for future work are suggested. A broad and current map of where AI and ML are used in the IoT, and of the problems that remain, is intended to be provided for practitioners and researchers.

Keywords: Internet of Things, Machine Learning, Artificial Intelligence, Deep Learning, Edge AI, Predictive Maintenance

1. Introduction

The Internet of Things (IoT) has connected billions of devices that continuously sense and report data about their environment. The value of the IoT lies less in the devices themselves than in what can be done with the data they produce, and it is here that artificial intelligence (AI) and, in particular, machine learning (ML) have become central. Patterns that are difficult to capture with fixed rules can be learned from data, which allows IoT systems to classify events, predict outcomes, detect anomalies, and increasingly to act on their own [1].

The pairing of AI and the IoT is now widespread across sectors, from consumer smart homes to industrial plants, healthcare, and city infrastructure. As deployments have grown, the role of AI has broadened from offline analytics toward real-time inference at the network edge and, most recently, toward the autonomous management of the networks themselves. This landscape is surveyed in the present review.

The remainder of the paper is organised as follows. The main ML techniques used in IoT settings are outlined first. Their application is then reviewed across analytics and predictive maintenance, and across healthcare, smart cities, and industry. The use of AI for IoT security and for network management is examined next, and the review closes with the main challenges and directions for future work.

2. Review Scope and Approach

This work is presented as a broad narrative review rather than a systematic one. Survey articles, peer-reviewed studies, and recent preprints were consulted, with an emphasis on material published between 2023 and 2026. The aim is coverage rather than depth on any single method, so the review favours breadth across techniques and application domains. Where a topic has been treated in detail elsewhere, the reader is referred to the relevant survey.

3. Machine Learning Techniques Used in the IoT

A range of learning techniques is used in IoT systems, and the choice depends on the task and the resources available. Supervised learning, in which models are trained on labelled examples, is used for classification and regression tasks such as activity recognition and failure prediction. Unsupervised learning is used where labels are scarce, for example in clustering and anomaly detection. Reinforcement learning, in which an agent learns from feedback, is applied to control and scheduling problems. Deep learning, using neural networks with many layers, underpins most recent advances, particularly for images, audio, and time-series data [1].

Two developments are especially relevant to the IoT. Federated learning allows models to be trained across many devices without moving raw data to a central server, which suits the privacy and bandwidth constraints of the IoT. On-device methods, grouped under the term TinyML, compress models so that inference can run on microcontrollers with very limited memory and power, and recent work has extended this from simple models toward tiny deep learning [2]. Together these techniques move intelligence closer to the device, which reduces latency and the amount of data that must be transmitted.

4. Data Analytics and Predictive Maintenance

One of the most established uses of ML in the IoT is predictive maintenance. Sensor data from machinery, such as vibration, temperature, and current, is used to forecast when a component is likely to fail, so that maintenance can be scheduled before a breakdown occurs. Studies in industrial IoT report that ML-based prediction can substantially outperform traditional schedule-based maintenance, with improvements in prediction accuracy and reductions in downtime and cost [3]. In smart-factory settings, AI-driven predictive maintenance has been used to cut unplanned downtime and extend equipment life [4].

More generally, the IoT produces continuous streams of data that are well suited to ML-based analytics. Forecasting demand, detecting drift in a process, and optimising energy use are all common applications. The pattern in each case is similar, in that historical sensor data is used to train a model that then informs a decision, either by alerting an operator or by feeding an automated control loop.

5. Applications in Healthcare, Smart Cities, and Industry

Healthcare is one of the fastest-growing areas of AI-enabled IoT. The Internet of Medical Things connects wearable sensors, implantable devices, and remote monitors, and ML is used to interpret the resulting signals for diagnosis, chronic-disease management, and early warning. Because health data is sensitive, security and privacy are particularly important in this domain, and reviews of healthcare-IoT

have highlighted the need to pair ML with strong protection of patient data [5].
In smart cities, AI-enabled IoT is used for traffic management, waste collection, environmental monitoring, and energy-efficient buildings, with the aim of reducing cost and environmental impact. In industry, the Industrial IoT applies the same tools to improve efficiency, safety, and automation, with predictive maintenance as a leading example. Across these domains the common theme is the use of learned models to turn large volumes of sensor data into timely decisions.

6. Artificial Intelligence for IoT Security

Security is both an application of AI in the IoT and a requirement for it. Because IoT devices are numerous and often weakly protected, ML is widely used for intrusion and anomaly detection, where it can flag attacks that signature-based tools miss. Deep learning models have been reported to improve detection at the scale of realistic IoT networks [6], and comprehensive surveys have catalogued the supervised, unsupervised, reinforcement, deep, ensemble, federated, and transfer learning methods applied to IoT security [1]. In sensitive domains such as healthcare, the same techniques are used to protect data and detect misuse [5].

7. Artificial Intelligence for IoT Network Management

The most recent shift is the use of AI to manage IoT networks, not only to analyse their data. As deployments grow in size and heterogeneity, manual configuration and troubleshooting do not scale, and learning-based methods are increasingly used to allocate resources, tune parameters, and respond to faults. Large language model based methods have been proposed for semantic communication at the network edge, where meaning rather than raw bits is prioritised to suit IoT constraints [7].
A further step is the use of agentic AI, in which models plan and act on the network. Cloud-based frameworks have been proposed in which agents monitor a heterogeneous IoT deployment, configure devices and gateways, and remediate faults with limited human input [8]. Related surveys describe how such agentic and LLM-based systems are being applied to autonomous IoT management and cybersecurity [9], and the broader move from high-level intents to autonomous action is an active research theme [10]. These approaches are promising, but the literature is consistent in stressing that autonomous control must be paired with guardrails and human oversight.

8. Challenges and Future Directions

Several challenges cut across these applications. Data quality and the scarcity of labelled data limit supervised methods, and models trained in one setting often transfer poorly to another. The limited memory, compute, and energy of IoT devices constrain what can run at the edge, although TinyML continues to narrow this gap [2]. Privacy remains a central concern, since useful models depend on large volumes of potentially sensitive data. The reliability and security of AI itself is a growing issue as models are given more control, and agent-based systems in particular need careful evaluation before they are trusted with autonomous action [11]. Progress is likely to come from combining efficient on-device learning, privacy-preserving training, and well-governed automation rather than from larger models alone.

9. Conclusion

Artificial intelligence and machine learning have become the primary means of extracting value from the

Internet of Things. Across analytics, predictive maintenance, healthcare, smart cities, industry, security, and network management, learned models are used to turn sensor data into decisions and, increasingly, into autonomous action. The techniques range from classical classifiers to deep learning, federated learning, and on-device TinyML, and the trend is toward moving intelligence closer to the device and toward greater autonomy. The main obstacles are data quality, limited device resources, privacy, and the reliability of autonomous systems. Addressed carefully, AI and ML will continue to expand what the IoT can do; addressed carelessly, they will introduce new risks of their own.

Acknowledgement
No external funding was received for this work. The authors thank their colleagues for helpful discussions.

References
1. "Machine Learning-based Security Solutions for IoT Networks: A Comprehensive Survey", Sensors, 2025, vol. 25, no. 11, article 3341.
2. "From Tiny Machine Learning to Tiny Deep Learning: A Survey", arXiv preprint arXiv:2506.18927, 2025.
3. "Industrial IoT Predictive Maintenance using Machine Learning Approach", Lecture Notes in Networks and Systems, Springer, 2024.
4. "AI-Powered Predictive Maintenance in IoT-Enabled Smart Factories", Research Annals of Industrial and Systems Engineering, 2024.
5. "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation", arXiv preprint arXiv:2401.09124, 2024.
6. "Deep Learning-based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach", EURASIP Journal on Information Security, 2025.
7. "Large Language Models for Semantic Communication in Edge-based IoT Networks", arXiv preprint arXiv:2407.20970, 2024.
8. R. Rajidi, "Wi-Fi Evolution and IoT Interoperability Challenges: A Cloud-based Agentic AI Framework for Intelligent Network Management", Proceedings of the 2026 IEEE World AI IoT Congress (AIIoT), 2026, pp. 831-837.
9. "Agentic AI and Large Language Models for Autonomous IoT Cybersecurity: A Systematic Survey, Taxonomy, and Research Roadmap", Electronics, 2026, vol. 15, no. 12, article 2740.
10. "From Intents to Actions: Agentic AI in Autonomous Networks", arXiv preprint arXiv:2602.01271, 2026.
11. "LLM Agents for Internet of Things Applications", OpenReview, 2025.