International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 11 November-2026 | Impact Factor: 3.5



AI-Based IOT Anomaly Detection and Predictive Maintenance

Radha Kadam[1], Sakshi Dhengre[2], Radha Yadaw[3]

[1] UG Student, Department of Computer Science & Engineering Data Science, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India
[2] UG Student, Department of Computer Science & Engineering Data Science, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India
[3] UG Student, Department of Computer Science & Engineering Data Science, Guru Nanak Institute of Technology, Nagpur, Maharashtra, India
Corresponding Author Email: radhakadam614@gmail.com | ORCID: https://orcid.org/[to be added]

How to Cite this Article:
Kadam, R., Dhengre, S. & Yadaw, R. (2026). AI-Based IOT Anomaly Detection and Predictive Maintenance. International Journal of Creative and Open Research in Engineering and Management, 02(11), 1-9. https://doi.org/10.55041/ijcope.v2i11.154

License:
This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.
© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.







https://doi.org/10.55041/ijcope.v2i11.154

Abstract—

Industrial equipment failures can cause costly downtime, safety risks, and poor product quality, while fixed maintenance schedules may replace components too early or miss faults that develop between inspections. Internet of Things (IoT) sensors now make continuous condition monitoring possible, but sensor data are often noisy, incomplete, or affected by changing operating conditions. This paper presents a comparative literature review of artificial intelligence (AI) methods for anomaly detection and predictive maintenance in IoT and Industrial IoT systems. The study is desk-based and examines statistical methods, classical machine learning, deep learning, sensor-data preprocessing, and edge and cloud deployment across five themes. The review finds that anomaly detection can flag unusual machine behavior, whereas predictive maintenance uses historical and live condition data to estimate the risk of failure. Recurring challenges include scarce fault labels, data drift, limited computing resources at the edge, weak model explainability, cybersecurity concerns, and the difficulty of comparing results across datasets. Combining IoT monitoring with suitable AI models can support earlier fault identification and better maintenance planning, but these benefits depend on data quality, domain-aware evaluation, and the integration of model outputs into maintenance decisions. The paper concludes that future studies should evaluate complete pipelines, from sensor data to maintenance action, using measures such as false-alarm rates and detection delay. Such work can help AI-based maintenance move from research prototypes to reliable industrial practice.

Keywords— Internet of Things (IoT); Industrial IoT; anomaly detection; predictive maintenance; machine learning; condition monitoring

I. INTRODUCTION

Industrial equipment is essential to manufacturing, energy, transportation, and other infrastructure. Unexpected equipment failures can interrupt production, increase repair costs, reduce product quality, and create safety risks. Conventional maintenance strategies are commonly organized as reactive maintenance, which occurs after a failure, or preventive maintenance, which follows a fixed schedule. Reactive maintenance may cause costly downtime, whereas scheduled servicing may replace parts that still have useful operating life.

The Internet of Things (IoT) enables machines and physical assets to be monitored through connected sensors. Depending on the equipment, sensors may measure vibration, temperature, pressure, current, acoustic signals, speed, humidity, or other process variables. The collected readings form time-series data that can be analyzed to understand normal behavior and identify unusual changes. Industrial IoT (IIoT) extends this approach to connected industrial equipment and production environments.

AI and machine-learning techniques can analyze sensor data at a scale that is difficult to achieve



through manual inspection alone. Anomaly detection identifies observations or patterns that differ from expected behavior. Predictive maintenance goes a step further by using condition data and predictive models to support decisions before a breakdown occurs. These tasks are related but not identical: an anomaly may indicate a fault, sensor noise, or a legitimate change in operating conditions, and not every anomaly results in equipment failure.

This paper reviews published research on IoT anomaly detection and AI-enabled predictive maintenance. It brings together studies on general IoT time-series anomalies, sensor-network approaches, industrial anomaly classification, and predictive-maintenance frameworks. The objective is to summarize common methods, compare their strengths and limitations, and identify research gaps relevant to practical systems.

II. LITERATURE REVIEW AND RESEARCH GAP

Research on IoT anomaly detection has expanded alongside the growth of connected sensors and industrial monitoring. Sgueglia et al. [1] reviewed IoT time-series anomaly-detection solutions and discussed dimensionality reduction, anomaly localization, real-time monitoring, datasets, and open challenges. Their review highlights that IoT data analysis must operate under timing and resource constraints, not simply maximize model accuracy.

DeMedeiros, Hendawi, and Alvarez [2] surveyed AI-based anomaly detection in IoT and sensor networks. Their work covers machine-learning and deep-learning approaches and emphasizes the importance of defining anomalies and understanding the characteristics of sensor data. The survey shows that anomaly detection spans multiple domains, making it difficult to rely on one algorithm for every deployment.

Rodríguez, Tobón, and Múnera [3] reviewed anomaly classification in the Industrial IoT. They found that much IIoT anomaly research has focused on cybersecurity events, while classification of industrial operational anomalies and the use of contextual information remain important research opportunities. This matters for maintenance because the system must distinguish equipment degradation from network attacks, sensor faults, and normal process variation.

A systematic mapping study published in IEEE Access [4] examined machine-learning approaches for anomaly detection in industrial machinery using IoT devices. The mapping considered sensor types, preprocessing, algorithms, application areas, and challenges across studies. It illustrates the growing interest in combining condition-monitoring data with AI, while also showing that the choice of model depends on the machine, signals, and fault types.

Zonta et al. [5] surveyed predictive maintenance in Industry 4.0 and described the role of data-driven monitoring and predictive approaches in industrial maintenance. More recently, a literature-review framework published in 2025 [6] analyzed a broad collection of Industry 4.0 predictive-maintenance publications and discussed issues such as model complexity, the availability of benchmark datasets, and the integration of machine learning into industrial practice. Table I summarizes the main focus and key contribution or limitation of each selected study.

Table I: Comparison Across Selected Literature

Study	Main Focus	Key Contribution / Limitation
Sgueglia et al. [1]	IoT time-series anomaly detection	Reviews methods, datasets, localization, and real-time constraints; further comprehensive solutions are needed.
DeMedeiros et al. [2]	AI anomaly detection in IoT and sensor networks	Surveys ML/DL methods and research gaps across sensor domains.
Rodríguez et al. [3]	Industrial IoT anomaly classification	Highlights security-heavy focus and need for operational anomaly classification and context.
Industrial machinery mapping [4]	IoT sensors and ML for machinery anomalies	Maps algorithms, preprocessing, and sensor types; deployment remains context-dependent.
Zonta et al. [5]	Predictive maintenance in Industry 4.0	Summarizes data-driven maintenance approaches and monitoring taxonomies.
Industry 4.0 review framework [6]	Predictive maintenance research landscape	Analyzes a broad publication set; identifies dataset, complexity, and integration challenges.



Research gap: Existing reviews often focus separately on IoT anomaly detection, industrial fault classification, or predictive maintenance. A practical maintenance solution needs a connected pipeline: sensor data collection, data quality checks, anomaly detection, failure-risk estimation, alerts, and maintenance decisions. Further work is needed to evaluate this complete pipeline under realistic operating conditions, including changing loads, limited labels, edge-device constraints, and the cost of false alarms.

III. METHODOLOGY

This paper uses a comparative literature-review methodology and does not report a new industrial experiment. Published review and research articles were selected for their relevance to AI-based anomaly detection in IoT or IIoT systems and predictive maintenance. The selected works cover general IoT time-series analysis, sensor-network anomaly detection, industrial anomaly classification, machinery monitoring, and Industry 4.0 maintenance.

For each work, the review considered its main focus, techniques discussed, application context, reported contribution, and limitations. Findings were grouped into five themes: (1) data acquisition and preprocessing; (2) anomaly-detection algorithms; (3) predictive-maintenance tasks; (4) deployment and system integration; and (5) challenges and future research. Since the included publications use different datasets, target faults, and evaluation metrics, their results are compared qualitatively rather than treated as directly interchangeable benchmark scores.

The review is desk-based and depends on the scope and reporting of the cited publications. It does not claim that all available literature has been covered, nor does it present newly measured accuracy, latency, or cost figures.

IV. RESULTS AND DISCUSSION

A. IoT Data Collection and Preprocessing

An IoT monitoring pipeline begins with sensors attached to machines or process equipment. Sensor readings may be transmitted through a gateway to an edge device or cloud platform. Before model inference, data commonly require timestamp alignment, missing-value handling, noise filtering, normalization, and segmentation into suitable time windows. Inadequate preprocessing can create false alarms or hide early warning signs. Sensor placement and sampling frequency are also important because a fault may appear only in a particular signal or time scale.

B. AI Techniques for Anomaly Detection

Statistical methods establish expected ranges or distributions and flag deviations. They are relatively simple and can be suitable where the operating process is stable, but may struggle with complex interactions among multiple sensor variables. Classical machine-learning methods, including Isolation Forest, One-Class SVM, clustering, and tree-based classifiers, can identify unusual patterns when appropriate features are available. Supervised classification can work well when labeled examples of normal and faulty states are sufficiently representative, but fault labels are often scarce.

Deep-learning models such as autoencoders, recurrent neural networks, and convolutional neural networks can learn more complex temporal or multivariate patterns. Autoencoders may be trained on normal behavior and use reconstruction error to flag unusual observations. Recurrent models can represent sequences, while convolutional models can extract patterns from signal windows. However, deep models may need more data and computing resources, and their decisions can be harder to explain. The literature does not establish a single best algorithm for all IoT settings; performance depends on data, fault type, and deployment requirements.

C. From Anomaly Detection to Predictive Maintenance

Anomaly detection answers whether current behavior differs from an expected baseline. Predictive maintenance aims to estimate future equipment condition, failure probability, fault category, or remaining useful life (RUL). A system may first detect an abnormal vibration pattern and then combine it with temperature, load, operating hours, and maintenance history to estimate risk. The output can be used to prioritize inspection, schedule servicing, or order replacement parts.

A detected anomaly should not automatically trigger a costly maintenance action. Transient events, changes in production settings, or faulty sensors can resemble equipment degradation. Effective systems therefore combine model scores with operational context, persistence rules, thresholds, and, where possible, expert confirmation. A useful system should communicate the suspected asset, time, signal, anomaly severity, and supporting evidence.



D. Edge and Cloud Deployment

Edge computing processes data near the machine, which can reduce communication delay and limit the amount of raw data sent to the cloud. It is useful for time-sensitive alerts and sites with unreliable connectivity, but edge hardware may constrain model size and update frequency. Cloud platforms provide scalable storage, centralized dashboards, and the ability to train or update models using data from multiple assets. A hybrid architecture can perform immediate screening at the edge and deeper analysis in the cloud.

E. Challenges and Research Opportunities

First, real industrial fault data are often imbalanced: normal operation is common, while failures are rare. Second, operating conditions change over time, creating data drift that can reduce model reliability. Third, datasets and evaluation practices vary, making cross-study comparisons difficult. Fourth, false positives can cause unnecessary inspections, while false negatives can miss dangerous faults. Fifth, industrial systems require cybersecurity, privacy, availability, and dependable communication. Finally, models must be interpretable enough for technicians to trust and act on their recommendations.

Future work should evaluate models on diverse machines and real-world data, report precision, recall, false-alarm rates, detection delay, and resource use, and assess performance under changing conditions. Research should also connect model predictions to maintenance workflows and include human feedback rather than treating prediction accuracy as the only measure of success.

DeMedeiros et al. [2] AI anomaly detection in IoT and sensor networks Surveys ML/DL methods and research gaps across sensor domains.

Rodríguez et al. [3] Industrial IoT anomaly classification Highlights security-heavy focus and need for operational anomaly classification and context.

Industrial machinery mapping [4] IoT sensors and ML for machinery anomalies Maps algorithms, preprocessing, and sensor types; deployment remains context-dependent.

Zonta et al. [5] Predictive maintenance in Industry 4.0 Summarizes data-driven maintenance approaches and monitoring taxonomies.

Industry 4.0 review framework [6] Predictive maintenance research landscape Analyzes a broad publication set; identifies dataset, complexity, and integration challenges.

V. CONCLUSION

The reviewed literature shows that AI-based IoT anomaly detection and predictive maintenance are important components of data-driven industrial operations. IoT sensors provide continuous information about equipment condition, while statistical, machine-learning, and deep-learning techniques can identify unusual behavior and support estimates of future failure. Anomaly detection and predictive maintenance complement each other, but they address different stages of the maintenance process.

The main benefits are earlier identification of potential faults, improved maintenance planning, reduced dependence on fixed schedules, and better visibility into machine condition. However, these benefits depend on reliable sensor data, representative training datasets, suitable model selection, and integration with operational decision-making. Data drift, limited fault examples, false alarms, explainability, and edge-device constraints remain significant barriers.

Future systems should combine anomaly detection with predictive models, contextual machine information, and technician feedback. Evaluation should include not only predictive metrics but also alert delay, false-alarm burden, resource consumption, and practical maintenance outcomes. A robust end-to-end design can help translate AI predictions into safer and more efficient maintenance practices.

REFERENCES

[1] A. Sgueglia, A. Di Sorbo, C. A. Visaggio, and G. Canfora, “A systematic literature review of IoT time series anomaly detection solutions,” Future Generation Computer Systems, vol. 134, pp. 170–186, 2022, doi: 10.1016/j.future.2022.04.005.

[2] K. DeMedeiros, A. Hendawi, and M. Alvarez, “A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks,” Sensors, vol. 23, no. 3, art. 1352, 2023, doi: 10.3390/s23031352.

[3] M. Rodríguez, D. P. Tobón, and D. Múnera, “Anomaly classification in industrial Internet of



things: A review," Intelligent Systems with Applications, vol. 18, art. 200232, 2023, doi: 10.1016/j.iswa.2023.200232.

[4] [Authors to be added], "Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping," IEEE Access, vol. 11, pp. 128288–128305, Nov. 2023, doi: 10.1109/ACCESS.2023.3333242.

[5] T. Zonta, C. A. da Costa, R. da Rosa Righi, M. J. de Lima, E. S. da Trindade, and G. P. Li, "Predictive maintenance in the Industry 4.0: A systematic literature review," Computers & Industrial Engineering, vol. 150, art. 106889, 2020, doi: 10.1016/j.cie.2020.106889.

[6] [Authors to be added], "A Literature Review Framework and Open Research Challenges for Predictive Maintenance in Industry 4.0," Computers & Industrial Engineering, vol. 206, art. 111193, 2025, doi: 10.1016/j.cie.2025.111193.