Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Machine Learning Techniques for Anomaly Detection in IoT and WSN: A review

Israa Abdulkadhim Jabbar Al Ali[a,*], *Manaf Mohammed Ali Alhaidery*[b]

[a,b] *University of Kerbala, College Of Education For Human Sciences, Kerbala, Iraq.*

Email: israa.jabbar@uokerbala.edu.iq ; manaf.m@uokerbala.edu.iq

ARTICLE INFO

Article history:
Received: 19/04/2025
Rrevised form: 22/05/2025
Accepted : 18/06/2025
Available online: 30 /06/2025

Keywords:

Anomaly Detection, Cybersecurity, Deep Learning, Internet of Things (IoT), Machine Learning, Wireless Sensor Networks (WSN)

ABSTRACT

Quick Internet of Things (IoT) and Wireless Sensor Networks (WSN) proliferation have considerably raised real-life and automation monitoring, data-based decision-making over various fields such as industrial systems, healthcare, and smart cities. Although great IoT device development defines security vulnerabilities and operational risks, it signifies strong anomaly diagnosis algorithms for recognizing system failures, unusual behaviors, and cyber threats. Traditional rule-based and statistical techniques cope with controlling active, massive, and high-dimensional IoT data aspects, creating methods of machine learning (ML) that are promising alternatives for appropriate and scalable unusual diagnosis. The present paper shows a general review of ML-based unusual diagnosis strategies in IoT and WSN, grouping them into hybrid, unsupervised, and supervised learning methods. In addition, it examines deep learning architectures, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and Transformer-based models, highlighting their strengths in capturing complex spatial and temporal dependencies in sensor data. Despite their efficiency, ML-based techniques meet some issues like real-life limitations, data scarcity, high computational costs, adversarial vulnerabilities, and a shortage of generalization over various IoT areas. For considering such issues, this review describes the present paper's directions. Though state-of-the-art methods' analysis and highlighting future trends, the present paper targets present worthy perspectives for investigators and practitioners in improving more adaptive, safe, effective ML-based unusual diagnosis responses for IoT and WSN

MSC..

https://doi.org/10.29304/jqcsm.2025.17.22198

1. Introduction

The Internet of Things (IoT) has become a game changer in the dynamic world of information technology (IT), connecting everyday gadgets to the Internet to build smarter, more interactive, and automated ecosystems. Nonetheless, the rapid development of IoT technology has been accompanied by significant security problems, which have piqued the interest of both researchers and industry experts [1]. The rapid growth of the IoT and Wireless Sensor Networks (WSNs) has had a substantial impact on several fields, including environmental monitoring, healthcare, smart city development, and industrial automation [2]. A typical IoT design is divided into three basic layers: perception (sensor), network, and application. However, due to limited resources and complex

[*] Corresponding author: Israa Abdulkadhim Jabbar Al Ali

Email addresses: *israa.jabbar@uokerbala.edu.iq*

Communicated by 'sub etitor'

system designs, IoT environments are vulnerable to a wide range of passive and active security attacks. These systems are extremely complicated and difficult to safeguard. As IoT adoption expands, it introduces several challenges across diverse applications, including issues of interoperability, data processing, standardization, storage, privacy, identity management, and trust. Addressing this broad spectrum of challenges is essential for developing a secure and reliable IoT ecosystem [3].

These systems continuously generate vast amounts of data that must be monitored for anomalies indicating potential malfunctions, environmental changes, or security breaches. Traditional rule-based anomaly detection techniques struggle to scale with the increasing complexity and dynamic nature of modern IoT and WSN environments [4].

Anomaly detection (AD) is important in many sectors, including removing noise from datasets and preventing data poisoning attempts. In the medical area, AD can be used to detect anomalous physiological circumstances, such as aberrant body temperatures, using health data collected from medical IoT devices, so assisting in the prevention of major incidents and management of ongoing conditions. In smart home contexts, it can detect abnormal patterns such as sudden temperature spikes, which could indicate malevolent interference. Similarly, in the manufacturing sector, AD aids machine condition monitoring and resource optimization by detecting anomalies in parameters such as smoke levels, temperature, and humidity, hence improving operational dependability and safety [5].

Quick IoT deployment has brought considerably complicated issues, AD is being progressively used for IoT data. ML methods are prevalent and are broadly applied in IoT, AD. Novel technical applications have appeared in recent years [6]. ML methods, such as DL, semi-supervised, supervised, and unsupervised learning models, have been broadly explored to increase AD accuracy and efficiency. Such strategies could recognize cyber threats, diagnose sensor failures, and optimize network performance in real-life apps [7].

AD that recognizes deviations from normal device/system behavior is becoming a crucial new security approach element. Through observing models and recognizing anomalies, AD could aid in diagnosing potential threats before they cause ruin [8]. Early AD makes it a quick task to avoid data breaches and decrease service disruption. Such a proactive strategy aids in recognizing and mitigating unauthorized access attempts, strengthening network security. Also, AD could adapt to novel threats that traditional techniques might overlook, presenting general protection. IoT systems in real-life applications need algorithms of security which are flexible and responsive to present threats. Performing strong AD raises total system resilience, keeping network integrity and operational stability. Since IoT ecosystems evolve, new security systems should evolve to stay ahead of rising important cyber threats [9].

Despite developments, AD based on ML in IoT and WSN meets some concerns, including restricted computational resources, energy limitations, high-dimensional data, and evolving attack models [10]. Also, accurate ML model selection relies on the dataset aspect, labeled data accessibility, and particular app needs.

The paper provides a general ML method applied to AD in IoT and WSN. We group present techniques given their learning paradigms and describe their strengths, restrictions, and real-life apps. In addition, we bold the main issues and future study directions to develop AD in resource-limited and active areas of IoT.

The paper is structured as follows: Section 2 gives an overview of anomaly detection in IoT and WSNs, focusing on core ideas, important problems, and the use of machine learning in this context. Section 3 provides a full classification and explanation of machine learning-based anomaly detection strategies, which include unsupervised, supervised, semi-supervised, and deep learning methods. Section 4 investigates real-world use cases and applications from a variety of industries, including cybersecurity, healthcare, and smart city infrastructures. Section 5 discusses existing constraints and future research possibilities. Finally, Section 6 wraps up the paper by summarizing the key findings and contributions.

2. Background and Fundamentals

2.1 Anomaly Detection in IoT and WSN

The IoT and WSNs are typically divided into three fundamental layers (Fig. 1): the Perception Layer, the Network Layer, and the Application Layer.

The Perception Layer serves as the system's sensory component, collecting physical data from the surroundings via sensors, RFID tags, and cameras. It acts as a vital link between the physical world and digital systems, yet it is highly vulnerable to physical security threats such as hardware tampering, node capture, and malicious interference. The Network Layer is in charge of transmitting the obtained data over communication protocols such as Wi-Fi, ZigBee, and cellular networks. This layer provides smooth connectivity between edge devices and central processing systems such as cloud services, but it is vulnerable to dangers such as illegal data access, denial-of-service (DoS) assaults, and traffic monitoring. The Application Layer is the highest level of the architecture, and it is responsible for interpreting and exploiting sent data to provide intelligent and domain-specific services. Its applications are diverse, ranging from smart home systems to remote healthcare monitoring and industrial automation. This layer is especially vulnerable to viruses, privacy breaches, and unwanted data access. Understanding this layered structure not only illustrates the flow of data in IoT systems, but also emphasizes the unique security challenges that exist at each level [2].

AD is an unusual model/manner's recognition in data, which considerably deviates from expected norms. In IoT and WSN areas, anomalies could be caused by network congestion, cyberattacks, sensor failures, and environmental shifts [11]. Diagnosing these anomalies is important to guarantee the effectiveness, security, and reliability.

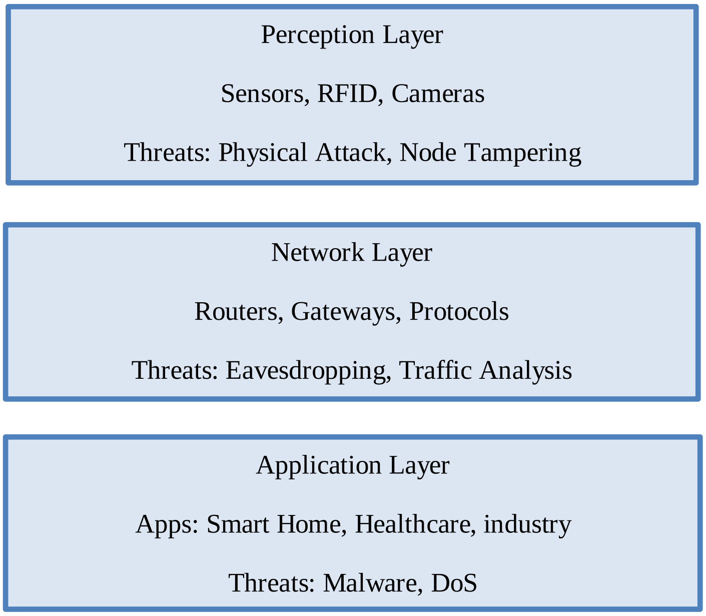
Perception Layer
Sensors, RFID, Cameras
Threats: Physical Attack, Node Tampering
Network Layer
Routers, Gateways, Protocols
Threats: Eavesdropping, Traffic Analysis
Application Layer
Apps: Smart Home, Healthcare, industry
Threats: Malware, DoS

Figure 1. IoT and WSN architecture

As you can see in Fig. 2, IoT and WSN anomalies could be grouped into three basic kinds [12]:

- **Point anomalies**: These are individual data points that differ dramatically from the predicted typical trend, such as a sudden increase in temperature readings recorded by a sensor.
- **Contextual anomalies:** occur when data points are odd solely in a particular context or setting. For example, a high temperature measurement in the winter may be regarded abnormal yet typical in the summer.
- **Collective anomalies**: This category consists of a collection of related data points that, when viewed together, reveal anomalous behavior. An odd pattern in network traffic may indicate a distributed denial-of-service (DDoS) attack.

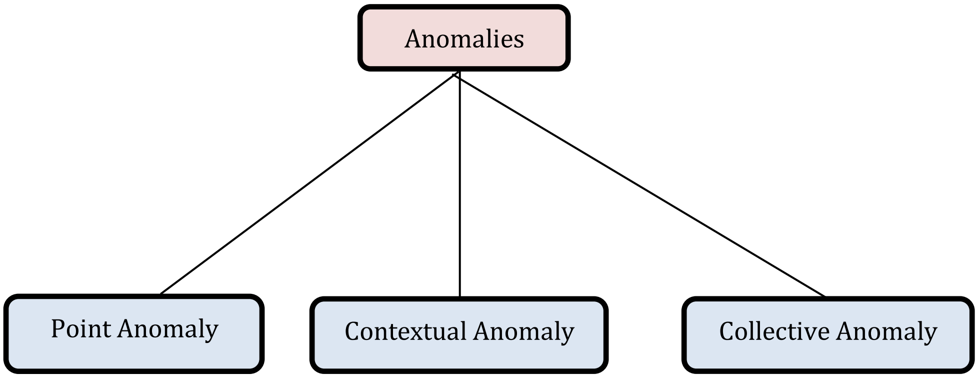

Figure 2. Types of Anomalies in IoT/WSN

2.2 ANOMALY DETECTION ISSUES FOR IOT AND WSN

AD in IoT and WSN is challenging because of some agents:

- **Resource limitations:** A lot of IoT and WSN devices have restricted battery life, computational power, and memory, making it hard to develop complicated ML models [13].
- **High-dimensional and heterogeneous data**: IoT devices make various data types such as images, time-series, and categorical data, requiring developed feature engineering methods [14].
- **Data imbalance**: Anomalous events are rare in comparison with normal events, causing imbalanced sets of data, which hinder supervised learning models' performance [15].
- **Real-life processing**: A lot of applications of IoT need real-life anomaly diagnosis, signifying light and effective ML models [16].
- **Security and privacy issues**: Transmitting and processing sensitive IoT data in centralized ML models has risks associated with data security and privacy [17].

2.3 MACHINE LEARNING FOR ANOMALY DETECTION

ML has drawn considerable attention for its ability to diagnose anomalies with no dependence on predefined laws. ML models could learn from historical data and recognize deviations that show potential threats. Basic ML methods applied for AD include:

- **Supervised Learning**: Needs labeled sets of data, where normal and anomalous samples are predefined. Usual mechanisms contain Neural Networks, Support Vector Machines (SVM), and Decision Trees [18].
- **Unsupervised Learning**: Does not need labeled data and diagnoses anomalies through recognizing deviations from learned models. Well-known techniques include K-Means grouping, Isolation Forest, and Autoencoders [19].
- **Semi-supervised Learning**: Applies a small labeled dataset integrated with massive unlabeled data for developing AD performance [20].
- **DL strategies**: Developed neural network frameworks like Convolutional Neural Networks (CNN), Transformers, and Long Short-Term Memory (LSTM) networks have been successfully used in AD in IoT and WSN because of their ability to extract complicated temporal and spatial features [21].

3. Machine Learning Methods for Anomaly Detection

ML methods have revolutionized AD in IoT and WSN by making automatic and adaptive abnormal model recognition possible. Present part groups such methods into DL, **supervised, unsupervised, semi-supervised techniques**, highlighting their use cases, restrictions, and benefits.

3.1 SUPERVISED LEARNING METHODS

Supervised learning depends on labeled sets of data where anomalies are marked. Such techniques are efficient when enough labeled data volume is accessible; however, they might struggle with unobserved anomalies.

- **SVM:** A Robust classification mechanism that explores an optimal hyperplane for separating normal and anomalous data points. This is broadly applied in IoT security apps, like intrusion detection [18].

- **Decision Trees and Random Forests:** Decision trees make a hierarchy of conditions to group data, and when random forests apply multiple trees, for develop robustness. They are interpretable and efficient for structured IoT data [18].
- **ANN:** These models learn complicated models from labeled data. They are efficient for AD; however, they need a massive labeled training data volume [18].

3.2 UNSUPERVISED LEARNING TECHNIQUES

Unsupervised techniques do not need labeled data and diagnose anomalies through recognizing deviations from learned models. They are effective in IoT and WSN scenarios where labeled data is scarce.

- **Clustering Algorithms (K-Means, DBSCAN):** Such a mechanism categorizes similar data points and recognizes outliers as anomalies. DBSCAN is specifically helpful to recognize anomalies in dense sensor networks [19].
- **Isolation Forest:** A tree-based ensemble technique that isolates anomalies by randomly partitioning data points. This is computationally effective and well-suited for IoT apps [19].
- **Principal Component Analysis (PCA):** Methods of dimensionality reduction that recognize anomalies through diagnosing deviations in data share principal components [19].

3.3 SEMI-SUPERVISED LEARNING TECHNIQUES

Semi-supervised techniques leverage a small labeled data with a massive unlabeled data, making them efficient for real-life IoT scenarios.

- **Autoencoders:** Neural networks trained to rebuild input data. High rebuild errors show anomalies [20].
- **Self-Learning Mechanisms:** Such models iteratively refine their decision limitations by applying labeled and unlabeled data [20].

3.4 DEEP LEARNING STRATEGIES

DL models could extract complicated features from high-dimensional IoT data, making them highly efficient for AD.

- **LSTM:** A recurrent neural network (RNN) variant modeled for sequential data analysis. This is efficient for diagnosing anomalies in time-series data made by IoT sensors [21].
- **CNN:** Applied for image-based AD, CNNs have been used to structure IoT data through learning spatial correlations [21].
- **Transformer Models:** Attention-based DL models which excel at processing massive data orders sequences, making appropriate AD in IoT networks [21].

3.5 MACHINE LEARNING METHODS' COMPARISON

Every ML technique has its strengths and weaknesses in IoT and WSN AD. Table 1 summarizes the main differences:

Table 1. ML Methods' Comparison for AD

ML Technique	Strengths	Weaknesses
SVM	High accuracy, robust for small datasets	Poor scalability, requires labeled data.
K-Means	No need for labeled data, simple implementation	Sensitive to parameter selection
Isolation Forest	No need for labeled data, simple implementation	Sensitive to parameter selection
LSTM	Fast and scalable, effective for high-dimensional data	May not capture complex patterns
Autoencoders	Learns feature representations automatically	High computational cost

4. REAL-LIFE APPLICATIONS AND CASE STUDIES

ML methods' application for AD in IoT and WSN spans different fields, such as industrial automation, cybersecurity, healthcare, environmental control, and smart cities. Present part bolds the main real-life implementations and case studies showing such strategies' efficiency.

4.1 CYBERSECURITY AND INTRUSION DETECTION IN IOT NETWORKS

Cyber threats, like unauthorized access, DDoS attacks, and malware propagation, pose considerable risks to IoT networks. ML-driven IDSs have been broadly adopted to increase security.

Smart Home IoT Security: Investigators performed IDS by applying an LSTM-driven DL model to diagnose anomalies in smart home devices' network traffic. This system successfully recognized unauthorized access tries with an accuracy of 96.5%, performing better than traditional rule-driven IDS [22].

Multiple integrating Isolation Forest and Autoencoders was developed for diagnosing unusual communication models in Industrial IoT (IIoT) networks, decreasing false positives, and with an accuracy of 99% [23].

4.2 HEALTHCARE IOT AND PATIENT MONITORING

Wearable IoT devices and remote patient monitoring systems make ongoing physiological data flows. Diagnosing anomalies in this data is critical for early disease detection and patient safety.

A DL-driven system applying CNN-LSTM was developed for diagnosing unusual heart rhythms in real-life from wearable ECG sensors. The system showed high precision in recognizing arrhythmias, decreasing misdiagnosis rates [24].

AD mechanisms were used for the hospital IoT systems in the hospital's network. Diagnosed anomalies are shown as graphs, letting us identify models over the hospital network. It helps recognize anomalies that span hybrid medical facilities, potentially showing more massive system-level risks [25].

4.3 INDUSTRIAL IOT AND PREDICTIVE MAINTENANCE

In industrial adjustments, IoT sensors continuously control machinery and tools for early fault diagnosis. Predictive maintenance systems apply ML for analyzing sensor data and diagnosing anomalies before failures happen.

An effective real-time recognition system was created to monitor sensor characteristics and provide feedback to operators. Data from industrial Computer Numerical Control (CNC) machines, such as operational temperature, vibration, and humidity, were examined using ML and Fast Fourier Transform (FFT) approaches to assess production quality. Vibration signals were translated to frequency representations, and manually gathered measurements, such as hole diameters in machined items, were used for quality control and defect diagnosis. Changes in machine settings create differences in vibration patterns and sensor data, which the Industry 4.0 module detects and informs operators to. The system was assessed using three alternative ML algorithms, which combined the results of various base estimators to improve prediction accuracy [26]. Furthermore, an LSTM-based anomaly detection model was created for an oil pipeline network to detect abnormal pressure changes, preventing potential breaches and limiting environmental concerns [27].

4.4 SMART CITIES AND INFRASTRUCTURE MONITORING

Smart city initiatives based on IoT depend on real-life data from sensors developed over urban infrastructures. AD has an important role in energy grid optimization, traffic management, and air quality monitoring.

The unsupervised learning strategy applies K-Means clustering. The presented system uses K-means clustering for categorizing network traffic data into clusters given their similarity. Through recognizing anomalous models in such groups, the system could efficiently diagnose network attacks [28].

LSTM and Autoencoder-based strategy was applied in smart grid systems for diagnosing threats and Federated Learning for resolving data silos and privacy problems [29].

4.5 ENVIRONMENTAL MONITORING AND DISASTER PREVENTION

WSNs are broadly applied for environmental monitoring, such as diagnosing seismic activity, forest fires, and air pollution. ML increases AD in such apps.

A hybrid DL model integrating humidity, SVM, CNN, wind speed data from WSN sensors, GRU (Gated Recurrent Unit) analyzed temperature, obtaining high accuracy in wildfire occurrences prediction [30].

AD mechanisms are given the deep bidirectional LSTM (DBiLSTM) mechanism, which is performed given the spatial features' extraction. The order data is processed by applying 3 models, such as CNN and CNN-LSTM, and CNN-DBiLSTM; in turn, the aim labels are grouped in the last layer [31].

Table 2 is a general comparison table summarizing ML methods applied in different IoT and WSN AD apps, such as their accuracy, aims, and other main agents.

Table 2. Comparison of ML methods for AD in IoT and WSN Apps

Application Domain	Ref	Case Study	ML Technique (s) Used	Objective	Accuracy (%)	Key Strengths	Key Limitations
Cybersecurity & Intrusion Detection	[22]	Smart Home IoT Security	LSTM-based IDS	Detect unauthorized access in smart home devices	96%	High detection rate, adaptive to dynamic threats	Requires a large labeled dataset
	[23]	IIoT Security	Isolation Forest + Autoencoders	Identify abnormal communication patterns in IIoT	99%	Reduces false positives, effective for large-scale systems	High computational cost
Healthcare IoT & Patient Monitoring	[24]	ECG Anomaly Detection	CNN-LSTM	Detect abnormal heart rhythms in wearable ECG sensors	67.3%	Real-time anomaly detection, reduced misdiagnosis	Requires extensive training data
	[25]	IoT-enabled Smart Hospitals	Graph-based Anomaly Detection	Identify EHR anomalies across multiple hospitals	-	Detects system-wide issues, interpretable patterns	Complex implementation, high resource demand
Industrial IoT & Predictive Maintenance	[26]	Manufacturing Equipment Monitoring	FFT + ML Ensemble Models	Detect faulty machine settings and production defects	97.6 %	Effective in analyzing sensor data trends	Computational complexity
	[27]	Oil & Gas Pipeline Monitoring	LSTM	Identify abnormal pressure fluctuations in pipelines	-	Prevents leaks and environmental hazards	Requires continuous retraining
Smart Cities & Infrastructure Monitoring	[28]	Traffic Anomaly Detection	K-Means Clustering	Detect traffic anomalies for smart city optimization	85.35%	Works well for unsupervised learning scenarios	Sensitive to parameter selection
	[29]	Smart Grid Anomaly Detection	LSTM + Autoencoder + Federated Learning	Detect cyber threats in smart grids while preserving	98%	Reduces data privacy concerns, scalable for	Federated learning adds communication overhead

				data privacy		large networks	
Environmental Monitoring & Disaster Prevention	[30]	Forest Fire Prediction	SVM + CNN + GRU	Predict wildfire occurrences using sensor data	97.95%	Captures complex patterns in environmental data	Requires diverse training data
	[31]	Seismic Anomaly Detection	CNN + LSTM + DBiLSTM	Detect seismic anomalies for early warning	97.23%	Effective in capturing spatial-temporal dependencies	Computationally expensive

When comparing machine learning algorithms for anomaly detection in IoT and WSN, each strategy has distinct strengths and weaknesses in terms of accuracy, efficiency, and practical applicability. Supervised learning algorithms, such as SVM, achieve excellent accuracy because they rely on labeled datasets; nevertheless, their scalability is limited, and the requirement for significant labeled data frequently presents issues in real-world IoT settings. Supervised learning algorithms, such as SVM, achieve excellent accuracy because they rely on labeled datasets; nevertheless, their scalability is limited, and the requirement for significant labeled data frequently presents issues in real-world IoT settings. Unsupervised algorithms, such as K-Means clustering and Isolation Forest, do not require labeled data, making them ideal for dynamic, ever-changing situations. However, these methods are susceptible to parameter settings and may produce inconsistent results. Deep learning techniques, such as LSTM networks and Autoencoders, excel at modeling complicated temporal and spatial correlations in sensor data, often outperforming standard algorithms in terms of accuracy and flexibility. Nonetheless, their high processing needs and reliance on huge volumes of training data can restrict their efficiency and usefulness in resource-constrained IoT devices. Hybrid models that integrate numerous techniques attempt to balance these trade-offs by harnessing the benefits of various methods, but also add complexity to implementation and interpretation. Overall, technique selection is significantly influenced by unique application requirements, data availability, and computational resources, emphasizing the importance of personalized solutions that address both performance and practicality in real-world IoT and WSN scenarios.

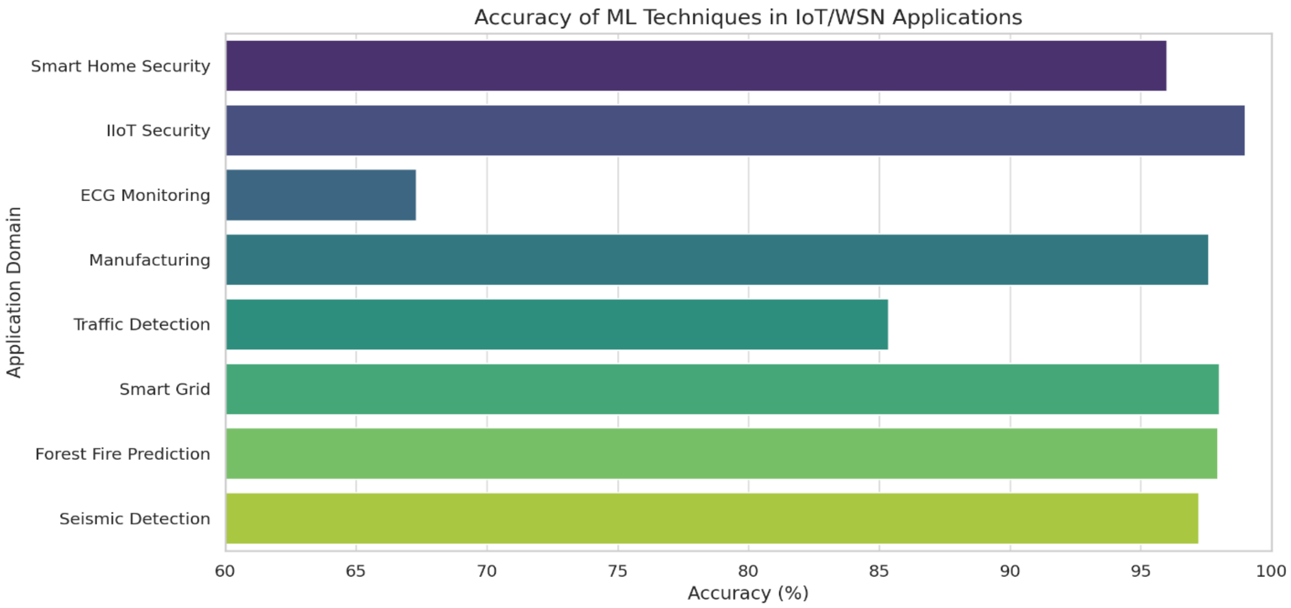

Figure 3. Accuracy comparison of ML techniques for anomaly detection across various IoT and WSN domains.

Figure 3 depicts a bar chart comparing the accuracy of various machine learning models used to detect anomalies in a variety of IoT and WSN applications. The highest accuracy (99%) in IIoT security was achieved with a hybrid model that combined Isolation Forest and Autoencoders. The highest accuracy (99%) in IIoT security was achieved with a hybrid model that combined Isolation Forest and Autoencoders. Smart grid anomaly detection employing an LSTM-Autoencoder-Federated Learning model also performed well, with an accuracy of 98%. Similarly, forest fire prediction and seismic anomaly detection achieved high accuracy rates (97.95% and 97.23%, respectively), demonstrating the efficiency of deep learning models such as CNN, GRU, and LSTM in capturing complicated environmental patterns. In contrast, the ECG anomaly identification job in the healthcare domain achieved the lowest accuracy (67.3%), most likely due to the difficulties associated with real-time physiological data fluctuation and little labeled data. These findings emphasize the need of choosing appropriate ML models based on the unique characteristics and requirements of each IoT application domain.

5. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite developments in ML for AD in IoT and WSN, some concerns exist. Such concerns stem from the active aspect of IoT areas, resource limitations, and the evolving cyber threats landscape. The present part defines the main issues and explores potential future research directions for mention.

5.1 CHALLENGES IN ML-DRIVEN ANOMALY DETECTION FOR IOT AND WSN

5.1.1 DATA SCARCITY AND IMBALANCED DATASETS

A lot of IoT AD patterns depend on supervised learning that needs a huge labeled data. Although real-life IoT sets of data sometimes lack enough labeled anomalous samples, causing weak model generalization. Anomalies are rare in comparison with normal data, resulting in imbalanced sets of data that bias models to normal samples [32]. A combination of semi-supervised and self-supervised learning methods with synthetic data creation techniques (like data augmentation, GANs) could mitigate data scarcity impacts.

5.1.2 HIGH DIMENSIONALITY AND NOISY DATA

IoT devices provide massive heterogeneous data volumes from several sensors, sometimes including extra/unrelated attributes. Noisy and missing data could degrade model performance, causing inappropriate AD [33]. Developed methods of feature selection, like Hunger Games Search (HGS) and Harris Hawks Optimization (HHO), could be applied to increase model robustness. Also, transformer-driven models could be explored to control high-dimensional sequential data.

5.1.3 REAL-LIFE ANOMALY DIAGNOSIS AND RESOURCE LIMITATIONS

Sometimes, IoT and WSN devices operate under serious computational limitations, energy, and memory restrictions, restricting the possibility of complicated DL models. Real-life AD is crucial for apps like IDS and predictive maintenance, needing low-latency processing [34]. Light DL models, like quantized neural networks, TinyML, and edge AI, could be explored for making effective AD possible on resource-limited devices.

5.1.4 ADVERSARIAL ATTACKS ON ML MODELS

ML models are vulnerable to adversarial attacks where carefully crafted inputs can deceive the AD system, causing misclassification. Attackers could manipulate IoT network traffic/ sensor data to bypass security measures [35]. Adversarially strong ML models' improvement, leveraging methods like federated learning, adversarial training, and differential privacy, could raise IoT-driven AD systems' security.

5.1.5 SHORTAGE OF GENERALIZATION OVER IOT FIELDS

ML models trained on one IoT system (like smart homes) sometimes fail to generalize to other fields (like industrial IoT). Device heterogeneity, environmental variations, and various anomaly definitions make cross-field learning hard [36]. Transfer learning and field adaptation methods could aid in adapting pre-trained patterns to novel areas of IoT with minimal labeled data

5.2 FUTURE RESEARCH DIRECTIONS

Emerging trends and research directions below could aid in overcoming present issues and increase AD in IoT and WSN.

5.2.1 FEDERATED LEARNING FOR DECENTRALIZED ANOMALY DETECTION

Federated learning makes collaborative model training possible over shared IoT devices with no raw data distribution, considering privacy and scalability issues [37]. Investigators could find out federated deep AD architectures that let IoT devices learn from decentralized data while maintaining data privacy.

5.2.2 EXPLAINABLE AI (XAI) FOR ANOMALY DETECTION

Most DL models act as black boxes, making their decision interpretations hard. Explainability is critical for IoT security apps' trust [38]. A combination of SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-agnostic Explanations), and attention-driven algorithms could develop transparency in AD systems.

5.2.3 GRAPH NEURAL NETWORKS (GNN) FOR IOT NETWORK ANOMALY DETECTION

As IoT devices form interconnected networks, Graph Neural Networks (GNNs) could efficiently obtain complicated relations among devices and diagnose unusual communication models [39]. Enhancing **GNN-driven AD patterns** for large-scale IoT networks, like smart cities and industrial IoT, could considerably improve cybersecurity.

5.2.4 SELF-LEARNING AND ADAPTIVE ANOMALY DETECTION MODELS

IoT systems anomalies evolve because of shifts in cyber threats, device behavior, and environmental agents. Static ML models tackle adapting to these active shifts [40]. Performing online and continual learning, reinforcement learning-driven AD models could aid systems' adaptation to novel anomalies in real life.

5.2.5 BLOCKCHAIN-DRIVEN ANOMALY DETECTION FOR IOT SECURITY

Blockchain technology could raise security through presenting IoT transactions’ tamper-proof logging**,** decreasing false positives, and making safe AD possible [41]. Exploring blockchain-combined ML AD systems **to** secure IoT networks, particularly in smart grids and industrial IoT.

6. CONCLUSION

The present review examined different strategies of ML for AD in IoT and WSN, grouping them into hybrid**,** supervised, and unsupervised learning methods. When supervised models like Decision Trees and RF need labeled sets of data, unsupervised models such as Autoencoders and Isolation Forests could recognize anomalies with no previous info. Hybrid models leverage several ML methods’ strengths for developing diagnosis performance. Also, DL frameworks, such as Transformer-based models, LSTM, and CNN, have illustrated promising outcomes in getting complicated temporal and spatial dependencies in IoT data flows. Despite such developments, some issues persist, such as data scarcity, high-dimensional noisy data, imbalanced datasets, a shortage of cross-field generalization, real-life processing limitations, and adversarial attacks**.** Considering such concerns needs future research for concentrating on new solutions like self-learning adaptive models, federated learning, Explainable AI (XAI), blockchain-driven anomaly diagnosis, and Graph Neural Networks (GNNs)**.** Such developments would not only develop AD accuracy but also increase security, interpretability, and scalability of ML-based solutions in IoT and WSN. As IoT ecosystems are evolving, a combination of developed ML methods with real-life IoT applications will be crucial for enhancing security, optimizing resource management, and ensuring reliable system function. Future research must focus on improving privacy-maintaining, light, energy-efficient AD models to face the increasing IoT and WSN areas’ needs. Through considering such issues and leveraging present AI technologies, ML-based AD could have an important role in next-generation IoT infrastructures, security, and optimization

.

References

[1] B. R. Kikissagbe and M. Adda, "Machine learning-based intrusion detection methods in IoT systems: A comprehensive review," *Electronics*, vol. 13, no. 18, p. 3601, 2024.
[2] L. Zolfagharipour, M. H. Kadhim, and T. H. Mandeel, "Enhance the Security of Access to IoT-based Equipment in Fog," in *Proc. Al-Sadiq International Conference on Communication and Information Technology (AICCIT)*, pp. 142–146, 2023.
[3] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing Internet of Things using machine and deep learning methods: a survey," *Cluster Computing*, vol. 27, no. 7, pp. 9065–9089, 2024.
[4] A. Adewuyi, A. A. Oladele, P. U. Enyiorji, O. O. Ajayi, T. E. Tsambatare, K. Oloke, and I. Abijo, "The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems," WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS, vol. 23, no. 1, pp. 379–394, 2024.
[5] A. Q. Khan, S. El Jaouhari, N. Tamani, and L. Mroueh, "Knowledge-based anomaly detection: Survey, challenges, and future directions," *Engineering Applications of Artificial Intelligence*, vol. 136, p. 108996, Oct. 2024.
[6] Y. Wang, R. Guo, and P. Min, "A Survey of Applications for Anomaly Detection in the IoT: Methods, New Perspectives, and Future," in *Proc. IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2453–2460, 2024.
[7] S. Kumari, C. Prabha, A. Karim, M. M. Hassan, and S. Azam, "A Comprehensive Investigation of Anomaly Detection Methods in Deep Learning and Machine Learning: 2019–2023," *IET Information Security*, vol. 2024, no. 1, p. 8821891, 2024.
[8] N. R. Palakurti, "Challenges and future directions in anomaly detection," in *Practical Applications of Data Processing, Algorithms, and Modeling*, IGI Global, pp. 269–284, 2024.
[9] E. Krzysztoń, I. Rojek, and D. Mikołajewski, "A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study," *Applied Sciences*, vol. 14, no. 24, p. 11545, 2024.
[10] L. Zolfagharipour and M. H. Kadhim, "A Technique for Efficiently Controlling Centralized Data Congestion in Vehicular Ad Hoc Networks," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 12, no. 2, pp. 267–277, 2025.
[11] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports*, vol. 14, no. 1, p. 12077, 2024.
[12] Z. Wang, M. Ye, J. Cheng, C. Zhu, and Y. Wang, "An Anomaly Node Detection Method for Wireless Sensor Networks Based on Deep Metric Learning with Fusion of Spatial–Temporal Features," *Sensors*, vol. 25, no. 10, p. 3033, 2025.
[13] P. He, Y. Zhou, and X. Qin, "A survey on energy-aware security mechanisms for the internet of things," *Future Internet*, vol. 16, no. 4, p. 128, 2024.
[14] L. Yang and A. Shami, "IoT data analytics in dynamic environments: From an automated machine learning perspective," *Engineering Applications of Artificial Intelligence*, vol. 116, p. 105366, 2022.
[15] B. H. Aubaidan, R. A. Kadir, M. T. Lajb, M. Anwar, K. N. Qureshi, B. A. Taha, and K. Ghafoor, "A review of intelligent data analysis: Machine learning approaches for addressing class imbalance in healthcare—Challenges and perspectives," INTELLIGENT DATA ANALYSIS, vol. 2025, Feb. 26, Article ID 1088467X241305509, 2025.
[16] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet of Things*, vol. 19, p. 100568, 2022.
[17] S. F. Bedewy, "The Impact of Data Security and Privacy Concerns on the Implementation of Integrated *Smart Cities: Foundations and Perspectives*, vol. 59, 2024.
[18] N. H. Mahmood, D. H. Hussein, and S. Askar, "Machine Learning for Network Anomaly Detection: A Review," *The Indonesian Journal of Computer Science*, vol. 14, no. 1, 2025.
[19] G. Princz, M. Shaloo, and S. Erol, "Anomaly detection in binary time series data: An unsupervised machine learning approach for condition monitoring," *Procedia Computer Science*, vol. 232, pp. 1065–1078, 2024.
[20] G. Long and Z. Zhang, "PUNet: A Semi-Supervised Anomaly Detection Model for Network Anomaly Detection Based on Positive Unlabeled Data," *Computers, Materials & Continua*, vol. 81, no. 1, 2024.
[21] B. Konatham, T. Simra, F. Amsaad, M. I. Ibrahem, and N. Z. Jhanjhi, "A secure hybrid deep learning technique for anomaly detection in IIoT edge computing," *Authorea Preprints*, 2024.
[22] R. Bensaid, N. Labraoui, H. Saidi, and H. Bany Salameh, "Securing fog-assisted IoT smart homes: a federated learning-based intrusion detection approach," *Cluster Computing*, vol. 28, no. 1, pp. 1–9, 2025.
[23] S. A. Elsaid and A. Binbusayyis, "An optimized isolation forest-based intrusion detection system for heterogeneous and streaming data in the industrial Internet of Things (IIoT) networks," *Discover Applied Sciences*, vol. 6, no. 9, p. 483, 2024.
[24] Y. Li, N. Sui, A. Gehi, C. Guo, and Z. Guo, "CardiacRT-NN: Real-Time Detection of Cardiovascular Disease Using Self-attention CNN-LSTM for Embedded Systems," in *Proc. International Symposium on Neural Networks*, pp. 610–621, 2024.
[25] H. Niu, O. A. Omitaomu, M. A. Langston, S. K. Grady, M. Olama, O. Ozmen, H. B. Klasky, A. Laurio, M. Ward, and J. Nebeker, "Anomaly detection in electronic health records across hospital networks: Integrating machine learning with graph algorithms," IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, 2025.
[26] V.. Justus and G. R. Kanagachidambaresan, "Intelligent single-board computer for Industry 4.0: Efficient real-time monitoring system for anomaly detection in CNC machines," *Microprocessors and Microsystems*, vol. 93, p. 104629, 2022.
[27] M. R. Fachrezi, A. F. Ihsan, and W. Astuti, "Anomaly Detection Using LSTM-Based Deep Learning on Natural Gas Pipeline Operational Data," in *Proc. 12th International Conference on Information and Communication Technology (ICoICT)*, pp. 500–506, 2024.
[28] D. Dwivedi, A. Bhushan, and A. K. Singh, "85.35," in *Proc. 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)*, pp. 72–76, 2024.
[29] R. Shrestha, M. Mohammadi, S. Sinaei, A. Salcines, D. Pampliega, R. Clemente, and A. L. Sanz," JOURNAL OF PARALLEL AND DISTRIBUTED COMPUTING, vol. 193, Nov. 1, Art. no. 104951, 2024.
[30] H. C. Reis and V. Turk, "Detection of forest fire using deep convolutional neural networks with transfer learning approach," *Applied Soft Computing*, vol. 143, p. 110362, 2023.
[31] T. Nie, S. Wang, Y. Wang, X. Tong, and F. Sun, "An effective recognition of moving target seismic anomaly for security region based on deep bidirectional LSTM combined CNN," *Multimedia Tools and Applications*, vol. 83, no. 22, pp. 61645–61658, 2024.
[32] M. S. Habeeb and T. R. Babu, "Network intrusion detection system: a survey on artificial intelligence-based techniques," *Expert Systems*, vol. 39, no. 9, p. e13066, 2022.
[33] A. Momand, S. U. Jan, and N. Ramzan, "A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy," *Journal of Sensors*, vol. 2023, p. 6048087, 2023.

[34] H. Kayan, Y. Majib, W. Alsafery, M. Barhamgi, and C. Perera, "AnoML-IoT: An end-to-end re-configurable multi-protocol anomaly detection pipeline for Internet of Things," *Internet of Things*, vol. 16, p. 100437, 2021.

[35] P. Moriano, S. C. Hespeler, M. Li, and M. Mahbub, "Adaptive Anomaly Detection for Identifying Attacks in Cyber-Physical Systems: A Systematic Literature Review," *arXiv preprint* arXiv:2411.14278, 2024.

[36] **C. Zhou, X. Ge, Y. Chang, M. Wang, Z. Shi, M. Ji, T. Wu, C. Lv.** "A Multimodal Parallel Transformer Framework for Apple Disease Detection and Severity Classification with Lightweight Optimization," AGRONOMY, vol. 15, no. 5, p. 1246, 2025.

[37] M. A. Husnoo, A. Anwar, M. E. Haque, and A. N. Mahmood, "Decentralized Federated Anomaly Detection in Smart Grids: A P2P Gossip Approach," *arXiv preprint* arXiv:2407.15879, 2024.

[38] A. N. Gummadi, J. C. Napier, and M. Abdallah, "XAI-IoT: an explainable AI framework for enhancing anomaly detection in IoT systems," *IEEE Access*, 2024.

[39] H. Guo, Z. Zhou, D. Zhao, and W. Gaaloul, "EGNN: Energy-efficient anomaly detection for IoT multivariate time series data using graph neural network," *Future Generation Computer Systems*, vol. 151, pp. 45–56, 2024.

[40] R. Sathya, J. Agrawal, D. Roy, and R. Dutta, "A self-adaptive and self-learning methodology for wireless intrusion detection using deep neural network," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 6, pp. 2084–2094, 2021.

[41] M. I. Okfie and S. Mishra, "Anomaly Detection in IIoT Transactions using Machine Learning: A Lightweight Blockchain-based Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14645–14651, 2024.