International Journal of Information Technology and Management
Vol. 20, Issue No. 2, August-2025, ISSN 2249-4510

DOI: https://doi.org/10.29070/n3a0qx64

Check for updates

The Role of Artificial Intelligence in Enhancing Fault Tolerance Of Wireless Sensor Networks: A Systematic Review

Narendra Singh Dangi [1] * , Dr. Arpana Chaorasiya [2]

1. Research Scholar (Computer Science), Madhyanchal Professional University, Bhopal, M.P., India
narendra950653@gmail.com ,
2. Professor (Computer Science), Madhyanchal Professional University, Bhopal, M.P., India

Abstract: Wireless Sensor Networks (WSNs) have emerged as indispensable infrastructures across diverse applications, including healthcare, smart cities, industrial automation, and military surveillance. Despite their utility, WSNs remain highly vulnerable to faults at the node, network, data, and security levels. Such failures can degrade network reliability, reduce lifespan, and compromise decision-making. Traditional fault detection and diagnosis (FDD) methods—statistical analysis, threshold monitoring, and rule-based techniques—struggle to cope with the increasing complexity, heterogeneity, and scale of modern WSNs. This systematic review explores the role of Artificial Intelligence (AI) in enhancing the fault tolerance of WSNs. Drawing upon a comprehensive synthesis of prior work, the review categorizes AI-driven approaches into machine learning, deep learning, fuzzy logic, expert systems, and bio-inspired algorithms. We highlight their contributions, limitations, and integration potential within resource-constrained environments. Finally, the review identifies future research directions, including lightweight AI models, explainable AI, federated learning, and hybrid fault-tolerant frameworks.

Keywords: Wireless Sensor Networks, Fault Tolerance, Artificial Intelligence, Machine Learning, Deep Learning, Fault Detection and Diagnosis, Edge Computing

X

INTRODUCTION

Wireless Sensor Networks (WSNs) are distributed systems composed of autonomous sensor nodes designed to monitor, sense, and transmit environmental, physical, or industrial parameters to a central base station. These networks represent a vital technological pillar of the Internet of Things (IoT) ecosystem, enabling real-time monitoring and intelligent decision-making across diverse application domains. Examples include environmental surveillance (e.g., monitoring air or water quality), medical monitoring (e.g., patient health tracking), disaster management (e.g., forest fire or flood detection), industrial process automation, military reconnaissance, and predictive maintenance in smart infrastructures. Their widespread adoption underscores the importance of ensuring that WSNs remain reliable, efficient, and resilient despite harsh deployment environments and hardware constraints.

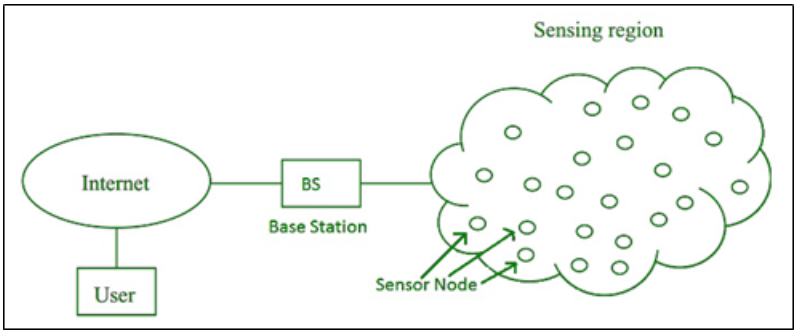

Figure 1 Wireless Sensor Network

However, WSNs are inherently vulnerable to a wide range of faults due to their distributed, resource-constrained, and often harsh operating conditions. Limitations in energy resources (battery depletion), environmental stresses (extreme temperatures, humidity, or physical damage), hardware/software failures, and cybersecurity threats contribute to frequent disruptions in network performance. These faults can lead to data loss, compromised accuracy, reduced network lifetime, and even catastrophic failures in mission-critical systems. Thus, fault tolerance—defined as the network's capacity to maintain performance and functionality despite the presence of faults—remains a foundational requirement for reliable WSN operation.

Traditional Fault Detection and Diagnosis (FDD) methods in WSNs, such as threshold monitoring, rule-based systems, and statistical analysis, have provided partial solutions. These methods are computationally lightweight and thus suitable for low-resource sensor nodes. However, their effectiveness diminishes in large-scale, heterogeneous, and dynamic WSN deployments. Static thresholds become outdated as environmental conditions shift, while rule-based models struggle with nonlinear or overlapping fault patterns. Moreover, these approaches often generate a high rate of false positives and negatives, reducing their reliability in real-world scenarios. Consequently, they are less capable of managing the complexity and unpredictability of next-generation WSNs, which demand adaptability and real-time responsiveness.

This limitation has paved the way for Artificial Intelligence (AI) as a transformative force in WSN fault tolerance. AI-driven models, powered by machine learning (ML), deep learning (DL), fuzzy systems, and bio-inspired algorithms, can learn from historical and real-time sensor data, detect subtle and complex fault patterns, and adaptively evolve to new conditions. Unlike static approaches, AI provides adaptive, predictive, and self-healing fault management systems. For instance, predictive analytics powered by AI can identify anomalies before they escalate into critical failures, reinforcement learning can dynamically reconfigure network routing to bypass faulty nodes, and deep learning can model spatial-temporal dependencies to enhance diagnosis accuracy.

Furthermore, the integration of AI with edge and fog computing frameworks allows for distributed intelligence in WSNs, reducing latency, conserving energy, and enabling real-time fault detection closer to the data source. Such advancements are particularly critical in time-sensitive and mission-critical applications, such as healthcare monitoring or battlefield surveillance, where even brief lapses in reliability can have severe consequences.

In summary, WSNs have become indispensable to modern intelligent systems, but their vulnerability to

diverse faults threatens their reliability. Conventional FDD techniques fall short in handling the complexity and scalability challenges of today's networks. AI, with its adaptability, predictive power, and self-learning capabilities, emerges as a cornerstone for enhancing WSN fault tolerance, ensuring that these networks remain robust, resilient, and capable of supporting the growing demands of IoT-driven environments.

FAULTS IN WIRELESS SENSOR NETWORKS

Faults in Wireless Sensor Networks (WSNs) occur at multiple levels—ranging from individual nodes to the communication infrastructure and even the data they generate. These faults directly threaten reliability, energy efficiency, and quality of service in WSN applications such as healthcare, environmental monitoring, and disaster management. Thus, robust Fault Detection and Diagnosis (FDD) is critical (Paradis & Han, 2007; Mahapatro & Khilar, 2013).

Node-Level Faults

Problems at the node level are among the most prevalent and serious types of failures in WSNs. When specific sensor nodes fail to function or stop working, it leads to these errors. Node failures can occur for a variety of reasons. First, most sensor nodes rely on non-rechargeable batteries for power, and when those run dry, the node will stop working permanently. Secondly, environmental stress, poor manufacture, or wear and tear can cause hardware failures such sensors, microcontrollers and or transceivers to malfunction. Third, software crashes resulting from bugs in firmware or corrupted updates can disrupt node functionality or cause data loss. Finally, environmental damage like physical impacts, extreme temperatures, dust, or water ingress can degrade or completely disable nodes (L. K. Wardhani 2022). Since each node plays a vital role in sensing and relaying data, any malfunction at the node level directly affects the quality and continuity of information transmitted to the base station. In large-scale WSN deployments, undetected node-level faults can multiply rapidly, reducing network efficiency and complicating fault localization. Thus, node-level fault management is a critical requirement for maintaining system integrity and data accuracy.

Network-Level Faults

Beyond individual node malfunctions, network-level faults affect the communication structure and overall data flow across the WSN. These faults often arise from disruptions in the communication infrastructure. Communication link failures, caused by physical obstructions, radio interference, or weather-related disturbances, can sever the connection between nodes, causing data to be lost or delayed. Routing failures may result from changes in network topology, such as mobile nodes or the death of key nodes, leading to incorrect or inefficient data routing (M. Vaqur 2022). Inconsistent or outdated routing tables can also misroute packets, increasing error rates. Another common issue is congestion and latency, which occurs when too many packets are transmitted simultaneously or when routing protocols are inefficient. This leads to data collisions, retransmissions, and excessive delays. Such errors can severely impair system performance in time-sensitive fields like emergency response or industrial automation. Network-level faults are often interlinked with node-level failures, creating cascading effects that complicate detection and recovery. As WSNs scale up, ensuring robust and fault-tolerant communication protocols becomes vital for

seamless and uninterrupted data transmission.

Data-Level Faults

Data-level faults in WSNs refer to errors or inconsistencies in the actual data sensed or transmitted by the network. These faults are particularly dangerous because they may not affect the functioning of the network directly but can mislead decision-making based on inaccurate information. A key issue is sensor calibration errors, where sensors drift from their correct measurement range over time, leading to inaccurate or unreliable readings. Another concern is redundant or missing data—a faulty sensor node may repeatedly send the same data or fail to send data altogether, causing gaps in the dataset or misleading redundancy. Outliers and noise, caused by environmental fluctuations, hardware instability, or electromagnetic interference, can introduce spurious values that distort the true data trends. Conventional threshold-based approaches may miss these outliers, leading to false alarms or important occurrences being unnoticed.[T. Zhang 2022]. Since many WSN applications involve automated systems that rely heavily on data accuracy, such faults can undermine the credibility and effectiveness of the entire system, especially in safety-critical sectors like healthcare or industrial monitoring.

Malicious Faults (Security-Related)

Security vulnerabilities and malicious actors are growing concerns in modern WSN deployments. Node capture attacks pose a significant threat to sensor networks that function in hazardous or dangerous environments because they enable bad actors to gain entry to nodes and modify their behavior. Additionally, they may try to fool the system into making a mistake or avoid discovery by injecting it with false data, a practice known as data injection. Another potential danger is Denial of Service (DoS) attacks, which are malicious cyberattacks that imitate legitimate network traffic in order to overwhelm nodes and make them unable to transfer valid data. These faults pose a distinct threat since typical defect diagnosis tools struggle to detect them. Traditional methods for WSN fault detection are inflexible and unable to adapt to new trends since they depend on predetermined criteria, thresholds, or routine inspections [D. Jana 2022]. The ever-changing structure of the network makes it possible that more subtle irregularities will go undetected. This provides solid evidence in favor of utilizing AI. Sensor networks that are wireless (WSNs) may analyze past data, identify patterns of defects, and react in real-time by applying models of machine learning and advanced learning. Effective and timely network maintenance can be facilitated by AI-based solutions that decrease the number of false positives & greatly enhance the precision of problem forecasts.

To find problems in WSNs, people typically utilize statistical models, compare thresholds, or do health checks periodically. However, these methods aren't adaptable enough to deal with dynamic network conditions and often fail to detect more subtle or complex fault patterns. [L. C. Brito 2022]. This is where the potential of AI really shines. Deep learning as well as machine learning can improve WSNs' ability to identify, forecast, and react to future failures by teaching them from their errors.

Implications

Across all categories, these faults collectively:

- Reduce data reliability, undermining analytics and decision-making.
- Increase energy consumption through retransmissions and redundant operations.
- Shorten network lifespan by exhausting critical nodes.
- Expose vulnerabilities that adversaries can exploit.

Hence, integrating robust fault detection and diagnosis mechanisms—increasingly AI-driven—is essential to sustain reliability and efficiency in next-generation WSNs.

ROLE OF ARTIFICIAL INTELLIGENCE IN FAULT TOLERANCE

Artificial Intelligence (AI) enhances fault tolerance in Wireless Sensor Networks (WSNs) through adaptive, data-driven capabilities that surpass traditional static methods. Below, we highlight the key contributions of AI in enabling robust, intelligent, and self-sustaining WSN operations—each supported by academic research.

Adaptability

AI models, such as neural nets and fuzzy logic systems, adapt to evolving fault patterns without manual threshold tuning. Elsharkawy et al. (2022) provide a taxonomy of AI-based fault-tolerance frameworks, including fuzzy and neural mechanisms that adapt dynamically.

Predictive Diagnosis

AI allows anticipating faults before they escalate. Luo & Nagarajan (2018) demonstrated autoencoder-based anomaly detection in WSNs that learns from historical and streaming data, achieving high accuracy and low false positives—proactively identifying anomalies in real time.

Reduced False Alarms via Contextual Awareness

By leveraging spatial and temporal correlations across sensor nodes, AI can distinguish between legitimate anomalies and environmental changes, substantially reducing false alarms. Self-healing networks, employing distributed intelligence and collaborative fault detection, achieve this contextual awareness (source: adaptive self-healing principles).

Self-Healing Mechanisms

AI-driven networks can autonomously reconfigure, reroute, or isolate failures. The ASAART protocol (Abba & Lee, 2015) exemplifies an adaptive, self-aware routing technique that recovers from node failures with improved packet delivery and energy efficiency.

Moreover, Miyaji & Omote (2015) present self-healing WSN designs capable of repairing compromised links over time without manual intervention, ensuring sustained network availability.

Table 1. Key AI Capabilities for Fault Tolerance in Wireless Sensor Networks

AI Capability	Description	Example Research
Adaptability	Learns and adjusts to evolving fault patterns autonomously	Survey of AI-based FT frameworks
Predictive Diagnosis	Early anomaly detection using historical and real-time data	Autoencoder-based anomaly detection
Reduced False Alarms	Context-aware detection using distributed intelligence	Self-healing sensor networks
Self-Healing	Autonomous diagnostics, rerouting, and network recovery	ASAART routing adaptation; self-healing schemes

AI TECHNIQUES FOR FAULT DIAGNOSIS IN WSNS

Artificial Intelligence (AI) has emerged as a powerful enabler of fault detection and diagnosis (FDD) in Wireless Sensor Networks (WSNs). Unlike traditional rule-based and statistical techniques, AI leverages data-driven learning to handle the complexity, heterogeneity, and scalability of WSNs. The following subsections outline the major AI approaches—machine learning (ML), deep learning (DL), expert systems, and bio-inspired algorithms—that enhance fault tolerance.

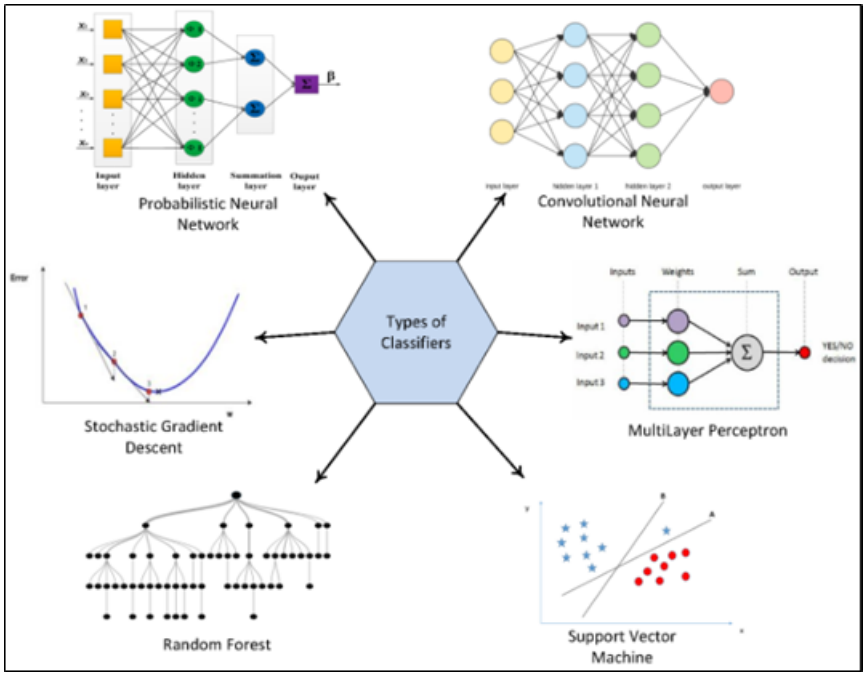

Figure 2 AI classification techniques for fault detection in WSNs

Machine Learning (ML)

Machine learning algorithms are widely adopted for fault diagnosis in WSNs due to their ability to learn patterns of normal and faulty behavior from historical and real-time data.

- **Supervised Learning:** Supervised ML relies on labeled datasets where sensor behaviors are pre-classified as normal or faulty. Algorithms such as Support Vector Machines (SVMs), Decision Trees (DTs), Random Forests (RFs), and Artificial Neural Networks (ANNs) have shown high accuracy in classifying faulty nodes. Zhang, Meratnia, & Havinga (2010) highlight that supervised models can effectively detect anomalies when labeled datasets are sufficiently large, but data labeling is often expensive and time-consuming. Similarly, Mahapatro & Khilar (2013) emphasize the effectiveness of supervised classifiers while noting their dependency on high-quality annotated data.
- **Unsupervised Learning:** When labeled data is unavailable, unsupervised clustering approaches like K-Means, DBSCAN, and Principal Component Analysis (PCA) are employed. These algorithms identify anomalies by detecting deviations from dominant cluster structures. Ayadi, Zidi, & Tabbane (2018) argue that unsupervised learning is particularly suited for large-scale WSNs deployed in dynamic environments, where continuous labeling is impractical.
- **Semi-Supervised Learning:** Semi-supervised techniques leverage a small set of labeled samples combined with abundant unlabeled data. Rassam, Maarof, & Zainal (2013) demonstrate that semi-supervised methods achieve a balance between supervised precision and unsupervised scalability, making them highly practical in resource-constrained networks.
- **Reinforcement Learning (RL):** Reinforcement learning treats sensor nodes as agents that learn optimal fault-handling strategies through interaction with the environment. RL-based approaches have been applied in fault recovery, energy-aware reconfiguration, and adaptive routing. Yuan et al. (2020) applied deep reinforcement learning (DRL) to optimize routing and recovery strategies, significantly enhancing fault tolerance and energy efficiency in IoT-driven WSNs.

Deep Learning (DL)

Deep Learning (DL) has gained traction in WSN fault diagnosis due to its superior ability to handle high-dimensional, spatio-temporal data.

- **Convolutional Neural Networks (CNNs):** CNNs are particularly suited for detecting spatial anomalies in WSNs, such as faulty patterns across sensor heatmaps or irregular data in geographic layouts. By automatically extracting hierarchical features, CNNs outperform traditional feature engineering approaches. Houssein et al. (2021) found CNN-based models to be effective in classifying sensor faults in IoT and WSN environments.
- **Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM):** RNNs and their advanced variant LSTMs are effective for analyzing temporal dependencies in sensor data streams. They can predict future failures by learning from historical patterns of degradation. Luo & Nagarajan (2018) demonstrated the use of autoencoder-RNN hybrids for anomaly detection, achieving higher accuracy in early fault prediction and reducing false alarms.

While DL approaches are powerful, they often require significant computational resources. Lightweight DL models and deployment at the edge or fog computing layers are increasingly being explored to mitigate these limitations.

Expert Systems

Expert systems use rule-based inference engines built on domain knowledge to detect faults. They are particularly effective in stable and controlled environments where fault types are well understood. Although transparent and interpretable, expert systems lack adaptability to unforeseen or evolving fault conditions (Paradis & Han, 2007).

Swarm Intelligence and Evolutionary Algorithms

Evolutionary algorithms attempt to simulate the processes of natural selection, mutation, and crossover; swarm intelligence takes its cues from the cooperative behavior of ant, bird, and bee colonies.(C. M. Furse 2021)

- **Particle Swarm Optimization (PSO)**: PSO is used for optimizing sensor placements, clustering, or identifying faulty nodes by simulating particles moving through a solution space. It finds the best configuration based on fitness functions, like energy efficiency or fault coverage.
- **Ant Colony Optimization (ACO)**: ACO mimics how ants find optimal paths. In WSNs, it is applied to routing algorithms and fault recovery, helping data packets avoid faulty nodes and reach their destination efficiently.
- **Genetic Algorithms (GA)**: GA is used to evolve fault detection rules or node deployment strategies over generations. It searches for optimal or near-optimal solutions in complex problem spaces and adapts over time.

These bio-inspired algorithms are especially valuable in large-scale WSNs due to their decentralized nature, scalability, and ability to find near-optimal solutions in dynamic environments [X. Xu 2022].

ADVANTAGES OF AI-DRIVEN FAULT DIAGNOSIS

The integration of Artificial Intelligence (AI) into Wireless Sensor Network (WSN) fault management offers several advantages over traditional statistical and rule-based methods.

- **Enhanced Detection Accuracy and Reduced False Positives:** AI models such as deep neural networks and ensemble learning methods have shown superior performance in anomaly detection by capturing complex non-linear fault patterns that conventional approaches often miss. They also reduce false alarms by distinguishing between true anomalies and environmental fluctuations (Houssein et al., 2021).
- **Scalability Across Large and Heterogeneous Networks:** AI approaches—particularly clustering and distributed learning—scale effectively in large WSN deployments, accommodating sensor heterogeneity and diverse data types. Semi-supervised and reinforcement learning frameworks adapt efficiently to varying network sizes (Ayadi, Zidi, & Tabbane, 2018).
- **Real-Time Adaptability to Dynamic Environments:** Reinforcement learning and adaptive neural

networks allow on-the-fly learning, enabling WSNs to self-adjust to changing conditions such as node mobility, energy variation, or environmental interference (Yuan et al., 2020).

- **Integration with Edge and Fog Computing:** Deploying AI models on edge and fog nodes reduces latency, minimizes energy consumption, and enables real-time diagnosis near the data source. This architecture prevents excessive reliance on cloud processing while maintaining accuracy (Elhoseny et al., 2019).
- **Potential for Hybrid Frameworks:** AI techniques can be integrated with traditional Fault Detection and Diagnosis (FDD) approaches, such as thresholding and statistical analysis. Hybrid systems enhance fault coverage, interpretability, and robustness, providing both adaptability and transparency (Mahapatro & Khilar, 2013).

CHALLENGES AND LIMITATIONS

Despite their promise, AI-driven fault diagnosis systems face several challenges in WSNs:

- **Resource Constraints:** Most WSN nodes operate with limited energy, processing, and memory capacity. Training or deploying complex deep learning models directly on nodes is often infeasible, necessitating lightweight or distributed solutions (Xu et al., 2020).
- **Data Limitations:** Supervised learning approaches rely on large labeled datasets, which are scarce in real-world WSNs. Moreover, class imbalance—with far fewer faulty samples compared to normal data—affects classifier performance (Rassam, Maarof, & Zainal, 2013).
- **Explainability**: Many AI models, particularly deep neural networks, are criticized as "black-box" systems. In safety-critical applications such as healthcare or industrial monitoring, lack of transparency undermines trust and hinders adoption (Gunning & Aha, 2019).
- **Integration Issues:** Integrating AI frameworks into existing WSN architectures requires hybridization and careful design. Without lightweight frameworks and interoperability standards, deployment may be impractical for resource-constrained networks (Elsharkawy et al., 2022).

FUTURE DIRECTIONS

Research trends suggest several promising directions for advancing AI-driven fault diagnosis in WSNs:

- **Development of Lightweight AI Models:** Designing energy-efficient models tailored for sensor nodes (e.g., quantized neural networks, TinyML) can address hardware constraints and extend network lifetime (Zhang et al., 2021).
- **Explainable AI (XAI):** Developing interpretable AI frameworks will allow human operators to understand and trust diagnostic outcomes, especially in critical environments like healthcare and military monitoring (Gunning & Aha, 2019).
- **Federated and Distributed Learning:** Federated learning enables decentralized training without raw data transfer, preserving privacy and reducing communication overhead—an attractive approach for WSN fault tolerance (Kairouz et al., 2021).
- **Real-World Testing and Validation:** While many AI approaches are tested in simulations, real-world deployments are necessary to validate robustness under environmental noise, adversarial threats, and hardware variability (Mahapatro & Khilar, 2013).

- **Hybrid AI-Traditional Approaches:** Combining statistical thresholding, rule-based logic, and AI-based learning offers a balance of efficiency, accuracy, and interpretability. Hybrid systems represent a practical step toward resilient WSN fault management (Paradis & Han, 2007).

CONCLUSION

Artificial Intelligence has emerged as a transformative solution to enhance fault tolerance in Wireless Sensor Networks (WSNs). By leveraging machine learning, deep learning, expert systems, and bio-inspired algorithms, AI enables adaptive, predictive, and self-healing fault management that surpasses the limitations of conventional approaches. These techniques improve detection accuracy, reduce false alarms, and provide scalability across heterogeneous and dynamic networks. Moreover, integration with edge and fog computing further strengthens real-time adaptability and energy efficiency. However, challenges such as resource constraints, scarcity of labeled datasets, and the lack of model explainability persist, necessitating lightweight, interpretable, and hybrid AI frameworks. Future advancements in Explainable AI, federated learning, and real-world validation will be critical to ensure reliability and trustworthiness. Ultimately, AI-driven fault tolerance will play a decisive role in building resilient, sustainable, and intelligent WSNs for diverse IoT applications.

References

1. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. Artificial Intelligence Review, 58(9). https://doi.org/10.1007/s10462-025-11292-w

2. Al-Dunainawi, Y., Al-Kaseem, B. R., & Al-Raweshidy, H. S. (2023). Optimized artificial intelligence model for DDoS detection in SDN environment. IEEE Access, 11, 106733–106748. https://doi.org/10.1109/ACCESS.2023.3319214

3. Zaman, S., et al. (2021). Security threats and artificial intelligence based countermeasures for Internet of Things networks: A comprehensive survey. IEEE Access, 9, 94668–94690. https://doi.org/10.1109/ACCESS.2021.3089681

4. Myakala, P. K., Bura, C., & Jonnalagadda, A. K. (2025). Artificial immune systems: A bio-inspired paradigm for computational intelligence. Journal of Artificial Intelligence and Big Data, 5(1), 1–13. https://doi.org/10.31586/jaibd.2025.1233

5. Kapu, V. K., & Karri, G. R. (2023). Efficient detection and mitigation of rushing attacks in VANETs using RAID: A novel intrusion detection system. Journal of Computer Science, 19(9), 1143–1159. https://doi.org/10.3844/jcssp.2023.1143.1159

6. Ebong, O., Edet, A., Uwah, A., & Udoetor, N. (2024). Comprehensive impact assessment of intrusion detection and mitigation strategies using support vector machine classification. Research Journal of Pure Science and Technology E, 7(2), 50–69. https://doi.org/10.56201/rjpst.v7.no2.2024.pg50.69

7. Liu, H., et al. (2024). Stacked intelligent metasurfaces for wireless sensing and communication:

Applications and challenges. IEEE Microwave Magazine, 1–8. https://doi.org/10.1109/MWC.001.2500002

8. Zhang, J., Zhang, K., An, Y., Luo, H., & Yin, S. (2024). An integrated multitasking intelligent bearing fault diagnosis scheme based on representation learning under imbalanced sample condition. IEEE Transactions on Neural Networks and Learning Systems, 35(5), 6231–6242. https://doi.org/10.1109/TNNLS.2022.3232147

9. Wang, C., Tang, N., Zhang, Q., Gao, L., Yin, H., & Peng, H. (2024). Expert experience and data-driven based hybrid fault diagnosis for high-speed wire rod finishing mills. Computational Modeling in Engineering & Sciences, 138(2), 1827–1847. https://doi.org/10.32604/cmes.2023.030970

10. Asutkar, S., & Tallur, S. (2023). Deep transfer learning strategy for efficient domain generalisation in machine fault diagnosis. Scientific Reports, 13(1), 1–9. https://doi.org/10.1038/s41598-023-33887-5

11. Jihani, N., Kabbaj, M. N., & Benbrahim, M. (2023). Sensor fault detection and isolation for smart irrigation wireless sensor network based on parity space. International Journal of Electrical and Computer Engineering, 13(2), 1463–1471. https://doi.org/10.11591/ijece.v13i2.pp1463-1471

12. Wardhani, L. K., Febriyanto, R. A., & Anggraini, N. (2022). Fault detection in wireless sensor networks data using random under sampling and extra-tree algorithm. 2022 10th International Conference on Cyber IT Services and Management (CITSM), 9935888. https://doi.org/10.1109/CITSM56380.2022.9935888

13. Vaqur, M., Rastogi, R., Chaudhary, P., Joshi, K., Bhagat, V. K., & Memoria, M. (2022). A review of fault detection and diagnosis protocols for WSNs. 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 879–883. https://doi.org/10.1109/COM-IT-CON54601.2022.9850600

14. Zhang, T., et al. (2022). Intelligent fault diagnosis of machines with small & imbalanced data: A state-of-the-art review and possible extensions. ISA Transactions, 119, 152–171. https://doi.org/10.1016/j.isatra.2021.02.042

15. Jana, D., Patil, J., Herkal, S., Nagarajaiah, S., & Duenas-Osorio, L. (2022). CNN and Convolutional Autoencoder (CAE) based real-time sensor fault detection, localization, and correction. Mechanical Systems and Signal Processing, 169, 108723. https://doi.org/10.1016/j.ymssp.2021.108723