Smart City Insights

www.sci.reapress.com

Smart City Ins. Vol. 2, No. 2 (2025) 109–118.

Paper Type: Original Article

An AI-Driven Adaptive Security Framework for Wireless Sensor Networks in Smart City Environments

Zeynab Parandavar[1,*], Javad Pourqasem[2]

[1] Department of Computer Engineering, Ayandegan Institute of Higher Education, Tonekabon, Iran; z.parand.1997@gmail.com.
[2] Department of Computer Engineering, Urmia University, 5756151818 Urmia, Iran; jpourmail@gmail.com.

Citation:

Received: 26 October 2024 *Revised: 24 December 2024* *Accepted: 12 February 2025*	Parandavar, Z., & Pourqasem, J. (2025). An AI-driven adaptive security framework for wireless sensor networks in smart city environments. *Smart City Insights, 2*(2), 109-118.

Abstract

As smart cities evolve, Wireless Sensor Networks (WSNs) are crucial in real-time data collection and monitoring. However, cyber-attacks increasingly target these networks, necessitating advanced security solutions. AI-powered security protocols offer a promising approach, using Machine Learning (ML) to detect and respond to threats in real time. This paper explores the application of AI-driven security mechanisms within smart city WSNs, including intrusion detection, anomaly detection, and automated response protocols. Simulations indicate that AI-based security models significantly enhance network resilience, reduce attack response time, and improve data integrity, making them ideal for future smart city deployments.

Keywords: AI-powered security, Smart city, Wireless sensor networks, Machine learning, Intrusion detection.

1 | Introduction

Smart cities represent an evolution in urban planning, incorporating interconnected networks of sensors, devices, and applications to improve city operations' efficiency and enhance residents' quality of life. Wireless Sensor Networks (WSNs) are fundamental components of this infrastructure, gathering and transmitting data about traffic, air quality, lighting, water systems, and more. However, as reliance on these networks grows, so does their vulnerability to cyber threats. As smart cities continue to expand, it is critical to ensure the security of these networks to maintain public trust and safeguard vital data [1].

The traditional approach to securing WSNs relies heavily on predefined security measures such as firewalls, encryption, and manual monitoring. Still, these solutions often fall short when faced with modern cyber threats that are increasingly adaptive and complex. Artificial Intelligence (AI)-powered security protocols offer a dynamic and intelligent solution to these challenges, with Machine Learning (ML) algorithms capable of

Corresponding Author: z.parand.1997@gmail.com
https://doi.org/10.22105/sci.v2i2.39

analyzing patterns, identifying anomalies, and responding to potential threats in real time [2]. In this discussion, we will explore the role of AI in enhancing the security of WSNs within smart cities, focusing on the advantages, challenges, and future potential of AI-driven security measures [3].

2 | The Role of AI in WSN Security

2.1 | Introduction to WSNs and Security Challenges

WSNs are foundational in the architecture of smart cities, forming the backbone of numerous critical applications, such as environmental monitoring, traffic management, public safety, and utilities. WSNs comprise numerous sensor nodes that gather, process, and communicate data within the network to provide real-time information. However, integrating WSNs within city infrastructures introduces significant security risks, given that the data they collect and transmit can be sensitive and critical to operations [4].

One of the main challenges is that WSNs are highly vulnerable to cyber threats due to several factors, including limited computational resources, low power requirements, and reliance on wireless communication channels. These factors make WSNs susceptible to attacks such as eavesdropping, data tampering, Denial of Service (DoS), and node compromise, which could lead to unauthorized access or disruption of services.

AI technologies have been increasingly employed in WSN security to address these issues and enhance detection, prevention, and response capabilities. AI-driven security solutions bring adaptive and autonomous mechanisms significantly strengthening WSN resilience against cyber threats [5–7].

2.2 | How AI Transforms WSN Security

AI is pivotal in improving WSN security by enabling networks to detect and respond to cyber threats in real time. The key ways in which AI enhances WSN security include:

I. Anomaly detection and threat prediction: AI algorithms can learn and model typical WSN behaviors, allowing them to detect anomalies that indicate potential security breaches. ML techniques, such as clustering, classification, and pattern recognition, are applied to analyze network data and identify deviations from normal behavior patterns. When an anomaly is detected, AI algorithms trigger alerts or initiate automated responses to mitigate potential threats before they escalate [6–8].

II. Real-time data processing: WSNs generate vast amounts of data, particularly in urban environments where hundreds or thousands of nodes may be active simultaneously. AI's ability to process and analyze this data in real time enables a proactive approach to security. AI models can sift through data streams from various sensor nodes, identify signs of malicious activity, and alert security protocols without human intervention. This automation reduces response time, critical in mitigating cyber threats in dynamic urban environments [9], [10].

III. Decentralized and autonomous decision-making: AI's most significant advantage to WSN security is its capacity to facilitate decentralized security mechanisms. Traditional security solutions often rely on centralized systems for monitoring and responding to threats, which can be impractical in large-scale WSNs due to latency and bottleneck issues. By contrast, AI-driven WSNs can operate autonomously, with nodes capable of independent threat assessment and response based on localized data and decision-making algorithms. It minimizes dependency on central servers and enhances the network's overall resilience [6], [11].

IV. Dynamic adaptation to evolving threats: cyber threats targeting WSNs continually evolve, with attackers employing increasingly sophisticated techniques. AI solutions can adapt to these emerging threats by learning from new data and updating security protocols. Through Reinforcement Learning (RL) and other adaptive algorithms, AI-based systems can adjust to new types of attacks, making them particularly valuable in environments like smart cities, where a variety of threats could arise due to the diverse applications of WSNs [12], [13].

2.3 | Key AI Techniques Used in WSN Security

Several AI techniques are commonly used to strengthen WSN security. These include:

2.3.1 | Machine learning

I. Supervised learning: ML models are trained on labeled datasets to recognize specific types of attacks. In WSN security, supervised learning algorithms can help identify known patterns of attacks, such as spoofing or DoS, based on historical data.

II. Unsupervised learning: in cases where labeled data is unavailable, unsupervised learning can detect anomalies by grouping data into clusters and identifying deviations. It is especially helpful in recognizing previously unknown attacks.

III. Reinforcement learning: this technique allows WSN nodes to optimize their security responses over time. By rewarding certain actions and penalizing others, RL enables WSNs to learn effective [6] defense mechanisms in dynamic environments [7], [8].

2.3.2 | Deep learning

Deep learning algorithms, particularly neural networks, have shown great promise in identifying complex and subtle patterns in WSN data. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are used for tasks such as intrusion detection, where they analyze data across time sequences to detect suspicious activity.

2.3.3 | Natural language processing

Natural Language Processing (NLP) algorithms can process text-based logs and reports generated by WSNs to identify potential threats in specific scenarios. NLP techniques can assist in analyzing system alerts or commands within smart city applications to detect unusual patterns that may signal security issues.

2.3.4 | Fuzzy logic

Fuzzy logic helps manage the inherent uncertainty in WSN environments. By allowing the system to make decisions even with imprecise or incomplete data, fuzzy logic can enhance WSN security, especially in complex situations where binary decision-making is inadequate.

2.3.5 | Game theory

Game theory models the interactions between attackers and defenders as strategic games, helping predict potential attackers' moves. This approach enables AI-driven security protocols to develop adaptive defense strategies that account for the dynamic nature of cyber threats.

3 | Literature Review

AI has proven to be a powerful tool in securing digital and physical networks across various sectors, including the Internet of Things (IoT), healthcare, finance, and, more recently, critical infrastructure systems like smart city WSNs. As these sectors expand their use of interconnected networks, they increasingly rely on AI-driven security solutions to combat sophisticated cyber threats [14], [15].

3.1 | AI in IoT Security

The IoT ecosystem, consisting of devices interconnected through the internet, has brought convenience and heightened security risks. IoT devices are typically constrained by low power and processing capabilities, making them vulnerable to attacks such as DoS, malware, and eavesdropping. AI-based solutions, particularly ML and deep learning, are commonly applied in IoT security to improve Intrusion Detection Systems (IDS) by learning from vast amounts of data and identifying malicious patterns. For instance, deep learning models such as CNNs can analyze data across different time frames to detect suspicious activities or malware

intrusions within IoT networks. RL has also proven effective in allowing IoT networks to adapt dynamically to changing threats by continuously optimizing security responses based on the environment and detected anomalies [16–18].

3.2 | AI in Healthcare Security

Healthcare systems generate and store extensive amounts of sensitive data, including patient health records, making them prime targets for cyberattacks. Protecting this information is critical, as data breaches can result in financial losses and damage patient privacy and trust. AI has been widely implemented in healthcare security to improve data privacy, detect unauthorized access, and protect critical medical systems from disruption. Techniques such as decision trees and deep learning models are used to classify normal and abnormal network behavior, helping to identify insider threats and block attempts to access patient information without proper authorization. NLP algorithms have also been employed to analyze textual data in health records, flagging potential risks in real time [19–21].

3.3 | AI in Financial Network Security

The financial sector is highly susceptible to cyber threats due to the high value of the data handled, including bank transactions, customer information, and payment records. AI-driven financial security solutions commonly use supervised and RL models to detect and prevent fraudulent activities. For example, decision trees are often used in fraud detection to identify patterns that indicate potential fraudulent transactions. RL enables banks to continuously adapt to new fraud patterns by analyzing real-time transaction data and improving detection algorithms. The predictive capabilities of AI are invaluable for identifying fraud risks and potential security breaches, allowing financial institutions to respond swiftly [14].

4 | Challenges in Implementing AI Security in WSNs

While AI-powered security protocols offer promising advancements for protecting WSNs, implementing these solutions in resource-constrained environments comes with challenges. Several factors complicate the effective use of AI for WSN security, from data privacy issues to computational requirements and operational hurdles. Here, we explore these primary challenges in more detail [17], [22].

4.1 | Data Privacy

AI algorithms often require substantial data to train and perform accurately, which introduces significant privacy and compliance concerns, particularly in WSNs deployed for smart city applications. These networks collect extensive, often sensitive data from various sources, such as environmental sensors, traffic monitors, and public safety devices. This data can contain personal information or other sensitive insights, especially in applications that involve citizen monitoring or infrastructure security. Handling and processing such data must comply with data protection regulations, including the General Data Protection Regulation (GDPR) and other local privacy laws.

Since AI models generally improve with access to larger datasets, achieving high accuracy without compromising privacy can be difficult. Techniques like federated learning, which enable model training without direct data sharing, have been explored as a potential solution. However, federated learning introduces its complexities and computational overhead, making it challenging for WSNs with limited processing capabilities. Ensuring data privacy while providing adequate data for AI models is a delicate balance that remains a significant obstacle in deploying AI security for WSNs [23], [24].

4.2 | Computational Load

WSN nodes are generally designed to be low-power and cost-effective, with limited processing capabilities. In contrast, AI algorithms, especially deep learning models, require significant computational resources to perform data processing, anomaly detection, and pattern recognition. The computational load associated with

these algorithms can strain WSN nodes, resulting in reduced efficiency, increased energy consumption, and shortened node lifespan.

The need for real-time processing, essential for prompt threat detection and response, compounds this computational challenge. Given the limited memory, storage, and processing power in WSN nodes, running complex AI algorithms may necessitate additional hardware or alternative methods like edge computing, where AI tasks are distributed across multiple nodes or offloaded to more powerful edge devices. However, such solutions can be costly and may introduce new vulnerabilities or latency issues, undermining the primary goals of WSN security [17].

4.3 | False Positives

Another significant challenge in implementing AI-based security for WSNs is managing false positives. False positives occur when the AI system incorrectly flags normal behavior as suspicious, which can lead to unnecessary alerts and trigger unwarranted security responses. In a WSN, high rates of false positives can result in resource wastage, as the network responds to non-existent threats by reallocating bandwidth, processing power, and energy to manage these "Threats." This hampers network efficiency and can lead to fatigue in monitoring and response systems, causing actual threats to be overlooked.

High false positive rates are common in anomaly detection algorithms, where distinguishing between harmless anomalies and actual threats can be difficult. Training AI models to improve accuracy without compromising sensitivity requires a delicate balance and often extensive fine-tuning of parameters. Additionally, techniques such as ensemble learning, where multiple models are combined to improve predictive accuracy, are sometimes applied to reduce false positives. However, this adds further computational overhead, making deploying in resource-limited WSN environments challenging [25].

4.4 | Limited Communication Bandwidth

WSNs typically rely on low-bandwidth communication channels to conserve energy and cost. However, AI-driven security solutions require substantial amounts of data to be transmitted, particularly when data is shared across nodes for collaborative learning or when information is sent to centralized servers for analysis. Limited bandwidth can bottleneck the communication required for AI models, delaying threat detection and response, which could compromise the overall effectiveness of WSN security.

One approach to this challenge is compressing data or using lightweight models specifically optimized for WSNs. However, these solutions often come at the cost of reduced model accuracy or increased complexity in data pre-processing. Striking a balance between model performance and communication efficiency remains a pressing challenge.

4.5 | Energy Consumption

AI algorithms generally require continuous data processing, which leads to increased energy consumption that poses another challenge for WSNs that rely on battery-powered nodes. Prolonged or intensive use of AI-driven security measures can quickly deplete node batteries, reducing network lifespan and increasing the maintenance costs associated with node replacement.

Researchers have explored low-power AI algorithms and energy-efficient hardware to mitigate this issue. However, these options may still fall short in large-scale WSNs, where individual nodes must operate for extended periods with minimal human intervention. Energy-efficient AI models that balance performance with power constraints are crucial for sustainable WSN security, though they remain an area of ongoing research [25].

5 | Limitations of AI-Powered Security in Smart City WSNs

While AI significantly enhances security in WSNs, several limitations impact its effectiveness and practicality. The key challenges are data biases, algorithmic complexity, and difficulties adapting to evolving threats. These limitations underscore the need for continuous improvements and innovative approaches to refine AI-driven security protocols in WSN applications [26].

5.1 | Data Biases

AI models rely on training data to identify patterns, detect anomalies, and respond to potential threats. However, the quality of these models is directly tied to the data on which they are trained. In WSN applications, biased or incomplete datasets can skew AI algorithms, leading to inaccurate threat detection. For instance, if the training data lacks examples of certain types of attacks, the AI system might fail to recognize similar threats in real-world scenarios. Data biases can also cause the AI model to exhibit false positives or negatives, leading to unnecessary alerts or missed threats. It is particularly concerning in smart city applications, where an oversight can compromise critical public services.

Addressing data biases in WSN security applications requires a robust dataset that captures a wide range of potential threats and normal network behaviors. However, collecting diverse data samples from real-world WSNs poses challenges, especially given the resource limitations of sensor nodes. Techniques like data augmentation and synthetic data generation are being explored to counter data biases, though they are still evolving and may not fully replicate real-world conditions.

5.2 | Algorithmic Complexity

The computational demands of AI algorithms, particularly deep learning and complex ML models, can be excessive for the resource-constrained nodes in WSNs. Advanced AI techniques often involve large numbers of parameters and extensive computation, which require substantial processing power, memory, and energy resources—constraints that are difficult to meet in typical WSN environments. This complexity can lead to inefficient models that strain the network, reduce node lifespan, and increase maintenance needs, making such models less feasible for large-scale WSN deployment.

Researchers have explored lightweight AI models, such as shallow neural networks, rule-based systems, and simplified decision trees, to address this issue. However, while these methods reduce computational demand, they may not provide the same accuracy and adaptability as more complex algorithms. Finding a balance between model complexity and efficiency is a key area of ongoing research in WSN security [27].

5.3 | Challenges in Adapting to New Threats

WSNs in smart cities are increasingly exposed to various evolving and sophisticated cyber threats. AI models trained on historical data may not be equipped to recognize or respond effectively to new, previously unseen attack types. For example, if a model is trained to detect only specific DoS attack patterns, it might fail to identify a modified or novel DoS attack variant. The static nature of many AI models, especially those that don't continuously learn from new data, limits their effectiveness in a dynamic threat landscape.

Techniques such as RL and continuous learning are being investigated to help AI models adapt to evolving threats by updating themselves based on new data. However, these methods have challenges, as continuous learning can increase computational demands and introduce new vulnerabilities. Implementing adaptive learning to balance responsiveness with resource constraints remains an area of active exploration in WSN security [28].

6 | Proposed Improvements

Optimizing AI-driven security protocols for WSNs involves addressing challenges like data privacy, computational load, and adaptability to evolving threats. By implementing specific improvements, including

enhanced privacy measures, lightweight AI models, and advanced threat intelligence capabilities, WSNs can achieve more effective, secure, and efficient operations, particularly in resource-constrained environments like smart cities [29].

6.1 | Enhanced Privacy Measures

Data privacy is a primary concern in AI-powered security for WSNs, especially in applications handling sensitive or Personally Identifiable Information (PII). Integrating privacy-preserving techniques, such as data anonymization and encryption, can help mitigate these risks.

Data anonymization involves removing or masking identifiable information in the data used to train AI models. By anonymizing data at the source, AI algorithms can still detect patterns and analyze security threats without exposing personal information, thus ensuring user privacy while supporting effective security measures.

Encryption: encrypting data in transit and at rest within WSNs can prevent unauthorized access and protect data integrity. AI algorithms designed to work within an encrypted environment, such as Secure Multi-Party Computation (SMPC) protocols, allow for computations on encrypted data without revealing the underlying information. This approach safeguards data and helps comply with data protection regulations like GDPR.

Implementing these privacy-enhancing techniques allows WSNs to utilize AI for security without compromising sensitive information, making them more viable for public and urban infrastructure applications [30].

6.2 | Lightweight AI Models

Since WSN nodes are typically resource-constrained, lightweight AI models are essential to reduce computational strain and conserve energy. These models are optimized to perform security functions with minimal processing power, memory, and energy, making them feasible for deployment across large-scale networks.

Simplified model architectures: shallow neural networks, decision trees, and rule-based systems provide effective security features while requiring less computational power. These models can still perform essential functions like anomaly detection, but are optimized for low-power devices in WSNs.

Edge computing integration: offloading complex computations to edge devices or nearby servers alleviates the strain on individual WSN nodes. This way, WSN nodes only transmit essential data to edge devices, where more complex AI algorithms process and analyze it. This distributed approach minimizes the computational burden on each node while preserving real-time threat detection and response capabilities.

Model compression and pruning: techniques such as model pruning, which removes redundant parameters, and quantization, which reduces precision, can help optimize AI models for WSN use. These strategies allow for more efficient use of node resources without significantly reducing model accuracy, ensuring that security measures are maintained without overloading the network [31].

By developing lightweight AI models, WSNs can efficiently support AI-driven security protocols, reducing computational load while maintaining high-security levels [27].

6.3 | Improved Threat Intelligence through RL

In a dynamic threat landscape, RL enables WSNs to adapt autonomously to new and evolving security threats. Unlike static models that rely on predefined patterns, RL allows networks to learn from interactions and optimize their responses over time.

Adaptive security response: RL-based algorithms allow WSNs to assess real-time network conditions and autonomously determine the optimal response to detected threats. For instance, in the case of a detected intrusion, RL enables the network to decide whether to isolate affected nodes, reroute data, or trigger an alert

based on past experiences and learned behavior. This adaptability significantly improves WSN's resilience against emerging threats.

Self-learning capabilities: RL algorithms can be designed to update themselves based on new data and threat patterns. By continuously analyzing data, the WSN gains the ability to detect novel threats and adapt its response accordingly. This self-learning capability is particularly valuable in smart cities, where threats evolve and vary due to the diverse applications of WSNs.

Resource-aware optimization: RL can optimize resource allocation within the network, allowing WSNs to balance security needs with resource constraints. For example, RL can help determine when to conserve energy by minimizing low-priority security checks and focusing on high-risk scenarios. This dynamic approach preserves WSN functionality and extends network life while maintaining strong security [28].

RL thus empowers WSNs to autonomously and effectively counter new threats, enabling a robust and adaptive security framework suitable for complex environments.

7 | Conclusion

AI-powered security protocols offer a groundbreaking solution for securing WSNs in smart cities. They significantly improve resilience against cyber threats and enable real-time threat detection and response. By leveraging AI techniques such as ML and RL, WSNs can autonomously detect anomalies, respond promptly, and adapt to evolving threats, addressing critical security needs in complex urban environments.

This study underscores the effectiveness of AI-driven security in addressing prevalent security challenges, including data privacy, computational limitations, and adaptive threat responses. Proposed improvements, such as enhanced privacy measures, lightweight AI models, and advanced threat intelligence, can further optimize AI-powered protocols for resource-constrained WSN environments, making them more efficient and sustainable.

As smart cities continue to expand, AI's role in network security will become increasingly vital, supporting the safe and reliable operation of essential urban services. With continued research and development, AI-driven security for WSNs holds immense potential to shape the future of urban infrastructure security, creating safer, more resilient cities in the face of emerging digital threats.

Funding

This research received no external funding.

Data Availability

Data supporting the findings can be made available upon request from the corresponding author.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Sharma, H., Haque, A., & Blaabjerg, F. (2021). Machine learning in wireless sensor networks for smart cities: A survey. *Electronics*, *10*(9), 1012. https://doi.org/10.3390/electronics10091012

[2] Koufoudakis, G., Oikonomou, K., Giannakis, K., & Aïssa, S. (2018). Probabilistic flooding coverage analysis for efficient information dissemination in wireless networks. *Computer networks*, *140*, 51–61. https://doi.org/10.1016/j.comnet.2018.05.005

[3] Jurado-Lasso, F. F., Marchegiani, L., Jurado, J. F., Abu-Mahfouz, A. M., & Fafoutis, X. (2022). A survey on machine learning software-defined wireless sensor networks (ml-SDWSNS): Current status and major challenges. *IEEE access*, *10*, 23560–23592. https://doi.org/10.1109/ACCESS.2022.3153521

[4] Moslehi, M. M. (2025). Exploring coverage and security challenges in wireless sensor networks: A survey. *Computer networks*, *260*, 111096. https://doi.org/10.1016/j.comnet.2025.111096

[5] Wang, S., Jiang, H., Qiao, Y., Jiang, S., Lin, H., & Sun, Q. (2022). The research progress of vision-based artificial intelligence in smart pig farming. *Sensors*, *22*(17), 6541. https://doi.org/10.3390/s22176541

[6] Delwar, T. S., Aras, U., Mukhopadhyay, S., Kumar, A., Kshirsagar, U., Lee, Y., … & Ryu, J. Y. (2024). The intersection of machine learning and wireless sensor network security for cyber-attack detection: A detailed analysis. *Sensors*, *24*(19), 6377. https://doi.org/10.3390/s24196377

[7] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors*, *22*(13), 4730. https://doi.org/10.3390/s22134730

[8] Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. *Journal of big data*, *11*(1), 16. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-023-00870-w

[9] Hu, L., Han, C., Wang, X., Zhu, H., & Ouyang, J. (2024). Security enhancement for deep reinforcement learning-based strategy in energy-efficient wireless sensor networks. *Sensors*, *24*(6), 1993. https://doi.org/10.3390/s24061993

[10] Satori, H. (2024). Machine learning attack detection based-on stochastic classifier methods for enhancing of routing security in wireless sensor networks. *Ad hoc networks*, *163*, 103581. https://doi.org/10.1016/j.adhoc.2024.103581

[11] Luo, T., & Nagarajan, S. G. (2018). Distributed anomaly detection using autoencoder neural networks in wsn for IoT. *2018 IEEE international conference on communications (ICC)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICC.2018.8422402

[12] Talukder, M. A., Khalid, M., & Sultana, N. (2025). A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. *Scientific reports*, *15*(1), 4617. https://www.nature.com/articles/s41598-025-87028-1

[13] Gueriani, A., Kheddar, H., & Mazari, A. C. (2023). Deep reinforcement learning for intrusion detection in IoT: A survey. *2023 2nd international conference on electronics, energy and measurement (IC2EM)* (Vol. 1, pp. 1–7). IEEE. https://doi.org/10.1109/IC2EM59347.2023.10419560

[14] Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and information management*, *8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

[15] Malibari, A. A., Nour, M. K., Al-Wesabi, F. N., Alabdan, R., Mohamed, A., Al Duhayyim, M., … & Gupta, D. (2023). Metaheuristics with deep learning enabled epileptic seizure classification for smart healthcare on cyborg robots. *Human-centric computing and information sciences*, *13*(39), 1–17. https://doi.org/10.22967/HCIS.2023.13.039

[16] Srinivasan, N. (2024). Artificial intelligence in IoT security: Review of advancements, challenges, and future directions. *Challenges, and future directions (may 29, 2024)*, *13*(7), 14–20. https://www.ijitee.org/wp-content/uploads/papers/v13i7/G991113070624.pdf

[17] Nawaz, M., & Babar, M. I. K. (2025). IoT and AI for smart agriculture in resource-constrained environments: Challenges, opportunities and solutions. *Discover internet of things*, *5*(1), 24. https://doi.org/10.1007/s43926-025-00119-3

[18] Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. *Scientific reports*, *13*(1), 21255. https://www.nature.com/articles/s41598-023-46640-9

[19] Yeng, P. K., Nweke, L. O., Yang, B., Ali Fauzi, M., & Snekkenes, E. A. (2021). Artificial intelligence--based framework for analyzing health care staff security practice: Mapping review and simulation study. *JMIR medical informatics*, *9*(12), e19250. https://preprints.jmir.org/preprint/19250?__hstc=102212634.67fe446999e9bea8b41a31f0ecdcb3c6.1762702304873.1762702304873.1762702304873.1&__hssc=102212634.1.1762702304873&__hsfp=3439553344

[20] Mariettou, S., Koutsojannis, C., & Triantafillou, V. (2025). Artificial intelligence and algorithmic approaches of health security systems: A review. *Algorithms*, *18*(2), 59. https://doi.org/10.3390/a18020059

[21] Khan, M. M., Shah, N., Shaikh, N., Thabet, A., & Belkhair, S. (2025). Towards secure and trusted AI in healthcare: A systematic review of emerging innovations and ethical challenges. *International journal of medical informatics*, *195*, 105780. https://doi.org/10.1016/j.ijmedinf.2024.105780

[22] Harahsheh, K. M., & Chen, C. H. (2023). A survey of using machine learning in IoT security and the challenges faced by researchers. *Informatica*, *47*(6), 1–54. https://doi.org/10.31449/inf.v47i6.4635

[23] Dritsas, E., & Trigka, M. (2025). A survey on cybersecurity in IoT. *Future internet*, *17*(1), 30. https://doi.org/10.3390/fi17010030

[24] Tsouplaki, A., Fung, C., & Kalloniatis, C. (2025). Enhancing IoT privacy with artificial intelligence: Recent advances and future directions. *Internet of things*, *34*, 101752. https://doi.org/10.1016/j.iot.2025.101752

[25] Mazhar, T., Talpur, D. B., Shloul, T. Al, Ghadi, Y. Y., Haq, I., Ullah, I., … & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain sciences*, *13*(4), 683. https://doi.org/10.3390/brainsci13040683

[26] Osamy, W., Khedr, A. M., Salim, A., El-Sawy, A. A., Alreshoodi, M., & Alsukayti, I. (2022). Recent advances and future prospects of using AI solutions for security, fault tolerance, and QoS challenges in WSNs. *Electronics*, *11*(24), 4122. https://doi.org/10.3390/electronics11244122

[27] Sathupadi, K., Achar, S., Bhaskaran, S. V., Faruqui, N., Abdullah-Al-Wadud, M., & Uddin, J. (2024). Edge-cloud synergy for AI-enhanced sensor network data: A real-time predictive maintenance framework. *Sensors*, *24*(24), 7918. https://doi.org/10.3390/s24247918

[28] Sinha, P., Sahu, D., Prakash, S., Rathore, R. S., Dixit, P., Pandey, V. K., & Hunko, I. (2025). An efficient data driven framework for intrusion detection in wireless sensor networks using deep learning. *Scientific reports*, *15*(1), 1–25. https://www.nature.com/articles/s41598-025-12867-x

[29] Hudda, S., & Haribabu, K. (2025). A review on WSN based resource constrained smart IoT systems. *Discover internet of things*, *5*(1), 56. https://doi.org/10.1007/s43926-025-00152-2

[30] Pispa, A., & Halunen, K. (2024). A comprehensive artificial intelligence vulnerability taxonomy. *Proceedings of the 23rd european conference on cyber warfare and security, eccws 2024*. Academic Conferences International Limited. https://doi.org/10.34190/eccws.23.1.2157

[31] Kadhim, M. R., Lu, G., Shi, Y., Wang, J., & Kui, W. (2025). Lightweight on-edge clustering for wireless AI-driven applications. *IET communications*, *19*(1), e12874. https://doi.org/10.1049/cmu2.12874