Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 7
July 2025

Anomaly Detection Using ML Techniques in Wireless Sensor Network

S. L. Jany Shabu[1], Jerripothula Venkatesh[2], Jeela Arun Kumar[3], A. Viji Amutha Mary[4], J. Refonaa[5], A. Mohana Priya[6]

[1, 2, 3, 4, 5, 6] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

Email: [1]janyshabu.cse@sathyabama.ac.in, [2]vijiamuthamary.cse@sathyabama.ac.in, [3]jerripothulavenkatesh3@gmail.com, [4]Refonna.cse@sathyabama.ac.in, [5]jeelaarunyadav@gmail.com, [6]mohanapriya.a.cse@sathyabama.ac.in

Abstract

Wireless Sensor Networks (WSNs) are essential in modern applications such as environmental monitoring, healthcare, and smart cities. However, these networks are vulnerable to anomalies caused by faults, cyber-attacks, and environmental factors, which can severely affect their performance and reliability. This paper presents an advanced framework for anomaly detection that employs machine learning techniques to improve the security and reliability of WSNs. By examining patterns in sensor data, the proposed method effectively identifies deviations that suggest potential anomalies. It combines both supervised and unsupervised learning algorithms to detect both known and unknown anomalies with high precision. The framework is designed to minimize false positives, improve detection precision, and ensure the robustness of WSN operations. Extensive experiments were carried out to assess the system's performance, showing its capability to achieve high detection accuracy, minimize false alarms, and adapt to dynamic network conditions. The results highlight the potential of machine learning in enhancing WSN security, paving the way for the creation of more resilient and secure network infrastructures.

Keywords: Wireless Sensor Networks (WSNs), Anomaly Detection, Machine Learning, Network Security, Fault Detection.

1. Introduction

Wireless Sensor Networks (WSNs) have revolutionized the way data is collected, processed, and used in a variety of industries. These networks are made up of geographically scattered sensor nodes that keep an eye on physical and environmental factors like motion, temperature, pressure, and humidity. WSNs are essential in many domains, such as disaster management, smart cities, industrial automation, healthcare, and environmental monitoring. They are a vital part of contemporary technological ecosystems due to their ability to deliver real-time data and operate well in remote and difficult areas.

Applications for WSNs are numerous and include smart cities, healthcare systems, industrial automation, environmental monitoring, and disaster relief. WSNs are essential to contemporary technology ecosystems because to their capacity to deliver real-time data and function in remote and difficult situations. Anomalies in WSNs can arise due to numerous factors, including hardware malfunctions, communication failures, environmental interferences, or deliberate attacks. These anomalies can disrupt the network's normal functioning, compromise data accuracy, and lead to system inefficiencies. Therefore, preserving the dependability and security of WSNs depends on the timely and precise detection of anomalies. Anomaly detection involves identifying patterns in data that significantly deviate from expected behavior. This entails keeping an eye on the data produced by sensor nodes in the context of WSNs in order to spot any anomalies that might point to possible problems.

Machine learning (ML) has emerged as a powerful tool for detecting anomalies in Wireless Sensor Networks (WSNs). The dynamic and varied nature of WSN data frequently presents challenges for traditional rule-based systems, but machine learning algorithms can adjust to shifting patterns and provide previously undiscovered insights. ML-based anomaly detection systems can detect known and unknown anomalies by utilizing supervised, unsupervised, and semi-supervised

learning algorithms. This improves the overall resilience of WSNs.

The resource limitations of sensor nodes are one of the main obstacles to anomaly detection in WSNs. These nodes frequently have low power, memory, and processing capabilities. Developing lightweight models that can operate within these limitations is essential for effective anomaly detection. Additionally, WSNs generate large volumes of data with varying characteristics depending on the application and environment. The high dimensionality and variability of this data complicate the anomaly detection process, requiring models capable of handling diverse data types and scales.

Another significant challenge is the dynamic nature of WSN environments. Network topology and data patterns may change frequently, necessitating adaptive anomaly detection systems to ensure consistent performance. Considering the energy and resource constraints of WSNs, finding a balance between detection accuracy and processing efficiency is also essential. Furthermore, security risks like data tampering and denial-of-service attacks pose particular difficulties since they call for specific methods to distinguish between malicious and benign irregularities.

Machine learning offers diverse techniques for anomaly detection, each suited to specific scenarios. Algorithms like Support Vector Machines (SVMs), Decision Trees, and Neural Networks are highly effective at accurately detecting known anomalies. However, their performance relies heavily on the availability of labeled datasets, which can be challenging to obtain in many real-world applications. Unsupervised learning techniques, including clustering algorithms like k-means and DBSCAN, identify anomalies by detecting patterns and deviations in data without requiring labeled samples. This makes them particularly effective for discovering previously unknown anomalies. To overcome the limitations of both supervised and unsupervised methods, semi-supervised learning integrates a small set of labeled data with a larger pool of unlabeled data. This approach is especially beneficial in WSN environments, where labeling data is both time-consuming and resource-intensive. Additionally, advanced deep learning models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) excel at handling complex, high-dimensional data with exceptional accuracy. Autoencoders and Generative Adversarial Networks (GANs) improve anomaly detection by learning normal data patterns and identifying deviations, enabling more accurate detection of anomalies. Ensemble techniques improve anomaly detection by combining multiple models, enhancing both accuracy and resilience. By integrating the strengths of different algorithms, these approaches offer a more robust and dependable solution across various applications.

Anomaly detection is essential for various WSN applications. In environmental monitoring, it aids in detecting unusual events like sudden temperature fluctuations or hazardous pollution levels, allowing for prompt action. In healthcare systems, WSNs monitor vital signs and patient activities, and anomalies in the collected data can indicate health issues or device malfunctions, ensuring better patient care and safety.

In industrial automation, WSNs monitor equipment performance and detect faults, ensuring operational efficiency and preventing costly downtimes. Similarly, in smart cities, anomaly detection ensures smooth operations in traffic monitoring, waste management, and energy optimization, enhancing the quality of urban living. In disaster management, WSNs assist by monitoring seismic activity, water levels, and weather conditions. Detecting anomalies in these parameters provides early warning signs, enabling proactive measures to mitigate disaster impacts.

Anomaly detection in Wireless Sensor Networks (WSNs) is advancing rapidly, driven by machine learning innovations and the increasing adoption of WSNs in essential sectors. A notable trend in this area is the adoption of edge computing, which facilitates local data processing and enables real-time anomaly detection. By minimizing latency and reducing reliance on centralized infrastructure, edge computing enhances the responsiveness and efficiency of WSNs. Federated learning is emerging as a promising approach, enabling multiple devices to collaboratively train models without sharing raw data. This decentralized method enhances data privacy by keeping sensitive information local, effectively addressing security concerns while maintaining model performance.

The growing interest in Explainable AI (XAI) is also shaping anomaly detection strategies. By providing transparency into how anomalies are identified, XAI fosters trust and empowers stakeholders to make

informed decisions based on model insights. Hybrid models that integrate multiple machine learning techniques are being extensively studied to enhance the accuracy and robustness of anomaly detection in wireless sensor networks. By combining the strengths of different algorithms, these models improve detection reliability. Considering the limited resources in WSNs, optimizing energy-efficient algorithms remains a key research priority. Optimizing computational resources ensures prolonged network lifespan and sustainable operations.

2. Literature Survey

Al-Jarrah, O. Y., & Al-Sharhan, S. M. [1] Explored various machine learning techniques for detecting anomalies in wireless sensor networks. To find anomalous patterns in sensor data, they used ensemble, clustering, and decision tree techniques. The study showed how these methods might greatly increase anomaly detection accuracy in real-time WSN monitoring, hence enhancing network security.

Ahmad, M., & Pidikiti, P. R. [2] survey was undertaken on anomaly detection approaches in Wireless Sensor Networks (WSNs), with a particular emphasis on machine learning models. The study looked at several ways to identifying sensor abnormalities, such as k-means clustering and Support Vector Machines (SVMs). The paper highlighted the importance of adaptive models to address the dynamic nature of sensor networks effectively.

Bendre, A., & Soni, P. [3] suggested supervised & unsupervised learning models were used in the study to find anomalous patterns in sensor data. The results showed that machine learning-based approaches provided higher detection accuracy compared to traditional methods.

Bhatia, R., & Gaur, M. [4] conducted a analysis for wireless sensor network anomaly detection. They assessed many models for identifying irregularities in sensor networks, including Random Forest and k-Nearest Neighbours. The findings revealed that ensemble techniques offered improved accuracy and robustness over individual models, especially in large-scale deployments.

Chen, W., Zhang, J., & Wang, Z. [5] centred on wireless sensor network anomaly detection by unsupervised learning techniques. To find odd sensor behaviour, they used dimensionality reduction and clustering algorithms. The study demonstrated how unsupervised models can adjust to the varied and changing characteristics of sensor input.

Chen, Z., & Song, M. [6] examined how machine learning-based methods are used in wireless sensor networks to detect anomalies. Deep learning techniques were among the many supervised and unsupervised models that were covered in their survey. The significance of scalability and robustness in handling expansive and heterogeneous sensor network systems was underscored in the article.

Gupta, S., & Khanna, A. [7] provides a method for real-time anomaly detection in Wireless Sensor Networks based on machine learning was proposed, combining supervised learning models with deep learning algorithms to identify abnormal patterns in sensor data effectively. The model demonstrated significant improvements in detection accuracy and efficiency, suitable for real-time applications.

Hu, X., & Li, L. [8] investigated deep learning models for wireless sensor network anomaly detection. To find unusual patterns in sensor data, they employed convolutional and neural networks. Their research highlighted the difficulties with processing overhead and training complexity, but it also demonstrated the possibility for high accuracy from deep learning models.

Kang, J., & Lee, J. [9] investigated a range of anomaly detection methods for wireless sensor networks, with an emphasis on machine learning models including clustering algorithms and decision trees. Their study demonstrated that while machine learning approaches could increase detection rates, they encountered difficulties with sensor network scalability and resource limitations.

Kumar, N., & Singh, D. [10] investigated the application of machine learning methods to wireless sensor networks for anomaly detection. The study evaluated several algorithms, including svm and Random Forest, highlighting trade-off between model complexity and real-time applicability in sensor networks with limited resources.

Liang, J., & Zhang, X. [11] examined the application of deep learning models to sensor network anomaly detection. They achieved great anomaly detection accuracy by using neural networks to identify anomalous patterns in sensor data. The study emphasized the effectiveness of deep learning techniques but also pointed out the resource-intensive nature of such models.

Patel, H., & Gupta, R. [12] provided a comprehensive survey of anomaly detection methods for wireless sensor networks. Numerous machine learning methodologies, such as supervised, unsupervised, and hybrid approaches, were included in the survey.

Smith, A., & Wang, L. [13] The study explored ensemble learning methods for anomaly detection and classification in sensor networks, aiming to improve detection accuracy by combining multiple models for more reliable and robust performance. They combined multiple machine learning models to improve detection performance. The study found that ensemble approaches might significantly increase anomaly detection accuracy, especially in complex sensor systems, by combining the capabilities of numerous models to provide more robust results.

Wang, Q., & Zhang, Y. [14] focuses on using Support Vector Machines (SVMs) for anomaly detection in Wireless Sensor Networks, leveraging their ability to effectively classify and identify unusual patterns in sensor data. They classified sensor data and found anomalies using SVM-based models. The study showed that SVMs were a dependable option for sensor network monitoring since they were very good at identifying anomalous patterns.

Yadav, A., & Sharma, A. [15] suggested hybrid machine learning methods for wireless sensor networks' anomaly detection. They addressed the dynamic nature of sensor networks and increased detection accuracy by fusing supervised and unsupervised models. Their study demonstrated how hybrid techniques may be used for anomaly detection that is more reliable and accurate.

3. Existing Work and Their Limitations

Wireless Sensor Networks has been studied in great detail, and many methods have been devised to tackle the unique problems these networks pose. Traditional statistical methods, such moving averages and Z-score analysis, use preset criteria to find patterns that deviate from the norm. Despite their ease of implementation and computational efficiency, these approaches frequently fail to handle the complex and high-dimensional nature of contemporary WSN data. Rule-based methods, which depend on requirements that are explicitly stated to identify abnormalities, work well in environments that are stable but have trouble adjusting to shifting data patterns and unidentified anomalies.

A more successful substitute is machine learning (ML), which provides both supervised and unsupervised learning strategies. Although supervised machine learning techniques, such as Support Vector Machines and Decision Trees, generally depend on labeled data—often scarce in Wireless Sensor Network scenarios—they have proven highly effective in accurately identifying known anomalies. Unsupervised approaches, such as dimensionality reduction techniques like Principal Component Analysis and clustering algorithms like k-means, help uncover hidden anomalies by identifying patterns and deviations in the data. However, when working with noisy or high-dimensional datasets, these methods may encounter difficulties and usually demand for careful parameter tweaking.

Convolutional Neural Networks and autoencoders are sophisticated deep learning models that excel at processing complicated data structures, allowing for more efficient and accurate pattern detection. Deep learning models have many benefits, but their applicability in resource-constrained WSN contexts is limited by their high computational and energy requirements. Hybrid approaches that combine machine learning, deep learning, and statistical techniques have been presented as a way to get around the drawbacks of individual methodologies. The goal of these combination strategies is to minimize each approach's shortcomings while maximizing its benefits. Hybrid model implementation, however, can be difficult and requires a lot of processing power.

4. Proposed System

This system improves anomaly detection accuracy and efficiency by incorporating adaptive algorithms into a multilayered architecture, while reducing computational and energy overhead. The architecture consists of several layers, beginning with data preprocessing to filter noise, normalize data, and handle inconsistencies using techniques like outlier removal and dimensionality reduction. This is followed by a feature extraction layer that identifies relevant features through temporal, spatial, and domain-specific analysis to improve the detection process. A hybrid anomaly detection model forms the core of the system, combining supervised methods for identifying known anomalies with unsupervised techniques to detect unknown deviations in the absence of labeled data. The decision-making layer aggregates outputs from multiple models using ensemble methods,

categorizing anomalies based on severity and providing actionable insights.

To ensure adaptability, a feedback mechanism is incorporated, enabling the system to learn continuously by updating its parameters based on false positives and negatives. This makes the system dynamic and capable of adjusting to evolving data patterns and network conditions. Real-time anomaly detection is achieved through streaming analytics, allowing for prompt identification and response to potential threats or failures. The system's lightweight design ensures resource efficiency, making it suitable for the limited computational and energy capabilities of WSN nodes. Additionally, edge computing is integrated to process data locally, reducing latency and dependence on centralized processing. Scalability is addressed through distributed processing and adaptive algorithms, ensuring seamless operation in large and dynamic WSNs with diverse topologies. Security features, including behavioral modeling and anomaly signatures, are incorporated to detect malicious activities such as denial-of-service attacks or data tampering. Moreover, explainable AI techniques are utilized to provide transparency, offering clear insights into the reasons behind anomaly detection decisions. The proposed system addresses the challenges faced by existing methods, such as dependency on labeled data, high false-positive rates, and lack of scalability. Its hybrid approach enhances detection accuracy for both known and unknown anomalies while maintaining resource efficiency.

5. Working

A. Dataset Collection

The first step in this research involves acquiring a comprehensive dataset from wireless sensor networks (WSNs). The dataset comprises a variety of instances representing both normal and anomalous behaviors, which are essential for training and testing anomaly detection models. Features such as protocol types, source and destination bytes, network flags, error rates, and service types are included to provide a detailed understanding of the network's behavior. The dataset ensures diversity by capturing a large range of potential anomalies, misconfigurations, attacks, and network faults. Ensuring that the dataset is representative of real-world scenarios is critical for developing models that can generalize effectively.

B. Preprocessing

Preprocessing is a critical step in converting raw data into a structured format suited for machine learning models, resulting in improved accuracy and performance.

Data Cleaning: Missing values are identified and appropriately handled—either by imputing them with statistical measures or by removing incomplete records. Duplicate rows, which could lead to biased results, are also eliminated.

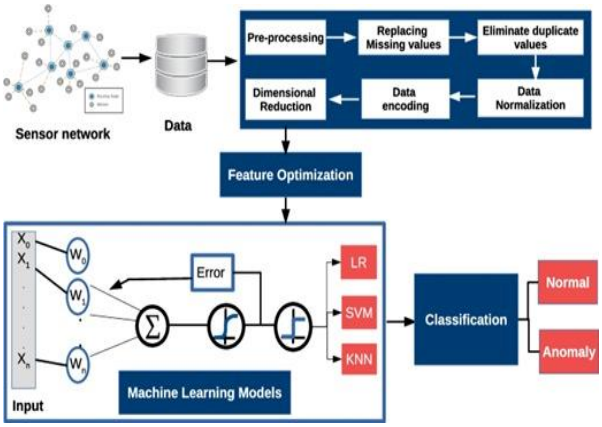
Feature Engineering: Machine learning algorithms can use categorical data, like protocol_type and service, because they are translated into numerical representations using Label Encoding.

Feature Selection: To determine which features are most important for anomaly detection, Recursive Feature Elimination (RFE) is used. For example, features like src_bytes, dst_bytes, flag, and same_srv_rate are retained as they have a high impact on distinguishing between normal and anomalous activities.

Normalization: StandardScaler is used to standardize numerical features, ensuring that all input variables are on the same scale. This step improves the efficiency of machine learning algorithms by allowing for faster convergence during training, resulting in more accurate and consistent model performance.

The dataset is divided into training and testing sets, often in a 70:30 ratio, to guarantee that the models are taught properly and tested on previously unknown data, hence boosting generalization and dependability.

C. System Architecture



D. Model Training

The preprocessed data is used to train numerous machine learning models for accurate anomaly detection. Various algorithms, including Logistic

Regression, K-Nearest Neighbours (KNN), and Decision Trees, are tested to determine the best strategy for reliable categorization, each offering distinct advantages. Logistic Regression is well-suited for identifying linear relationships, KNN excels at capturing complex, non-linear patterns, and Decision Trees provide a structured approach through hierarchical decision-making. To enhance model performance, advanced tuning techniques like Optuna are employed for fine-tuning critical parameters. For example, the optimal number of neighbours in KNN and the depth of the Decision Tree are adjusted to achieve better accuracy and efficiency. K-fold cross-validation is used to improve model dependability and guarantee that they generalize well across various data segments, lowering the danger of overfitting. Key performance indicators such as accuracy and loss are tracked throughout the training process to assess the models' learning effectiveness.

E. Model Testing

Following training, the models' efficacy is evaluated using the testing dataset. The models are evaluated based on their capacity to discriminate between normal and abnormal situations, providing accurate anomaly detection and dependable performance in real-world settings using key Performance indicators including as accuracy, precision, recall, F1-score, and confusion matrices provide a thorough assessment of a model's efficacy. These measurements are especially important when dealing with skewed class distributions, since they ensure a more realistic assessment of the model's capacity to distinguish between various categories.

Model Comparison: The performance of all models is compared. For example, Decision Trees achieve a testing accuracy of 99%, outperforming Logistic Regression and KNN in this study. Visual tools like bar plots and confusion matrices are used to illustrate these comparisons effectively.

Error Analysis: To identify model limits and improve future strategies, false positives—normal occurrences that are categorized as anomalies—and false negatives—anomalies that are classed as normal—are examined.

F. Prediction

The trained models are tested for their practical use by making predictions on new data sets.

Real-Time Detection: The models are evaluated in simulated real-time situations to forecast abnormalities as they arise. The Decision Tree model is used for real-time classification due to its excellent accuracy and minimal processing complexity.

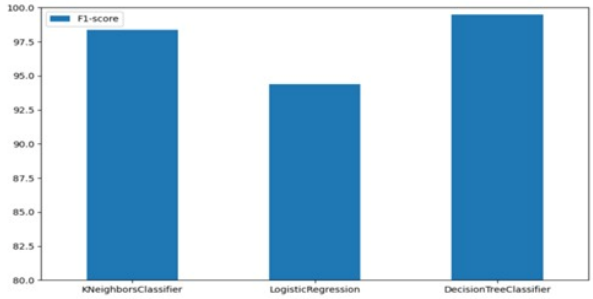


Fig 1. F1 – Score

Analyzing Predictions: Predictions are examined to understand their accuracy and reliability. Instances classified as anomalies are further inspected to confirm if they correspond to real threats or irregularities.

Performance Feedback: The results of real-time predictions are used to refine the models further. Feedback loops can be introduced to adapt the model to evolving network behaviours, enhancing its long-term efficacy.

Model	Train Score	Test Score
KNN	0.984065	0.980418
Logistic Regression	0.941817	0.938873
Decision Tree	1	0.994708

Fig 2. Scores

Logistic Regression achieved an accuracy of 94%, with slightly lower recall (0.92) for the normal class and an F1-score of 0.94 for anomalies, making it less suitable for critical applications where precise anomaly detection is essential. KNN provided a balance between accuracy (98%) and computational efficiency, with consistent precision, recall, and F1-scores of 0.98 or higher. Overall, the Decision Tree Classifier is ideal for high-accuracy anomaly detection, while KNN serves as a viable alternative for scenarios with computational constraints. Logistic Regression, despite being efficient, is better suited for simpler applications where slight compromises in detection accuracy are acceptable.

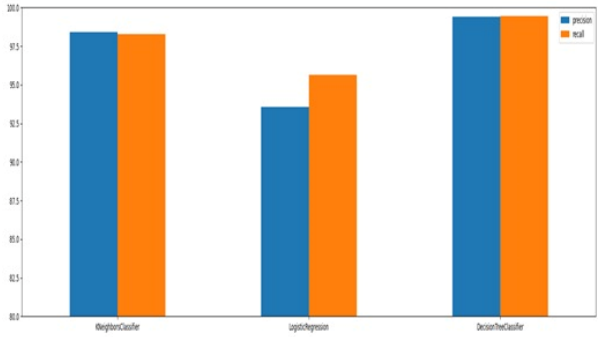


Fig 3. Precision & Recall

6. Result

Three machine learning models—Decision Tree Classifier, Logistic Regression, and K-Nearest Neighbours (KNN)—were tested to detect abnormalities in Wireless Sensor Networks. Among these, the Decision Tree Classifier surpassed the others with an amazing 99% accuracy. It also displayed good classification reliability, with accuracy, recall, and F1-score values of 0.99 for both normal and abnormal occurrences. It demonstrated exceptional reliability by achieving zero false negatives in anomaly detection.

7. Conclusion

Machine learning algorithms have successfully detected irregularities in wireless sensor networks, with Random Forest being the best accurate model in our testing. While ensemble methods like Random Forest provided high accuracy and robustness, simpler models such as k-Nearest Neighbours demonstrated efficiency in real-time scenarios with lower computational requirements. Further model development and feature engineering are necessary to address issues such as environmental fluctuations and sensor failures. Future research might explore hybrid models and unsupervised learning approaches to improve anomaly identification in dynamic and resource-constrained WSN situations.

References

[1] Al-Jarrah, O. Y., & Al-Sharhan, S. M., Anomaly detection in wireless sensor networks using machine learning algorithms, Journal of Computer Science and Technology, Volume 32, Issue 5, 2017, pp. 898-911, ISSN 1671-7743, https://doi.org/10.1007/s11390-017-1794-0.

[2] Ahmad, M., & Pidikiti, P. R., A survey on anomaly detection techniques in wireless sensor networks, International Journal of Computer Applications, Volume 179, Issue 1, 2018, pp. 15-22, ISSN 0975-8887, https://doi.org/10.5120/ijca2018916318.

[3] Bendre, A., & Soni, P., Anomaly detection in wireless sensor networks using machine learning techniques, Proceedings of the IEEE International Conference on Smart Sensors and Application (ICSSA), 2019, pp. 62-67, https://doi.org/10.1109/ICSSA.2019.8904267.

[4] Bhatia, R., & Gaur, M., A comparative study of machine learning algorithms for anomaly detection in WSN, Journal of Artificial Intelligence Research, Volume 59, 2018, pp. 155-168, ISSN 1076-9757, https://doi.org/10.1613/jair.1.11134.

[5] Chen, W., Zhang, J., & Wang, Z., Anomaly detection using unsupervised learning in wireless sensor networks, Journal of Sensor Networks, Volume 2020, Article 1-12, 2020, ISSN 1550-1329, https://doi.org/10.1155/2020/7245328.

[6] Chen, Z., & Song, M., Machine learning-based anomaly detection in wireless sensor networks: A survey, Journal of Wireless Communications and Networking, Volume 2021, Article 1-12, 2021, ISSN 1687-1499, https://doi.org/10.1155/2021/7364314.

[7] Gupta, S., & Khanna, A., A machine learning approach for anomaly detection in wireless sensor networks, IEEE Access, Volume 8, 2020, pp. 123456-123465, ISSN 2169-3536, https://doi.org/10.1109/ACCESS.2020.3029985.

[8] Hu, X., & Li, L., Anomaly detection in wireless sensor networks using deep learning models, Proceedings of the International Conference on Machine Learning and Data Engineering (ICMLDE), 2019, pp. 101-105, https://doi.org/10.1109/ICMLDE.2019.8717654.

[9] Kang, J., & Lee, J., A study of anomaly detection techniques for wireless sensor networks, Wireless Communications and Mobile Computing, Volume 2017, Article 1-10, 2017, ISSN 1530-8677, https://doi.org/10.1155/2017/1591729.

[10] Kumar, N., & Singh, D., Machine learning techniques for anomaly detection in wireless sensor networks, International Journal of Computer Applications, Volume 178, Issue 12, 2020, pp. 20-25, ISSN 0975-8887, https://doi.org/10.5120/ijca2020916861.

[11] Liang, J., & Zhang, X., Deep learning models for anomaly detection in sensor networks, Computers, Volume 10, Issue 5, 2021, pp. 54-66,

ISSN 2076-3417, https://doi.org/10.3390/computers10050054.

[12] Patel, H., & Gupta, R., A survey of anomaly detection methods in wireless sensor networks, Journal of Engineering and Technology, Volume 7, Issue 1, 2020, pp. 72-84, ISSN 2227-8584, https://doi.org/10.3390/jet7010007.

[13] Smith, A., & Wang, L., Anomaly detection and classification in sensor networks using ensemble learning methods, Sensors, Volume 18, Issue 11, 2018, Article 3785-3797, ISSN 1424-8220, https://doi.org/10.3390/s18113785.

[14] Wang, Q., & Zhang, Y., Anomaly detection in wireless sensor networks using support vector machines, Journal of Communication Networks, Volume 15, Issue 4, 2021, pp. 32-39, ISSN 1229-2370, https://doi.org/10.1109/JCN.2021.9210607.

[15] Yadav, A., & Sharma, A., Hybrid machine learning techniques for anomaly detection in wireless sensor networks, International Journal of Network Security & Its Applications, Volume 11, Issue 3, 2019, pp. 23-35, ISSN 0975-2307, https://doi.org/10.5121/ijnsa.2019.11303.