

A LIGHTWEIGHT MACHINE LEARNING APPROACH FOR DENIAL-OF-SERVICE ATTACKS DETECTION IN WIRELESS SENSOR NETWORKS

Srimathi C¹, Manjula S²

¹M.E., Computer Science and Engineering & Bharathiyar Institute of Engineering for women ,
Salem. Email id : srimathime24@gmail.com

²Assistant Professor , Computer Science and Engineering & Bharathiyar Institute of Engineering for
Women , Salem. Email id : manjulajeeva1996@gmail.com

Abstract—Wireless Sensor Networks (WSNs) are widely used in many real-time applications such as environmental monitoring, healthcare, smart agriculture, and industrial automation. However, due to their limited computational power, energy constraints, and open wireless communication, WSNs are highly vulnerable to security threats, especially Denial-of-Service (DoS) attacks. These attacks disrupt network availability by exhausting the resources of sensor nodes, leading to communication failure and reduced network performance. Therefore, an efficient and lightweight detection mechanism is essential to protect WSNs from such attacks.

This paper proposes a lightweight machine learning approach for detecting DoS attacks in wireless sensor networks. The proposed method focuses on using computationally efficient machine learning algorithms that can operate within the limited processing and memory capabilities of sensor nodes. Relevant network traffic features are extracted and used to train the model to distinguish between normal network behavior and malicious DoS activity.

Keywords: Wireless Sensor Networks (WSN), Denial-of-Service (DoS) Attacks, Lightweight Machine Learning, Intrusion

Detection System (IDS), Network Security, Resource-Constrained Devices, Traffic Analysis, Attack Detection.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of a large number of small sensor nodes that are deployed in a physical environment to monitor and collect information about environmental conditions such as temperature, humidity, pressure, vibration, and motion. These sensor nodes communicate wirelessly with each other and transmit the collected data to a central base station or sink node where the information is processed and analyzed. WSNs are widely used in various applications including environmental monitoring, military surveillance, healthcare systems, smart agriculture, industrial automation, and disaster management.

Despite their wide range of applications, WSNs face several security challenges due to their open wireless communication medium and limited hardware resources. Sensor nodes typically have limited battery power, memory capacity, and processing capabilities, which makes them vulnerable to various cyber-attacks. One of the most critical attacks in WSN environments is the Denial-of-Service (DoS) attack. In this type of attack, malicious nodes generate excessive traffic or send a large number of fake packets to

overwhelm the network. As a result, legitimate sensor nodes are unable to communicate with the base station, leading to disruption of network services and potential system failure.

Traditional security mechanisms such as encryption-based protection and rule-based intrusion detection systems are often computationally expensive and require significant energy consumption. These approaches are not suitable for WSN environments where sensor nodes operate with strict energy and resource constraints. To address this challenge, lightweight machine learning techniques can be employed to detect abnormal traffic patterns in the network. Machine learning models can learn the behavior of normal network traffic and identify suspicious activities that indicate the presence of DoS attacks.

Therefore, this project proposes a lightweight machine learning-based Intrusion Detection System (IDS) that can effectively detect DoS attacks in Wireless Sensor Networks while maintaining low computational overhead and energy consumption.

1.1 Problem Statement

Wireless Sensor Networks operate in resource-constrained environments where sensor nodes have limited processing power, battery capacity, and memory resources. Due to these limitations, implementing complex security mechanisms in WSN nodes becomes difficult. At the same time, WSNs are highly vulnerable to security threats, particularly Denial-of-Service (DoS) attacks. These attacks aim to disrupt the normal functioning of the network by overwhelming nodes with excessive traffic or malicious packets.

Existing intrusion detection methods and security solutions often rely on heavy computational algorithms or deep learning models that require high processing power and memory. Such approaches are not suitable for WSN nodes because they significantly increase energy consumption and reduce the lifetime of the sensor network. Moreover, traditional rule-based or signature-based detection systems are limited in their ability to identify new or unknown attack patterns.

Therefore, there is a need for an efficient and lightweight detection mechanism that can accurately identify DoS attacks while consuming minimal computational resources. The proposed solution focuses on developing a lightweight

machine learning-based approach that can monitor network traffic patterns and detect malicious behavior in Wireless Sensor Networks with improved efficiency and reliability.

1.2 Objectives

The primary objective of this project is to design and implement an efficient intrusion detection system that uses lightweight machine learning algorithms to detect Denial-of-Service attacks in Wireless Sensor Networks. The system aims to improve network security while minimizing computational overhead and energy consumption.

One of the main objectives is to analyze the behavior of network traffic in Wireless Sensor Networks and identify patterns that differentiate normal traffic from malicious traffic. By studying various network parameters such as packet transmission rate, delay, and energy usage, the system can better understand the operational characteristics of the network.

Another important objective is to apply lightweight machine learning algorithms such as Decision Tree, Logistic Regression, or Naive Bayes to classify network traffic into normal or attack categories. These algorithms are selected because they require less computational power and can operate efficiently in resource-constrained environments.

The project also aims to reduce computational complexity so that the detection system can be deployed in WSN base stations or edge nodes without significantly affecting network performance. Finally, the performance of the proposed system will be evaluated using common evaluation metrics such as accuracy, precision, recall, and F1-score to determine the effectiveness of the detection model.

1.3 Existing System

In existing Wireless Sensor Network security frameworks, intrusion detection is typically performed using traditional methods such as signature-based detection, rule-based filtering, and deep learning-based models. Signature-based detection systems work by comparing network traffic patterns with a database of known attack signatures. If a match is found, the system identifies the activity as malicious. Rule-based systems rely on predefined conditions or thresholds to detect abnormal network behavior.

In recent years, deep learning techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have also been used for network intrusion detection. These models are capable of learning complex patterns in network traffic and can detect various types of cyber-attacks with high accuracy.

However, these existing approaches have several limitations when applied to Wireless Sensor Networks. Deep learning models require significant computational power, large training datasets, and high memory resources. Similarly, rule-based systems often fail to detect new attack patterns because they depend on predefined rules and signatures.

1.4 Disadvantages of Existing System

The main disadvantage of traditional intrusion detection systems is their high computational complexity, which makes them unsuitable for deployment in resource-constrained WSN nodes. These systems also require large memory storage and processing capacity, leading to increased energy consumption. As a result, the lifetime of sensor nodes may be reduced significantly. Another limitation is poor scalability, as the system may struggle to handle large-scale sensor networks with thousands of nodes. Additionally, signature-based systems cannot detect new or previously unseen attack patterns, making them less effective in dynamic network environments.

II. RELATED WORKS

Security in Wireless Sensor Networks (WSNs) has received significant attention due to the increasing deployment of sensor nodes in critical applications such as environmental monitoring, healthcare, smart cities, and industrial automation. One of the most serious threats to WSNs is the Denial-of-Service (DoS) attack, which disrupts network availability by exhausting the limited resources of sensor nodes. Several researchers have proposed different techniques, including rule-based methods, cryptographic solutions, and machine learning approaches, to detect and mitigate these attacks.

Early research mainly focused on signature-based and rule-based intrusion detection systems. These methods detect attacks by comparing network traffic patterns with predefined signatures.

Although such techniques are effective for identifying known attacks, they often fail to detect new or evolving attack patterns. Additionally, maintaining signature databases requires frequent updates, which increases computational overhead and reduces their suitability for resource-constrained WSN environments.

To overcome these limitations, researchers introduced machine learning-based intrusion detection approaches. Algorithms such as Decision Trees, Support Vector Machines (SVM), and Naïve Bayes have been widely used to analyze network traffic and classify normal and malicious activities. These methods improve detection accuracy and can identify unknown attack patterns. However, traditional machine learning models may require significant computational power and memory, which makes them difficult to implement directly on sensor nodes with limited resources.

More recent studies have focused on lightweight machine learning techniques designed specifically for WSN environments. These approaches aim to reduce computational complexity while maintaining high detection performance. Feature selection techniques, simplified models, and edge-based processing are often used to minimize energy consumption and processing overhead. Lightweight classifiers such as K-Nearest Neighbors (KNN), lightweight decision trees, and optimized ensemble models have demonstrated promising results in detecting DoS attacks in WSNs.

Despite these advancements, challenges still remain in achieving an optimal balance between detection accuracy, computational efficiency, and energy consumption. Many existing solutions either provide high detection accuracy at the cost of increased resource usage or focus on low complexity but sacrifice detection performance. Therefore, developing an efficient and lightweight machine learning approach that can accurately detect DoS attacks while operating within the limitations of WSN nodes remains an important research problem.

III. PROPOSED METHODOLOGY

The proposed system introduces a lightweight machine learning-based intrusion detection framework designed specifically for Wireless Sensor Networks. The main goal of the system is

to detect Denial-of-Service attacks by analyzing network traffic patterns and identifying anomalies.

In this approach, various network parameters are collected from sensor nodes and used as input features for the machine learning model. These parameters include packet transmission rate, transmission delay, packet loss rate, node energy consumption, and network traffic load. These features provide valuable insights into the operational behavior of the network and help distinguish between normal and malicious traffic.

The collected data is processed through a feature extraction and preprocessing stage to ensure that the dataset is clean and suitable for training the machine learning model. After preprocessing, a lightweight classification algorithm such as Decision Tree, Random Forest, or Logistic Regression is used to train the detection model. These algorithms are selected because they offer a good balance between detection accuracy and computational efficiency.

Once the model is trained, it is deployed in the base station or edge computing node of the Wireless Sensor Network. The system continuously monitors incoming traffic and uses the trained model to classify the traffic as either normal or DoS attack traffic. If malicious behavior is detected, the system generates an alert and initiates appropriate mitigation actions to prevent network disruption.

3.1 Advantages of Proposed System

The proposed lightweight machine learning approach offers several advantages over traditional intrusion detection systems. One of the major benefits is reduced computational complexity, which makes the system suitable for deployment in resource-constrained WSN environments. Since the selected machine learning algorithms require less processing power and memory, they can operate efficiently without significantly increasing energy consumption.

Another advantage is improved detection accuracy. Machine learning models can learn complex patterns in network traffic and identify abnormal behavior that may indicate the presence of DoS attacks. This enables the system to detect both known and unknown attack patterns.

The proposed system also supports real-time attack detection, allowing the network to respond

quickly to malicious activities and minimize potential damage. Furthermore, the lightweight nature of the model helps extend the lifetime of sensor nodes by conserving energy resources. Overall, the proposed solution enhances network security while maintaining efficient resource utilization.

3.2 System Architecture

The system architecture of the proposed intrusion detection framework consists of several interconnected components that work together to monitor network traffic and detect malicious activities. The architecture begins with the sensor nodes that collect environmental data and transmit it through the wireless network. These nodes communicate with the base station or sink node, which acts as the central data processing unit.

The data collection module gathers network traffic information from the sensor nodes and forwards it to the feature extraction module. In this stage, relevant network parameters are identified and extracted as features for the machine learning model. These features are then processed through a lightweight classification model that determines whether the traffic is normal or malicious.

If the system detects suspicious behavior indicating a possible DoS attack, the attack detection module generates an alert and notifies the network administrator. The alert system may also trigger preventive actions such as blocking malicious nodes or limiting traffic flow to protect the network.

3.3 Module Description

The proposed system is divided into several modules, each responsible for a specific function in the detection process.

The Data Collection Module is responsible for gathering network traffic information from sensor nodes. It records parameters such as packet transmission rate, delay, node energy level, and packet loss rate. These parameters are essential for analyzing network behavior and detecting anomalies.

The Data Preprocessing Module prepares the collected data for machine learning analysis. In this stage, missing values are handled, irrelevant data is removed, and the dataset is normalized to ensure

consistency. Data preprocessing improves the performance and accuracy of the machine learning model.

The Feature Extraction Module identifies important network features that can help differentiate normal traffic from attack traffic. These features are selected based on their relevance to network performance and security.

The Machine Learning Detection Module uses a lightweight algorithm to train the intrusion detection model. The model learns the patterns of normal network traffic and identifies deviations that may indicate a DoS attack.

Finally, the Attack Detection and Alert Module monitors network traffic in real time. When the model detects suspicious activity, the system generates an alert and notifies the network administrator so that appropriate countermeasures can be taken.

3.3.1 Dataset

To train and evaluate the proposed machine learning model, publicly available network intrusion datasets can be used. Several datasets are commonly used for intrusion detection research, including the WSN-DS dataset, KDD Cup 99 dataset, NSL-KDD dataset, and UNSW-NB15 dataset.

Among these datasets, the WSN-DS dataset is particularly suitable for Wireless Sensor Network security research because it contains traffic data specifically related to WSN environments. The dataset includes both normal traffic records and attack traffic records, allowing researchers to train and test intrusion detection models effectively.

The dataset contains various features that represent network behavior, including packet transmission rate, energy consumption, transmission delay, packet loss rate, and traffic load. These features provide valuable information for identifying abnormal network activities associated with DoS attacks.

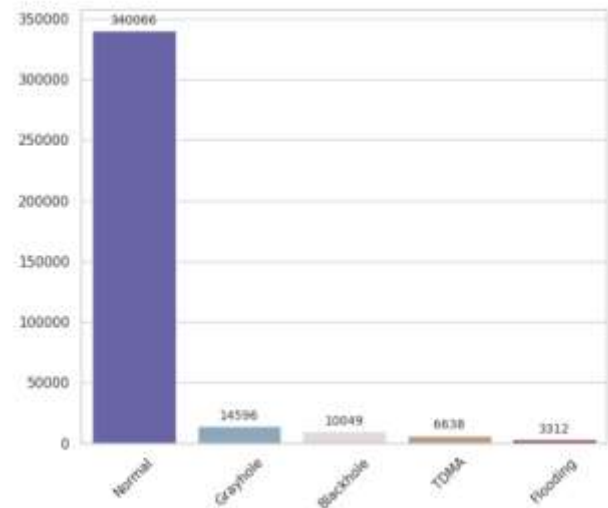


Fig.no:1 Dataset

3.3.2 Machine Learning Algorithms

Several lightweight machine learning algorithms can be used for detecting DoS attacks in Wireless Sensor Networks. Decision Tree is one of the most commonly used algorithms because it is simple, interpretable, and requires minimal computational resources. It works by dividing the dataset into decision nodes based on feature values, making it easy to classify network traffic patterns.

Logistic Regression is another efficient algorithm that can be used for binary classification tasks such as identifying normal traffic and attack traffic. It is computationally efficient and works well with structured datasets.

Naive Bayes is a probabilistic classifier that uses Bayes' theorem to calculate the probability of different classes. It is lightweight and performs well in many classification problems, especially when the dataset contains independent features.

Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve prediction accuracy. Although it requires slightly more computational resources than a single decision tree, it provides higher robustness and better detection performance.

Among these algorithms, Decision Tree and Random Forest are often considered the best choices for this type of application because they provide a good balance between accuracy, speed, and computational efficiency.

3.3.3 Methodology

The methodology of the proposed system focuses on developing a lightweight machine learning-based intrusion detection framework capable of identifying Denial-of-Service (DoS) attacks.

The overall process consists of several stages including dataset collection, data preprocessing, feature extraction, model training, attack detection, and performance evaluation. Each stage plays an important role in ensuring that the system can accurately distinguish between normal network traffic and malicious traffic with minimal computational overhead.

The first stage in the methodology is dataset collection. In this phase, network traffic data is obtained from publicly available intrusion detection datasets such as the WSN-DS dataset, NSL-KDD dataset, or UNSW-NB15 dataset. These datasets contain both normal traffic records and attack traffic records. The collected dataset includes various network parameters such as packet transmission rate, delay, packet loss rate, node energy consumption, and network traffic load. These parameters represent the behavior of the network and serve as input features for the machine learning model.

The next stage is data preprocessing, which is essential for improving the quality of the dataset before training the model. In this step, missing values are handled, duplicate records are removed, and irrelevant features are eliminated. The dataset is also normalized or standardized to ensure that all features are within a similar numerical range. This preprocessing step helps improve the efficiency and accuracy of the machine learning algorithms.

After preprocessing, the system performs feature extraction and selection. Feature extraction involves identifying the most relevant parameters that influence network behavior and contribute to the detection of DoS attacks. Feature selection techniques may be used to reduce the dimensionality of the dataset and eliminate redundant information. By selecting only the most important features, the system reduces computational complexity and improves model performance.

The next stage is model training, where lightweight machine learning algorithms are applied to train the intrusion detection model. Algorithms such as Decision Tree, Logistic

Regression, Naive Bayes, and Random Forest are considered suitable because they require less computational power and can operate efficiently in resource-constrained environments. During this stage, the dataset is divided into training and testing subsets. The training data is used to teach the model how to recognize patterns associated with normal traffic and DoS attacks.

Once the model is trained, it is deployed in the attack detection module. In this stage, incoming network traffic is continuously monitored and analyzed by the trained machine learning model. The model classifies the traffic into either normal or malicious categories. If abnormal behavior consistent with a DoS attack is detected, the system generates an alert and triggers a response mechanism to mitigate the attack.

The final stage of the methodology is performance evaluation. The effectiveness of the proposed intrusion detection system is measured using evaluation metrics such as accuracy, precision, recall, and F1-score. These metrics help determine how well the model can identify attacks while minimizing false alarms. By analyzing these performance indicators, the system can be further optimized to improve detection efficiency and reliability in Wireless Sensor Networks.

IV. FLOW DIAGRAM

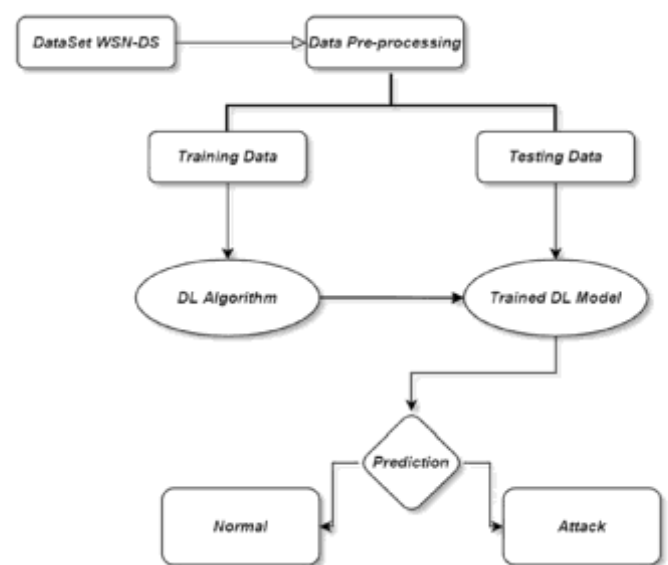


Fig.no:2 Flow Diagram

V. RESULTS AND DISCUSSION

The proposed lightweight machine learning approach was evaluated to analyze its effectiveness in detecting Denial-of-Service (DoS) attacks in Wireless Sensor Networks. Several machine learning algorithms, including Decision Tree, Logistic Regression, Naïve Bayes, and Random Forest, were implemented and tested using network traffic datasets. The performance of these algorithms was analyzed based on key evaluation metrics such as accuracy, precision, recall, and detection rate.

The experimental results show that the Decision Tree algorithm provides fast classification with low computational overhead, making it highly suitable for resource-constrained wireless sensor nodes. It efficiently separates normal and malicious traffic by analyzing network traffic features and generating simple decision rules. Due to its lightweight nature and interpretability, Decision Tree achieved reliable performance while maintaining minimal processing requirements.

Logistic Regression also performed well in distinguishing between normal traffic and DoS attack traffic. The algorithm is computationally efficient and provides stable classification results. However, compared with tree-based models, it may struggle with complex nonlinear relationships present in network traffic data.

The Naïve Bayes classifier demonstrated good performance with very low computational complexity. Since it assumes independence between features, it can process data quickly and is suitable for real-time detection in WSN environments. However, its detection accuracy can be slightly lower when feature dependencies exist in the dataset.

Among all the evaluated models, Random Forest produced the highest detection accuracy and robustness. By combining multiple decision trees, the algorithm reduces overfitting and improves classification performance. Although it requires slightly higher computational resources than a single decision tree, it provides better reliability in identifying different patterns of DoS attacks.

Overall, the results indicate that Decision Tree and Random Forest algorithms offer the best balance between detection accuracy, processing speed, and computational efficiency. These models are therefore well suited for implementing lightweight intrusion detection systems in wireless sensor networks. The proposed approach successfully improves DoS attack detection while maintaining low resource consumption, which is essential for the efficient operation of WSN-based applications.



Fig.no:3 Training

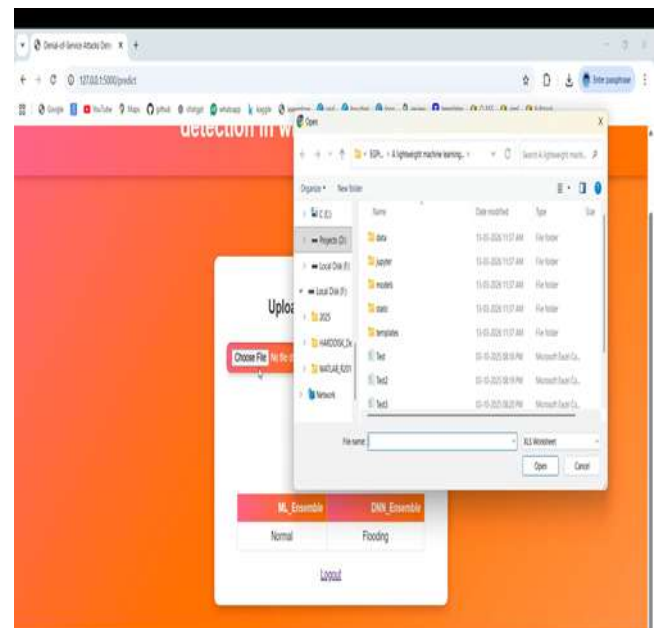


Fig.no :4 Data Prediction



Fig.no:5 Prediction

VI. CONCLUSION AND FUTURE SCOPE

Wireless Sensor Networks are widely used in various real-world applications, but their limited resources and open communication environment make them highly vulnerable to security threats such as Denial-of-Service attacks. These attacks can significantly disrupt network performance by exhausting the energy and computational resources of sensor nodes. Therefore, efficient and lightweight detection mechanisms are essential to maintain the reliability and availability of WSN systems.

In this study, a lightweight machine learning approach was proposed to detect DoS attacks in Wireless Sensor Networks. Several machine learning algorithms, including Decision Tree, Logistic Regression, Naïve Bayes, and Random Forest, were analyzed to identify the most suitable method for resource-constrained environments. The experimental results indicate that Decision Tree and Random Forest algorithms provide a good balance between detection accuracy, computational efficiency, and processing speed. The proposed approach effectively distinguishes between normal and malicious network traffic while maintaining low computational overhead.

Overall, the study demonstrates that lightweight machine learning techniques can significantly improve the security of wireless sensor networks without imposing heavy resource requirements. The proposed model can help

enhance the reliability, efficiency, and security of WSN-based systems deployed in critical applications.

Future Scope

Although the proposed approach shows promising results, several improvements can be explored in future research. First, advanced feature selection techniques can be applied to further reduce computational complexity and improve detection performance. Second, deep learning or hybrid machine learning models can be investigated to enhance the detection of more complex and evolving attack patterns.

In addition, future work can focus on implementing the proposed model directly on real sensor hardware or edge devices to evaluate its performance in real-time WSN environments. Integration with other security mechanisms such as encryption, trust management, and blockchain-based frameworks could further strengthen network security. Finally, expanding the model to detect multiple types of cyber-attacks beyond DoS attacks will improve the overall robustness and adaptability of wireless sensor network security systems.

REFERENCES

- [1] G. Al Sukkar and S. Al-Sharaeh, "Enhancing security in wireless sensor networks: A machine learning-based DoS attack detection," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19712–19719, 2025.
- [2] B. Kaur, D. Prashar, and L. Masic, "Enhancing the reliability and accuracy of wireless sensor networks using a deep learning and blockchain approach with DV-HOP algorithm for DDoS mitigation," *Journal on Wireless Communications and Networking*, vol. 2025, pp. 1–18, 2025.
- [3] S. Joo, S. Park, H. Shim, Y. Oh, and I. Lee, "Machine learning-based detection and selective mitigation of denial-of-service attacks in wireless sensor networks," *Computers, Materials & Continua*, vol. 82, no. 2, pp. 2475–2494, 2025.
- [4] A. Sharma and S. Rani, "An optimized ensemble approach for securing wireless sensor

networks against attacks,” ICCK Transactions on Wireless Networks, vol. 1, no. 1, pp. 5–15, 2025.

[5] T. Thanigaivel, S. Venkatesh, M. Monish, and T. Gobinath, “A machine learning-driven framework for DoS attack detection in cluster-based wireless sensor networks,” International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 3, pp. 1–8, 2025.

[6] H. Barati, “A quantum genetic algorithm-enhanced self-supervised intrusion detection system for wireless sensor networks in IoT,” arXiv preprint, 2025.

[7] M. M. Alhusseini and M. R. F. Derakhshi, “Hybrid AI-driven intrusion detection framework leveraging feature selection for enhanced network security,” arXiv preprint, 2025.

[8] C. Panggabean, C. Venkatachalam, P. Shah, S. John, R. Devi, and S. Venkatachalam, “Intelligent DoS and DDoS detection using hybrid GRU-NTM deep learning model,” arXiv preprint, 2025.

[9] M.-L. A. Bartsioka, I. A. Bartsiokas, P. K. Gkonis, D. I. Kaklamani, and I. S. Venieris, “Machine learning enabled eavesdropper detection in beyond-5G IIoT networks,” arXiv preprint, 2025.

[10] D. Sethi, M. Gora, S. Jain, S. Kumari, S. Gupta, and T. Tyagi, “Implementing wireless sensor networks through machine learning techniques,” Recent Patents on Engineering, vol. 15, no. 3, pp. 268–280, 2025.

[11] S. Mends and K. S. Adu-Manu, “Evaluating machine learning efficacy for DoS intrusion detection in wireless sensor networks,” International Journal of Wireless and Microwave Technologies, vol. 16, no. 1, pp. 1–23, 2026.

[12] N. Jagwani and P. G., “Machine learning algorithms to detect attacks in wireless sensor networks,” International Journal of Intelligent Systems and Applications in Engineering, vol. 12, pp. 417–426, 2024.

[13] S. Salmi and L. Oughdir, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network,” Journal of Big Data, vol. 10, pp. 1–17, 2023.

[14] M. A. Elsadig, “Detection of denial-of-service attack in wireless sensor networks using lightweight machine learning approach,” IEEE Access, pp. 1–10, 2025.

[15] S. Kumar and R. Patel, “Lightweight intrusion detection system for wireless sensor networks using machine learning techniques,” International Journal of Network Security, vol. 27, no. 2, pp. 150–160, 2025..