Cureus Journal of Computer Science

Open Access Original Article

A Hybrid Rule-Based and Machine Learning Approach for Distributed Denial of Service (DDoS) Attack Detection and Mitigation in Wireless Sensor Network–Enabled Smart Healthcare Systems

Received 01/20/2026
Review began 01/22/2026
Review ended 02/12/2026
Published 02/20/2026

DOI:
https://doi.org/10.7759/s44389-026-00030-0

Pushpa Singh [1] , Shalini Swami [2]

1. Department of Computer Science & Engineering, G.L. Bajaj Institute of Technology & Management, Greater Noida, IND 2. Department of Information Technology, Noida Institute of Engineering and Technology, Greater Noida, IND

Corresponding author: Pushpa Singh, pushpa.gla@gmail.com

Abstract

This paper presents a rule-based and machine learning (ML)-driven technique for the efficient detection of Distributed Denial of Service (DDoS) attacks in healthcare wireless sensor networks (WSNs). The proposed method involves design and analysis of various rules on extracted features of the WSN-DS dataset. The rule-based approach selects efficient rules to identify normal flow, and in case of suspicious flow, ML techniques are utilised to identify types of DDoS attacks, such as “Blackhole”, “Flooding”, “Grayhole”, and “TDMA.” Decision Tree, Support Vector Machine classifiers, Gaussian Naïve Bayes, and K-Nearest Neighbour are applied to evaluate the accuracy of the model. The rule-based classifier effectively differentiates normal and suspicious traffic, with an accuracy of 97.29%. Following detection, the decision tree classifier attains the highest accuracy - 99.43% - in classifying the various DDoS attack types. After identifying the specific variant of the DDoS attack, appropriate mitigation strategies can be effectively implemented. The proposed method introduces simple rules to classify normal and suspicious traffic flows. These rules are computationally lightweight and therefore help to reduce the overall cost of the intrusion detection system. The proposed method enhances the security of healthcare WSN/wireless body area network, highlighting its potential for real-world application in safeguarding healthcare infrastructure against DDoS attacks.

Categories: Safe and trustworthy AI in healthcare, Machine Learning (ML), AI/ML-based decision support systems
Keywords: wireless sensor network, machine learning, denial of services attacks, rule-based, intrusion detection system

Introduction

Wireless Body Area Sensor Network (WBAN) and Body Area Network (BAN) are two utilities that play an important role in analyzing patient vitals remotely or locally. These networks enable healthcare systems to monitor and gather important patient data in real-time for further investigation to diagnose, treat, and manage patient histories [1]. The main difference between WBAN and BAN is that WBAN can be monitored through local wireless through the internet in remote locations, and BAN works with physically attached equipment within the device in the room. Security is very important for the sensor network environment because WBAN is connected with this network, and hence, it directly affects the patient’s health monitoring. However, the protocol and algorithm as used in traditional wireless sensor networks (WSNs) setups are not feasible in WBAN due to distinct applications and attributes. A BAN environment is a small setup of nodes. Nodes are placed in the human body. Usually, these are mobile in nature nodes and mainly used for remote monitoring. BAN uses the IEEE 802.1x standard for communication, which is mainly used for short distances, requires less power, and is reliable. WBAN has various security challenges due to resource constraints. The main challenge in this network is to collect bio-signals data of the patient without any security breach. Data is the most important part of this network because it is directly related to a patient's life [2]. The architecture of WBAN is basically divided into four layers for communication, and all these layers have their security requirements, including in-body, on-body, and off-body communication.

Layer 1 is used to communicate within the body and is equipped with sensor nodes such as nanodevices implanted in the body. Layer 2 is used in the communication between in/on-body sensors and nodes. Layer 3 is used to share data between wearable nodes and centre units like Wi-Fi, Bluetooth, Zigbee, etc. Layer 4 involves communication between the centre unit and healthcare servers, such as wifi and IEEE 802.x standards. Major security threats in this network are Denial of Service (DoS) attacks, modification in data, and spoofing. In WBAN, security solutions emphasise authentication of data, integration, and availability. WBANs must be secured from Distributed Denial of Service (DDoS) attacks because they handle critical real-time health data of the patient, and any interruption can endanger patient safety. WBAN networks consist of resource-constrained sensor nodes that can easily be exhausted by excessive

How to cite this article
Singh P, Swami S (February 20, 2026) A Hybrid Rule-Based and Machine Learning Approach for Distributed Denial of Service (DDoS) Attack Detection and Mitigation in Wireless Sensor Network–Enabled Smart Healthcare Systems. Cureus J Comput Sci 3 : es44389-026-00030-0. DOI https://doi.org/10.7759/s44389-026-00030-0

traffic. A DDoS attack can also disconnect patients from essential medical services, affecting the reliability and trust of healthcare systems. Hence, it is significant to prevent WBAN from DDoS attacks using an intrusion detection mechanism to enhance communication channels. Integration of data depends upon authentication. There are various mechanisms implied to protect against unauthorised access, such as only admins deciding to grant legitimate users access, no permission for users to change their access rights, defining access roles for every user, and providing access key encryption on the basis of their role in the organization. All these solutions depend upon the needs of the organization to address issues and privacy concerns of the WBAN [3].

There are several security issues explained in [4-5] that lead to DoS and DDoS attacks in the network. These involve botnet infrastructures, inadequate safety upgrades, a lack of network protocols, improper authentication, etc. DDoS poses significant risks to data security, disrupting patient care and causing financial losses and operational chaos [6-7]. These attacks stop the communication between patients and hospitals, which leads to compromised patient health. Additionally, DoS/DDoS attacks can result in data security breaches, operational disruptions, and financial losses within the organization. Integration of technologies in healthcare helps the end user and healthcare system but is also prone to a range of security threats against patient information, vital resources, and other operations involved.

The role of the Intrusion Detection System (IDS) in DoS attacks is to analyze traffic flow to gain prior knowledge about abnormal behavior. Additionally, IDS contributes to the security, integrity, and accuracy of the patient data by solving the issues at both the data and network levels. This helps to build trust of patients in the healthcare system [8]. However, the use of various machine learning (ML) and rule-based techniques is suggested to address security threats in the healthcare system. Rule-based systems work on predefined rules and patterns to detect and reduce the effect of the attacks and help to enhance the security by analyzing traffic flow and the behavior of the system and help to automate the security parameters like intrusion detection, access control, etc. Meanwhile, ML inspects past collected data to detect the patterns that are used to find security breaches and improve threat detection capabilities. ML models trained from the previous attack data help to identify threats in real time, which increases the improvement in threat mitigation [9].

Types of DDoS attacks

Several variants of DDoS attacks are blackhole attack, flooding attack, grayhole attack, and Time Division Multiple Access (TDMA) attack. This subsection describes the types of DDoS attacks in the healthcare system.

Blackhole Attack: A malicious node that absorbs all incoming packets and drops them rather than forwarding them to the right place. A Blackhole attack from the perspective of healthcare can happen if a node deviously advertises the shortest path from a hospital server to a doctor's console and then silently drops all the received packets. Early detection of a black hole attack may secure the digital healthcare system. Hence, defense and mitigation strategies against black hole and selective forwarding attacks for medical WSNs in the IoT devices are required [10].

Flooding Attack: An attacker injects extreme fake packets to exhaust the network resources. In WBAN, routing is supported via the coordination and connection of the nodes. An attacker may send a lot of requests or a flood of requests to establish a TCP connection to use all WBAN resources [11].

Grayhole Attack: A selective forwarding attack where a node intermittently drops packets. In IoMT , a grayhole attack occurs when an attacker compromises a sensor or relay node in the network and selectively starts dropping packets of certain types of data while forwarding other types of data. This ensures that the attacker avoids detection while compromising the reliable delivery of vital health data. This selective dropping of network data may result in an incorrect patient status interpretation and may risk the lives of patients dramatically [12].

TDMA-Based Attacks: Exploitation of TDMA slot allocation or synchronisation (e.g., slot misuse, jamming). The misbehaving node may transmit in a slot other than its assigned slot or keep silent during critical slots, leading to packet collisions, delays, or loss of vital health information. Due to this, crucial physiological signals, like ECG signals or emergency alerts, may not reach the medical server on time, which can lead to erroneous patient monitoring and delayed clinical decisions.

It is important to accurately identify these types of DDoS attacks in the digital healthcare system so that appropriate mitigation techniques can be applied effectively. The proposed methods developed an effective way of detecting types of DDoS attacks in WBANs. The proposed work involves identifying security threats, developing Rule-ML-based classifiers, and using ML-based classifiers to classify the types of DDoS attacks. So that effective mitigation techniques can be applied immediately just after the detection of the attack.

Hence, the aim of this paper is to implement an effective IDS to detect DDoS attack types in a remote healthcare system. This enhances the security, data integrity, and system reliability of patients' data.

Materials And Methods

Literature survey

As the usage of the internet increases, WBAN systems are key for healthcare systems that facilitate remote patient monitoring and emergency responses [13-14]. However, because the communication medium is wireless, they are susceptible to various attacks [15-16]. Out of these attacks, DDoS attacks are one of the biggest cyber attacks [17]. The author explained that these attacks overwhelm networks, delay access, and make systems vulnerable to exploitation. There is a need for cybersecurity management to mitigate the impact of attacks in the healthcare system. The main objective of the paper was to address research gaps in long-term security sustainability and strength in BANs [18]. The trust-based IDS detects and prevents Denial of Sleep attacks in WBAN by picking random keys, passwords, and node values and also takes data of energy consumption and an agent database. The author explained that to protect the network against security threats, various methods are used, such as IDS, authentication, encryption, etc., and each with its advantages and limitations [19]. The study proposed that Decision Tree (DT) and XGBoost outperform in detecting DoS in WSN and achieve a higher true positive rate and lower false positive rate across different datasets. It helps in enhancing WSN security against such attacks [20]. Salmi and Oughdir [21] presented a deep learning technique to detect DoS attacks in a wireless network with the highest accuracy of 98.79%. Furthermore, supervised ML algorithms are proven to be the best for DDoS attack detection [22].

IoT-based remote healthcare systems focus on preventive healthcare and provide high-quality medical services [23]. IoT devices, when utilized in medical equipment, are referred to as Internet of Medical Things devices. Internet of Medical Things devices are prone to becoming botnets for launching complex multi-vector DDoS attacks [24]. Kumavat and Gomes [25] presented a multi-layer tree-based model to identify attackers, DoS attacks, and their root cause. A TCN-based DDoS detection and mitigation mechanism in the healthcare system was presented by Akhi et al. [26]. However, the types of DDoS attacks remain to be explored. Due to the relative ease of deployment of DDoS attacks, their high effectiveness, and the difficulty in stopping them, DDoS attacks are becoming common and need to be identified and mitigated. Hence, high-quality health services will be possible when the network is secure and free from threats and attacks. The major contribution of this paper is designing a rule-ML-based IDS to detect DoS attacks. Extract the important feature from WSN-DS that is suitable for designing the rule. Analysis of the suitability of the rule-based and ML classifiers.

Proposed rule - ML-based techniques for DDOS attack detection

This study considers a healthcare-oriented wireless sensing framework that integrates both WSN and WBAN. WBAN nodes are deployed on or around patients to continuously collect physical data, while the WSN infrastructure enables multi-hop communication between WBAN gateways and the central monitoring server (healthcare server). Within this environment, the network traffic is exposed to various security threats, including DDoS, which can severely disrupt data availability and reliability. To address these challenges, an IDS is integrated to monitor network traffic behavior and identify malicious activities using rule-based and ML-driven techniques.

The proposed work represents the integration of rule-based and ML-based methods that help to detect normal traffic and attacks and their type. We used the proposed rule in an IDS-enabled healthcare system, as depicted in Figure *1*.

FIGURE 1: Proposed rule - ML-based techniques for DDoS attacks detection

ML, Machine Learning; IDS, Intrusion Detection System

The proposed systems presented secure and efficient operations in WBAN in healthcare by employing the combination of a rule-based classifier and an ML-based classifier. To examine the patient remotely or within the premises, there is a need for sensors that are attached to the patient to collect the health-related data, such as bloop pressure, heart rate, and other essential data to monitor the patient in real time. Vital information of the patient is sent through the local network as a gateway through the public network to the healthcare server. The IDS imposes its two components, rule-based and ML-based classifiers, on the incoming data to analyze the incoming traffic patterns to identify normal flow and attacks. The IDS works as a firewall that first analyzes the traffic and then takes possible action. Rule-based utilized to detect normal flow and attacks. If the rule-based method detects normal flow, then the

data is transmitted to healthcare staff, such as doctors and paramedical staff. If an attack is detected on the basis of known patterns, mainly DDoS attacks, an ML classifier is used to label the attack type (Blackhole, Grayhole, Flooding, Scheduling). Administrative bodies continuously monitor the incoming data; if any anomaly is detected, they stop transmitting data and take mitigation steps to alert the system. The proposed work has two important modules. One module is a rule-based classifier, and the other is an ML-based classifier. Both modules are based on and utilize the WSN-DS dataset.

WSN-DS dataset

WSN-DS is widely used for evaluating ML-based intrusion detection techniques in resource-constrained sensor networks [27]. The dataset includes labelled instances of normal traffic as well as multiple attack scenarios such as DDoS: grayhole, flooding, and TDMA-based attacks, making it suitable for training and validating IDS models in healthcare-oriented WSN and WBAN environments. This dataset consists of 374,661 records and 19 features. Descriptions of 19 features are given in [24]. The distribution of records in the dataset is as follows: “Normal - 340,066”, “Grayhole - 14,596”, “Blackhole - 110,049,” “TDMA - 6,638”, and “Flooding - 3,312” and their percentage distribution is 90.77%, 3.90%, 2.68%, 1.77%, and 0.88%, respectively. Preprocessing is significant to find the noise or null values in the dataset. Also, it is used to check whether the dataset is balanced or not. WSN-DS is not a balanced dataset. Here, “normal” values are in the range of “340,066 out of 374,661,” and the rest are “attacks.” Also, our proposed approach will balance the dataset. This is because in the proposed approach, the “normal” flow will be identified using the rule-based classifier.

Rule-based classifier

To create a rule-based system, we required relevant features. Hence, we need feature extraction methods to check whether they are relevant or not. Feature selection is the process of extracting the important features that help to increase the accuracy.

Methods used for feature selection are extracted from the WSN-DS [27] dataset: information gain and Gini index for statistical measures and principle component analysis for orthogonal components to capture maximum variance in the dataset [28]. We have created four rules to separate normal flow and suspicious flow (attack). Rules are created by using simple if-then-else conditions. Out of all the rules, we found that the combination of rule 1 and rule 2, which we name as rule 3 and rule 4, gives the highest accuracy to detect attacks and separate normal flow, as shown in Table *1*. Hence, we will apply rule 4 to classify the traffic flow. Rule-based is simple and easy to apply; moreover, the computation is less complex. In the above rule 1, index1=4 indicates the current column no. 5 in the WSN-DS dataset; the corresponding name of the column is “Dist_To_CH”. Similarly, in rule 2, the corresponding value in the dataset, i.e., index2=12, represents the current column no. 13. The name of the corresponding column is “DATA_S,” and values[index1] specifies the values in the respective columns. Similarly, values[index2] specifies the values in the respective columns. The rule-based classifier classifies the details of whether the received traffic is “normal” or the traffic is an “attack,” thereby passing the classifier to save computational time.

S. no.	Rules	Accuracy (%)
Rule 1	if index1 == 4 and values[index1] > 0 then return "Normal" else “attack”.	85.79%
Rule 2	if index1 == 4 and values[index1] == 0 && index2 ==12 and values[index2] >2 then return "Normal", else “attack”.	11.43%
Rule 3	Combine Rule 1 && Rule 2	97.22%
Rule 4	If index1 == 5 && values[index1] = 0 then return "Normal", else “attack”.	97.29%

TABLE 1: List of rules

The rule-based classifier is computationally efficient for identifying traffic patterns as normal or malicious. Since the WSN-DS dataset is an imbalanced dataset, rule-based techniques can easily separate the “normal” and “suspicious” traffic flow. Furthermore, the system must also mitigate the attack after identifying its type, which becomes feasible when the specific type of DDoS attack, such as Blackhole, Flooding, Grayhole, or TDMA, is accurately classified.

ML-based classifier

Furthermore, ML-based classifiers are applied to detect types of DDoS attacks, as briefly explained as a subsection of the introduction. It is important to accurately identify these types of DDoS attacks so that appropriate mitigation techniques can be applied effectively. We have used various well-known ML classifiers to train and test the models. DT, K-Nearest Neighbor, Support Vector Machine, and Gaussian

Naïve Bayes have been applied for finding the best suitable model to predict the types of DDoS attacks. The accuracy of each applied model is displayed in Table 2 at split point 0.2 and 0.3.

ML model names	Model overall accuracy at split point 0.2	Model overall accuracy at split point 0.3
DT	99.43%	99.36%
KNN	95.63%	95.27%
Gaussian NB	79.21%	79.20%
SVM	72.06%	71.81%

TABLE 2: Model analysis on ML-based classifier

DT, Decision Tree; KNN, K-Nearest Neighbors; ML, Machine Learning; NB, Naive Bayes; SVM, Support Vector Machine

These ML-based classifiers are implemented within the IDS to determine whether the traffic flow is "normal" or an "attack." If the proposed IDS detects an attack, it is essential to identify the specific type of DoS attack so that appropriate mitigation techniques can be applied. The DT classifier is used to detect the type of DoS attack.

Results And Discussion

Experiment setup

The experiment has been performed using the WSN-DS dataset, and the classifier is implemented in Python. Data processing and model development were carried out using standard Python libraries, including NumPy, Pandas, Scikit-learn, and the Google Colab editor. The dataset was evaluated using train-test split ratios of 0.2 and 0.3. A DT classifier was used as the primary model, along with Support Vector Machine, K-Nearest Neighbor, and Naïve Bayes for comparative analysis. Model performance was measured using overall classification accuracy and various ML classifiers, and the result is shown in Table 2.

Model experimental analysis

First of all, a rule-based classifier is applied (see Table 1) to check that the flow is "normal" or "attack." If the proposed IDS finds an attack, then it is very significant to identify the type of DDoS attack so that suitable mitigation techniques can be applied. An ML-based DT classifier is applied to detect the type of DDoS label. An ML-based DT classifier is applied to detect the type of DDoS variant/types. To further analyze the DT classifier, the model was evaluated using different splitting criteria, namely the Gini index and entropy, along with varying random_state values, as presented in Table 3 with the corresponding accuracy results.

DT with or without parameter		
Decision Tree	Model overall accuracy default criterion = 'gini'	Model overall accuracy criterion = 'entropy'
DT criterion = 'gini/entropy'	99.29%	99.39%
DT criterion = 'gini/entropy', random_state = 42	99.34%	99.43%

TABLE 3: Model analysis on decision tree (DT) classifier

Figure 2 represents the confusion matrix that was used to summarize the performance of a DT classifier. The matrix provided the insight information between actual labels and predicted labels. The performance metrics of the classifier are represented in terms of precision, recall, F1 score, and accuracy of each type of DDoS attack, as shown in Table 4. This approach not only improves detection performance but also strengthens the resilience of healthcare sensor networks against evolving cyberattacks.

FIGURE 2: Confusion matrix of the decision tree

TDMA, Time Division Multiple Access

Decision Tree				
Types of DDoS Attacks	Precision	Recall	f1-score	Accuracy (%)
Blackhole	0.99	0.99	0.99	99%
Flooding	1.00	1.00	1.00	100%
Grayhole	0.99	0.99	0.99	99%
TDMA	1.00	1.00	1.00	100%

TABLE 4: Classification report of decision tree

DDoS, Distributed Denial of Service; TDMA, Time Division Multiple Access

After identifying the types of DDoS attacks, IDS can transition towards efficient mitigation techniques.

Mitigation strategies

Mitigation Strategies for Blackhole Attack

Secure routing protocols and trust-based assessment techniques have the potential to mitigate blackhole attacks. These techniques assess packet forwarding behavior to identify malicious nodes. Authenticated Routing for Ad hoc Networks, Secure Ad hoc On-Demand Distance Vector [29], and Secure Efficient Ad hoc Distance Vector, etc., are well-known secure routing protocols. Trust-Aware Routing Frameworks is very effective against blackhole and grayhole attacks. The proposed ML-based IDS can detect abnormal routing advertisements and enable the isolation of malicious nodes. These techniques assess packet forwarding behavior to identify malicious nodes. The proposed ML-based IDS can detect abnormal routing advertisements and enable the isolation of malicious nodes.

Mitigation Strategies for Flood Attacks

Flooding attacks are generally mitigated using rate-limiting mechanisms [30], secure routing protocols, trust-based routing frameworks, REWARD-based suppression techniques [31], etc., which are used to identify and isolate nodes generating excessive traffic.

Mitigation Strategies of Grayhole Attack

Grayhole attacks usually drop packets selectively and can be mitigated by using multipath acknowledgement schemes, which could validate the successful forwarding of packets along with dynamic rerouting around suspected nodes; statistical clustering approaches that isolate nodes with anomalous forwarding rates; hybrid detection frameworks [32] that combine anomaly and cryptographic checks for improving the accuracy of detection; and finally trust/reputation systems that make routing adaptive to the observed node behavior.

Mitigation Strategies for TDMA Attacks

An efficient mitigation strategy for TDMA attacks comprises a dynamic scheduling approach, an anti-jamming approach, a time synchronisation method, and a cross-layer redundancy feature. The anti-jamming feature, spread-spectrum communication, and time randomization place additional restrictions on attackers' attempts to disrupt TDMA schedules. The time synchronization method ensures time slot maintenance in the occurrence of a TDMA attack, and the use of cross-layer and IDS-based detection techniques enables early recognition of time anomalies.

Some available texts on mitigation strategies are discussed in Table *5*, thereby ensuring the availability of healthcare services and protecting patient-critical data.

DDoS attack type	Mitigation techniques
Blackhole Attack [29-32]	• Secure routing protocols (SAODV, ARAN) • Multipath routing • Monitoring of packet forwarding behaviour
Flooding Attack [30-33]	• Rate limiting • Trust-based Techniques • Reward-based Techniques
Grayhole Attack [32-34]	• Watchdog monitoring • 2ACK acknowledgement schemes • Statistical clustering approaches • Multipath routing
TDMA-Based Attacks [35,36]	• Time synchronisation • Dynamic slot assignment/dynamic scheduling • Secure synchronisation • Anti-jamming approach • Cross-layer redundancy feature

TABLE 5: Mitigation strategies for DDoS

ARAN, Authenticated Routing for Ad hoc Networks; DDoS, Distributed Denial of Service; SAODV, Secure Ad hoc On-Demand Distance Vector; TDMA, Time Division Multiple Access

Overall, the experimental analysis confirms that the selected classifiers perform reliably on the WSN-DS dataset, with DT emerging as a competitive and interpretable model for intrusion detection. The observed trends across different split points validate the robustness of the experimental setup and the effectiveness of the proposed approach.

Conclusions

Proposed rule-based and ML-based IDS significantly enhance the accuracy and efficiency of DDoS attack detection in wireless sensor environments used for healthcare. The proposed model first detects the suspicious traffic flow (DDoS attack) based on a rule. Using a DT classifier, the proposed model achieves a maximum accuracy of 99.43%, making it highly effective for safeguarding WBAN-based healthcare systems. DT classifies the categories of DDoS attacks, which include “Blackhole”, “Flooding”, “Grayhole”, and “TDMA.” So that appropriate mitigation strategies can be applied effectively to counter various types of evolving DDoS attacks. The model is further extended by outlining the mitigation strategies that the proposed system can apply based on the detected DDoS attack, enabling timely and appropriate responses to evolving cyber threats.

This study has certain limitations. The evaluation relies on a WSN-DS dataset, which may not fully reflect real healthcare network conditions. The rule-based classifier depends on predefined rules applied to the WSN-DS dataset that may not adapt well to progressing attack patterns. Similarly, the DT classifier may face generalisation challenges when exposed to unseen or highly sophisticated DDoS variants. Additionally, mitigation strategies are not described, and real-time performance in healthcare environments has not extensively tested. Future work will focus on generalising the rules, real-world traffic validation, and wider experimental simulation and testing of healthcare systems.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Pushpa Singh, Shalini Swami

Acquisition, analysis, or interpretation of data: Pushpa Singh, Shalini Swami

Drafting of the manuscript: Pushpa Singh, Shalini Swami

Critical review of the manuscript for important intellectual content: Pushpa Singh, Shalini Swami

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there

are no other relationships or activities that could appear to have influenced the submitted work.

Data Availability Statements

The datasets (and/or code) supporting this study are available from the corresponding author upon reasonable request.
The data (and/or code) supporting this study are openly available in {REPOSITORY} at {DOI/URL}, reference {ACCESSION ID}.
All data generated or analyzed during this study are included in this published article and/or its appendices.
Data sharing is not applicable. This work is theoretical; no datasets were generated or analyzed.

References

1. Akbar MS, Hussain Z, Sheng M, Shankaran R: Wireless body area sensor networks: Survey of MAC and routing protocols for patient monitoring under IEEE 802.15.4 and IEEE 802.15.6. Sensors. 2022, 22:8279. 10.3390/s22218279
2. Yaghoubi M, Ahmed K, Miao Y: Wireless body area network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. Journal of Sensor and Actuator Networks. 2022, 11:67. 10.3390/jsan11040067
3. Roy M, Chowdhury C, Aslam N: Security and privacy issues in wireless sensor and body area networks. Handbook of Computer Networks and Cyber Security. Gupta B, Perez G, Agrawal D, Gupta D (ed): Springer, Cham; 2020. 173-200. 10.1007/978-3-030-22277-2_7
4. ul Sami I, Ahmad MB, Asif M, Ullah R: DoS/DDoS detection for E-healthcare in internet of things. International Journal of Advanced Computer Science and Applications. 2018, 9:297-300. 10.14569/ijacsa.2018.090140
5. Mihoub A, Ben Fredj O, Cheikhrouhou O, Derhab A, Krichen M: Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering. 2022, 98:107716. 10.1016/j.compeleceng.2022.107716
6. Joshua ESN, Bhattacharyya D, Rao NT: Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: a complete systematic approach. Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems. Karaca Y, Baleanu D, Zhang YD, Gervasi O, Moonis M (ed): Academic Press, London; 2022. 291-310. 10.1016/B978-0-323-90032-4.00007-9
7. Wazzan M, Algazzawi D, Bamasaq O, Albeshri A, Cheng L: Internet of Things botnet detection approaches: Analysis and recommendations for future research. Applied Sciences. 2021, 11:5713. 10.3390/app11125713
8. Yang Y-M, Chang K-C, Luo J-N: Hybrid neural network-based intrusion detection system: Leveraging LightGBM and MobileNetV2 for IoT security. Symmetry. 2025, 17:314. 10.3390/sym17030314
9. Al-Turjman F, Baali I: Machine learning for wearable IoT-based applications: A survey. Transactions on Emerging Telecommunications Technologies. 2022, 33:e3635. 10.1002/ett.3635
10. Mathur A, Newe T, Rao M: Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. Sensors. 2016, 16:118. 10.3390/s16010118
11. Asam M, Jamal T, Adeel M, Hassan A, Butt SA, Ajaz A, Gulzar M: Challenges in wireless body area network. International Journal of Advanced Computer Science and Applications. 2019, 10:336-341. 10.14569/ijacsa.2019.0101147
12. Fasunlade O, Zhou S, Sanders D: Security threats and possible countermeasure in digital healthcare. 2021 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA. 2021, 1297-1302. 10.1109/CSCI54926.2021.00265
13. Chakraborty C, Gupta B, Ghosh SK: A review on telemedicine-based WBAN framework for patient monitoring. Telemedicine and e-Health. 2013, 19:619-626. 10.1089/tmj.2012.0215
14. Majeed JH, Aish Q: A remote patient monitoring based on WBAN implementation with internet of thing and cloud server. Bulletin of Electrical Engineering and Informatics. 2021, 10:1640-1647. 10.11591/eei.v10i3.1813
15. Hasan MK, Ahasan Habib AKM, Islam S, Safie N, Sheikh Abdullah SNH, Pandey B: DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. Energy Reports. 2023, 9:1318-1326. 10.1016/j.egyr.2023.05.184
16. Ul Islam MN, Fahmin A, Hossain MS, Atiquzzaman M: Denial-of-service attacks on wireless sensor network and defense techniques. Wireless Personal Communications. 2021, 116:1993-2021. 10.1007/s11277-020-07776-3
17. De Neira AB, Kantarci B, Nogueira M: Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks. 2023, 222:109553. 10.1016/j.comnet.2022.109553
18. Ananthi JV, Jose PSH: A perspective review of security challenges in body area networks for healthcare applications. International Journal of Wireless Information Networks. 2021, 28:451-466. 10.1007/s10776-021-00538-3
19. Jebur TK: Securing wireless sensor networks, types of attacks, and detection/prevention techniques, an educational perspective. ASEAN Journal of Science and Engineering Education. 2024, 4:43-50. 10.17509/ajsee.v4i1.57431
20. Abidoye AP, Obagbuwa IC, Azeez NA: Mitigating denial of service attacks in fog-based wireless sensor networks using machine learning techniques. Journal of Data, Information and Management. 2023, 5:207-225. 10.1007/s42488-023-00100-1
21. Salmi S, Oughdir L: Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data. 2023, 10:17. 10.1186/s40537-023-00692-w
22. Abiramasundari S, Ramaswamy V: Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms. Scientific Reports. 2025, 15:13098. 10.1038/s41598-024-84879-y
23. Li C, Wang J, Wang S, Zhang Y: A review of IoT applications in healthcare. Neurocomputing. 2024, 565:127017. 10.1016/j.neucom.2023.127017
24. Aguru AD, Erukala SB: A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning. Information Sciences. 2024, 662:120209. 10.1016/j.ins.2024.120209

25. Kumavat KS, Gomes J: Multi-layer DDoS attacks detection with mitigation in IoT-enabled sensor network. Cybersecurity. 2025, 8:72. 10.1186/s42400-025-00378-1
26. Akhi M, Eising C, Dhirani LL: TCN-based DDoS detection and mitigation in 5G healthcare-IoT: A frequency monitoring and dynamic threshold approach. IEEE Access. 2025, 13:12709-12733. 10.1109/access.2025.3531659
27. Almomani I, Al-Kasasbeh B, Al-Akhras M: WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors. 2016, 2016:4731953. 10.1155/2016/4731953
28. Swami S, Singh P, Chauhan SS: Design and analysis of an integrated rule-based and machine learning system for DoS attack detection in wireless sensor networks. 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India. 2024, 1046-1052. 10.1109/IC3SE62002.2024.10593610
29. Nakano Y, Matsuzawa T: Preventing black hole attacks in AODV using RREQ packets. Network. 2023, 3:469-481. 10.3390/network3040020
30. Pramodh Krishna D, Sandhya E, Shareef Sk K, et al.: Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection. Scientific Reports. 2025, 15:818. 10.1038/s41598-024-84421-0
31. Ahmed B: A comprehensive review of recent types of flooding attack and defense methods in IoT-based smart environments. Journal of Soft Computing and Data Mining. 2024, 5:110-136.
32. Yazdanypoor M, Cirillo S, Solimando G: Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks. Applied Sciences. 2024, 14:7982. 10.3390/app14177982
33. Wang H, Zhang D, Shin KG: Detecting SYN flooding attacks. Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, New York, NY, USA. 2002, 1530-1539. 10.1109/INFCOM.2002.1019404
34. Cho Y, Qu G: A hybrid trust model against insider packet drop attacks in wireless sensor networks. Sensors. 2023, 23:4407. 10.3390/s23094407
35. Samaddar A, Easwaran A, Tan R: A schedule randomization policy to mitigate timing attacks in WirelessHART networks. Real-Time Systems. 2020, 56:452-489. 10.1007/s11241-020-09354-z
36. Mohammadani KH, Memon KA, Memon I, Hussaini NN, Fazal H: Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks. International Journal of Distributed Sensor Networks. 2020, 16:1-18. 10.1177/1550147720921624