Al-Noor Journal of Engineering Management and Computer Science

ISSN: 3079-0689 (Online)

https://njemcs.edu.iq/index.php/njemcs/

Comprehensive Analysis of Classification Algorithms in Wireless Body Area Networks: Advanced Techniques for Securing and Optimizing Trustworthy Node Identification

Israa Ibraheem Al Barazanchi [1,2,*], Ali Adham[3], Wahidah Hashim [1], Reema Thabit [1] , Mashary Nawwaf Alrasheedy[4,5]

[1]College of Computing and Informatics, Universiti Tenaga Nasional (UNITEN), 43000 Kajang, Selangor, Malaysia.
[2] College of Engineering, University of Warith Al-Anbiyaa, Karbala, Iraq
[3] Iraqi Society of Engineering Management [b]
[4]Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, 43600 Bangi Selangor, MALAYSIA
[5]Department of Computer Science, Applied College, university of Hail, P.O.Box 2440, Hail, 55424, Saudi Arabia

ARTICLE INFO

Article history:
Received 05 November 2024
Revised 05 November 2024
Accepted 10 November 2024
Available online 10 November 2024

Keywords:
Wireless Body Area Networks,
Node Classification,
Security and Privacy,
Machine Learning,
Trustworthiness,
Energy Efficiency

ABSTRACT

Wireless Body Area Networks (WBANs) have become essential in healthcare, fitness, and emergency monitoring, where they support real-time data collection and transmission from wearable or implantable sensors. However, the effectiveness of WBANs depends heavily on reliable and secure node classification, as these networks face numerous challenges, including data integrity issues, privacy concerns, and resource constraints. This study addresses the critical problem of accurately and securely classifying nodes in WBANs to ensure that only trusted data sources contribute to network operations, thus minimizing risks related to data breaches, energy inefficiency, and misclassification. The primary objective of this study is to analyze and evaluate various classification algorithms—ranging from traditional machine learning techniques to advanced AI models—within the context of WBANs. Additionally, this study explores methods to enhance WBAN security and optimize resource consumption, focusing on power efficiency, latency reduction, and error mitigation. Our contributions include a comparative analysis of different algorithms based on performance metrics such as accuracy, precision, recall, F1 score, energy efficiency, and robustness. We also introduce a framework for incorporating security-enhanced classification techniques, such as encryption, data anonymization, and authentication, to safeguard WBAN data and maintain network integrity. By providing a comprehensive overview of current challenges and advanced classification methods, this study aims to inform the development of scalable, secure, and efficient classification models tailored to WBANs. Our findings underscore the importance of balancing accuracy, energy efficiency, and security to create WBAN systems that are both trustworthy and adaptable. This research contributes to the ongoing evolution of WBAN technology, paving the way for improved reliability in applications that demand high standards of data integrity and real-time monitoring.

1. Introduction

Wireless Body Area Networks (WBANs) are specialized networks designed to support continuous health monitoring and data transmission through small, wearable devices placed on or within the human body [1]. These

Corresponding author E-mail address: israa.albarazanchi2023@gmail.com

networks consist of various sensors that monitor physiological parameters, such as heart rate, blood pressure, body temperature, and movement patterns. These sensors are connected to a central hub, which aggregates and transmits data to external servers or healthcare systems for further analysis. WBANs play a critical role in healthcare, enabling real-time patient monitoring and preventive healthcare through early detection of potential health issues. Additionally, WBANs are integral to the wearable technology industry, where they are used in fitness trackers, smartwatches, and medical devices for both personal and clinical applications. Beyond healthcare, WBANs have applications in sports performance tracking, emergency response systems, and even in military and defense, where monitoring physiological data of personnel can enhance safety and operational efficiency [2]. The demand for secure, efficient, and reliable WBANs is growing as these networks become increasingly integrated into our daily lives and medical systems. Node classification within WBANs is essential for ensuring network security, data integrity, and operational efficiency. In a WBAN, each sensor, or "node," is responsible for gathering critical health or fitness data, making the reliability of each node crucial to the network's overall functionality. Classifying nodes as either trusted or untrusted allows the network to identify and address potentially compromised sensors that may transmit false or malicious data, which could endanger patient safety or lead to inaccurate health monitoring [3]. This classification is particularly vital in healthcare settings, where decisions based on sensor data can directly impact patient care. Effective node classification can help prevent issues such as data breaches, unauthorized access, and energy inefficiency. Furthermore, classifying nodes based on trustworthiness allows WBANs to prioritize resources and focus computational power on processing data from trusted sensors, which is crucial for extending the battery life of these devices and ensuring efficient data handling. In short, accurate and reliable node classification enhances WBAN performance by improving security, data quality, and system robustness [4]. The primary objective of this study is to explore and analyze advanced classification techniques that secure and optimize trustworthy node identification within WBANs. Given the sensitive nature of WBAN data and the increasing reliance on these networks for critical healthcare and wearable applications, there is a pressing need to implement robust classification algorithms that ensure the reliability of sensor nodes. This study aims to provide a comprehensive analysis of current classification algorithms used in WBANs, examining their strengths, limitations, and suitability for different applications. Furthermore, it seeks to identify advanced techniques that address common challenges in WBAN classification, such as low power consumption, high classification accuracy, and resistance to potential security threats. By focusing on the efficiency and security of these classification algorithms, the study aims to offer insights into optimizing WBAN performance and ensuring that only trustworthy data is transmitted and processed, ultimately contributing to the reliability and safety of WBAN applications [5]. The paper is organized into several sections, each addressing a key aspect of classification algorithms in WBANs. The Introduction section provides background information on WBANs, their applications, and the importance of node classification for network security and efficiency. This is followed by a Background and Key Concepts section, which covers WBAN architecture, common security challenges, and the concept of node trustworthiness [6]. The Overview of Classification Algorithms for WBANs section introduces the main types of classification algorithms used in WBANs, including machine learning and deep learning approaches. In the Advanced Techniques for Node Classification section, more sophisticated algorithms are discussed, such as spatial models, metaheuristic algorithms, and ensemble methods that enhance classification accuracy and efficiency [7]. A Comparative Analysis of Classification Algorithms section follows, providing a detailed comparison of various techniques

based on key performance metrics. The Security and Optimization in Node Classification section focuses on methods for securing and optimizing node classification processes, emphasizing power efficiency and latency reduction. The paper then discusses the Applications of Trustworthy Node Classification in WBANs across various fields, such as healthcare, sports, and military [8]. In the Challenges and Future Directions section, potential research areas and challenges in advancing node classification methods are addressed. Finally, the Conclusion section summarizes the study's findings, discusses the implications for WBAN security and efficiency, and offers final remarks on the future of trustworthy node classification in WBAN applications. Figure 1 provides a simplified representation of key components within a Wireless Body Area Network (WBAN) [9]. At the center is an outline of a human body with sensors placed on critical points, such as the chest and wrist, to collect health-related data like heart rate, temperature, and movement. These sensors transmit data through arrows leading to a central hub, which aggregates the information for analysis [10].

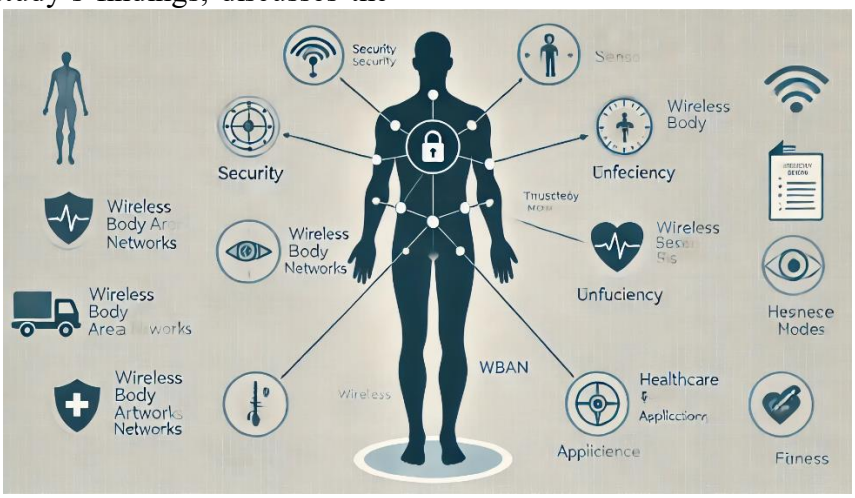

Figure 1. Simplified Diagram of Wireless Body Area Network (WBAN) Node Classification and Data Flow

2. **Related Work**

Wireless Body Area Networks (WBANs) represent a specialized category within wireless networks, designed for on-body or in-body sensors that collect physiological and environmental data from individuals. They are primarily used in healthcare and fitness industries, where they offer real-time monitoring of health metrics such as heart rate, body temperature, movement, and glucose levels [11]. The underlying concepts that support WBAN functionality are centered around network architecture, security measures, and trustworthiness of nodes, all of which are essential to ensure the reliable and secure operation of these networks. The architecture of a WBAN consists of several interconnected components, with nodes, gateways, and data flow pathways being central to the network's operation. Nodes in a WBAN typically refer to small, lightweight sensors placed on, around, or inside the human body [12]. Each node is responsible for monitoring specific physiological signals, such as body temperature, ECG, EEG, or motion data, depending on the application. These nodes are designed for low power consumption and typically operate on limited battery life, which requires efficient energy management. Gateways act as the central hub or controller in WBANs, receiving data from the individual nodes, consolidating it, and then relay it to external devices or cloud-based systems for analysis and storage. These gateways could be in the form of a smartphone, smartwatch, or other wearable devices [13]. Data flow in WBANs is often continuous, as the sensors regularly transmit data to ensure real-time monitoring. The network configuration is typically designed to accommodate reliable and low-latency data transfer to support applications that demand prompt responses,

such as medical alerts in healthcare scenarios. Table 1 provides an overview of the various types of sensors commonly used in Wireless Body Area Networks (WBANs), detailing their range, application fields, system types, wave types, and communication protocols [14]. Each sensor type is listed alongside its maximum operational range, indicating the distance within which it effectively transmits data (in meters or contact-based). The table also includes the application areas, such as cardiology, respiratory health, and fitness, as well as the associated system types like health monitoring or motion tracking systems. Additionally, it identifies the wave type each sensor relies on, categorized by range (e.g., electrical, infrared, mechanical), and lists compatible communication protocols (e.g., Bluetooth Low Energy (BLE), Zigbee, and NFC). This structured view highlights how these sensors work within WBANs, emphasizing their role in securely and efficiently transmitting health and activity data [15].

Table 1. WBAN Sensor Types, Ranges, Applications, and Protocols

Sensor Type	Range	Application Field	System Type	Type of Wave (Range)	Protocol Name
Electrocardiogram (ECG)	Up to 2 meters (m)	Cardiology, Patient Monitoring	Health Monitoring Systems	Electrical Waves (Short-Range)	Bluetooth Low Energy (BLE), Zigbee
Electromyography (EMG)	Up to 2 meters (m)	Muscle Activity, Rehabilitation	Rehabilitation and Fitness Systems	Electrical Waves (Short-Range)	Bluetooth, BLE
Electroencephalogram (EEG)	Up to 1 meter (m)	Neurology, Brain-Computer Interface	Brain-Monitoring Systems	Electrical Waves (Short-Range)	Zigbee, Wi-Fi
Blood Pressure Sensor	Up to 2 meters (m)	Hypertension, Cardiovascular Health	Cardiovascular Monitoring Systems	Mechanical (Pressure) Waves (Short-Range)	BLE, Zigbee
Glucose Sensor	Contact-based	Diabetes Management	Diabetes Monitoring Systems	Chemical Reaction (Short-Range)	NFC (Near Field Communication)
Body Temperature Sensor	Contact-based or < 1 meter (m)	Fever Detection, Health Screening	Health Monitoring Systems	Infrared Waves (Short-Range)	BLE, Zigbee
Pulse Oximeter	Up to 1 meter (m)	Oxygen Saturation, Respiratory Health	Respiratory Monitoring Systems	Light Waves (Infrared/Red, Short-Range)	BLE, Zigbee
Accelerometer	Up to 10 meters (m)	Fall Detection, Physical Activity	Activity Tracking Systems	Mechanical Waves (Short-Range)	BLE, ANT+
Gyroscope	Up to 10 meters (m)	Posture Monitoring, Balance Analysis	Motion Tracking Systems	Mechanical Waves (Short-Range)	BLE, ANT+
Respiration Sensor	Up to 2 meters (m)	Breathing Rate, Sleep Apnea Detection	Respiratory Monitoring Systems	Acoustic Waves (Short-Range)	BLE, Wi-Fi
pH Sensor	Contact-based	Wound Monitoring, Health Diagnostics	Diagnostic Systems	Chemical Reaction (Short-Range)	NFC, Zigbee
Electrochemical Sensor	Contact-based	Chemical Detection, Metabolite Monitoring	Biochemical Monitoring Systems	Chemical Reaction (Short-Range)	NFC, Zigbee
Infrared Sensor	Up to 5 meters (m)	Body Temperature, Gesture Recognition	Thermal Imaging Systems	Infrared Waves (Short-Range)	BLE, Zigbee
Pressure Sensor	Contact-based	Posture Correction, Pressure Ulcer Prevention	Rehabilitation Systems	Mechanical Waves (Short-Range)	BLE, NFC
Humidity Sensor	Up to 2 meters (m)	Skin Hydration, Sweat Analysis	Skin Monitoring Systems	Mechanical (Moisture) Waves (Short-Range)	BLE, Zigbee
Optical Sensor	Up to 2 meters (m)	Heart Rate, Blood Flow	Health Monitoring Systems	Light Waves (Optical, Short-Range)	BLE, Zigbee

2.1 Security and Trust Challenges in WBANs

Security is a critical concern in WBANs due to the sensitive nature of the data collected and the unique challenges posed by operating in close proximity to the human body. Data breaches are a primary risk, as unauthorized access to a WBAN could result in exposure to sensitive health information, leading to privacy violations and potential misuse of data [16]. The lightweight, low-power nature of WBAN nodes also restricts the types of encryption and security measures that can be applied, making them susceptible to hacking attempts. Node compromises represent another challenge, where individual sensors may be physically or digitally altered to transmit erroneous data. This could occur due to malware attacks or physical tampering, resulting in a network that cannot be fully trusted for accurate data transmission. Privacy issues arise because WBANs continuously monitor and transmit highly personal information, such as vital signs and movement patterns [17]. This constant data flow poses a risk if it falls into unauthorized hands or if the data transmission is not properly encrypted. Securing these networks is thus essential to maintaining user trust and protecting sensitive health data [18]. Table 2 presents essential parameters for evaluating security and trust challenges in Wireless Body Area Networks (WBANs) [18]. It lists each parameter along with its unit of measure and data type, providing a structured way to quantify and monitor security aspects within WBAN systems [19]. Key parameters include data integrity, node, trust level authentication time and encryption strength which are crucial for maintaining secure and reliable network performance. Other parameters like false positive rate latency and battery life impact help gauge the efficiency and reliability of security protocols applied in WBANs. This overview aids in identifying potential vulnerabilities and optimizing trust management within these networks [20].

Table 2. Key Parameters for Security and Trust Challenges in WBANs

Parameter	Unit of Measure	Data Type	Description
Data Integrity	Percentage (%)	Float	Measures the accuracy and consistency of data over time.
Node Trust Level	Score (0-1)	Float	Indicates the reliability of a node, where 0 is untrusted and 1 is fully trusted.
Authentication Time	Seconds (s)	Float	Time taken to verify the identity of a node or user.
Data Encryption Strength	Bits	Integer	Indicates the level of encryption, e.g., 128-bit, 256-bit.
Power Consumption	Watts (W)	Float	Amount of energy used by security protocols on WBAN devices.
Data Transmission Rate	Bits per second (bps)	Float	Speed of data transfer between nodes, impacting real-time security measures.
Packet Loss Rate	Percentage (%)	Float	Percentage of lost data packets, which can indicate security breaches.
Latency	Milliseconds (ms)	Float	Delay in data transmission, often affected by security processing times.
False Positive Rate	Percentage (%)	Float	Rate at which legitimate nodes are incorrectly classified as untrusted.
False Negative Rate	Percentage (%)	Float	Rate at which compromised nodes are incorrectly classified as trusted.
Access Control Level	Discrete levels (e.g., 0-3)	Integer	Defines the access rights of nodes, with levels for different permissions.
Signal-to-Noise Ratio (SNR)	Decibels (dB)	Float	Measures of signal quality, low SNR may suggest interference or attacks.
Intrusion Detection Accuracy	Percentage (%)	Float	Indicates the success rate of detecting unauthorized access.
Battery Life Impact	Hours	Float	Reduction in battery life due to security mechanisms.

To maintain network integrity and ensure data reliability, WBANs employ node classification to distinguish between “trusted” and “untrusted” nodes. A trusted node is one that consistently transmits reliable, accurate data, free from interference or compromise. Trusted nodes are critical in applications like healthcare, where inaccurate readings could lead to incorrect diagnoses or treatments [21]. Conversely, an untrusted node is one that may

have been compromised, either by malfunction, unauthorized tampering, or because of a cyberattack. Classification algorithms analyze data transmission patterns, consistency, and integrity to assess the trustworthiness of each node [22]. By categorizing nodes into trusted and untrusted groups, WBAN systems can isolate compromised nodes, prioritize secure data streams, and make more accurate decisions based on trustworthy information. This classification not only enhances the reliability of data collected within the network but also contributes to the overall security of the WBAN by preventing malicious or faulty nodes from affecting the entire system. Effective node classification, therefore, is foundational to a well-functioning, secure, and trustworthy WBAN [23]. Security and trust challenges in Wireless Body Area Networks (WBANs) have significant impacts on network functionality, data integrity, and user trust. These effects are particularly pronounced in applications where WBANs monitor critical health parameters, as any compromise in security or trust can have serious consequences [24]. Below are some of the primary effects:

1. Data Integrity and Accuracy: Security and trust issues can compromise the integrity of the data collected by WBANs, leading to inaccurate readings and unreliable monitoring. For example, compromised nodes may transmit incorrect health data due to interference or tampering, which could result in inaccurate diagnoses or inappropriate treatments in healthcare applications. When data from untrusted nodes is mistakenly accepted, it can distort the overall data flow, reducing the network's reliability.

2. Privacy Violations: Since WBANs collect highly sensitive personal information, such as heart rate, glucose levels, and activity data, security challenges pose a risk of privacy breaches. Unauthorized access to a WBAN could expose this information, which is not only a violation of user privacy but also a potential risk in medical contexts. For instance, data intercepted from a WBAN could be misused for purposes like identity theft, profiling, or targeted attacks, thereby impacting user trust and willingness to use such systems.

3. Reduced Network Reliability: Trust issues within a WBAN can undermine network reliability, as the system must continuously evaluate whether data from each node is trustworthy. This process consumes computational resources and can slow down data processing, reducing network efficiency and potentially introducing delays. In critical applications, such as real-time patient monitoring, these delays can affect timely interventions, posing risks to user safety.

4. Increased Power Consumption: Addressing security and trust challenges often requires complex authentication, encryption, and trust-assessment protocols, which can increase power consumption. WBAN devices, especially wearable sensors, operate on limited battery life. Enhanced security measures can drain these devices faster, reducing their operational lifespan and requiring more frequent maintenance or battery replacements, which affects their usability and practicality in long-term applications.

5. Susceptibility to Malicious Attacks: Unaddressed security vulnerabilities make WBANs susceptible to various types of attacks, such as data tampering, replay attacks, or denial-of-service (DoS) attacks. For instance, a compromised node could be used as an entry point for attackers to disrupt the entire network, flooding it with malicious traffic or corrupting data to compromise system functionality. The lack of robust security measures increases the likelihood of such attacks, thereby posing potential risks for users who rely on WBANs for critical health monitoring.

6. Erosion of User Trust: Trust challenges impact user perception of WBAN reliability. If a user doubts the security of their WBAN, they may hesitate to adopt or

use the technology, especially in contexts where data privacy is paramount, like healthcare. When users cannot fully trust that their data is private and secure, they may seek alternatives or avoid using WBANs altogether. This erosion of trust limits the adoption and impact of WBANs, reducing their potential benefits for patient monitoring, preventive healthcare, and fitness applications.

7. Operational Costs and Maintenance: Maintaining high security standards in WBANs often involves regular updates to security protocols, which can increase operational costs and maintenance demands. Frequent updates and the need for continuous monitoring to address emerging security threats place a burden on healthcare providers, developers, and end-users. Additionally, ensuring that all devices remain secure and trustworthy can be challenging, especially in environments with multiple sensors and complex network structures, leading to increased costs in both time and resources.

8. Regulatory and Compliance Challenges: As WBANs often handle sensitive health information, they are subject to regulations and standards that mandate stringent data security and privacy practices (such as HIPAA in the U.S.). Failure to address security and trust challenges can result in non-compliance, exposing providers and developers to legal repercussions. Non-compliance with these standards can lead to fines, restricted use, and limitations on deploying WBAN technology in certain regions or applications, thereby limiting the reach and growth of WBAN systems.

Table 3 outlines the primary security and trust challenges currently affecting Wireless Body Area Networks (WBANs). Each row highlights a specific problem, detailing the cause behind it and the potential damage it may cause. Key challenges include data integrity compromises, privacy breaches, and denial-of-service attacks, often caused by issues like unauthorized access, weak encryption, or lack of intrusion detection systems [25]. The potential damages range from inaccurate health data and privacy loss to reduced device lifespan and legal non-compliance. This overview emphasizes the need for robust security measures to ensure WBAN reliability and user trust [26].

Table 3. Key Security and Trust Challenges in WBANs: Problems, Causes, and Potential Damages

Problem	Cause	Potential Damage
Data Integrity Compromise	Unauthorized access, node tampering, malware	Inaccurate health data, potential misdiagnoses, and compromised treatment decisions in healthcare applications.
Privacy Breach	Weak encryption, insufficient authentication measures	Exposure of sensitive health information, risk of identity theft, and loss of user privacy and trust.
Node Impersonation	Lack of robust authentication protocols, spoofing attacks	Malicious nodes masquerading as trusted ones, leading to false data entry and network corruption.
High Power Consumption	Overly complex security protocols, continuous monitoring	Reduced battery life of WBAN devices, requiring frequent recharging or replacement, impacting device usability.
Denial of Service (DoS) Attacks	Network overload, lack of intrusion detection	Service interruptions, loss of real-time monitoring capability, and potential harm in critical health situations.
False Node Classification	Inadequate classification accuracy, false positives/negatives	Misclassification of trusted/untrusted nodes, affecting data reliability and increasing vulnerability to attacks.
Packet Loss	Network interference, malicious attacks targeting packets	Loss of critical health data, reduced data transmission reliability, and compromised real-time monitoring.
Increased Latency	Complex encryption processes, trust evaluation overhead	Delayed data transmission, especially harmful in real-time health monitoring where prompt response is essential.
Malicious Data Injection	Lack of secure data validation,	Corruption of WBAN data stream, potential harm from inaccurate data in

	compromised nodes	health monitoring applications.
Erosion of User Trust	Security breaches, privacy concerns	Reduced adoption and use of WBAN technology, limiting its potential benefits for healthcare and fitness.
Regulatory Non-compliance	Insufficient adherence to data protection standards	Legal penalties, restricted WBAN deployment in healthcare, and potential loss of reputation and trustworthiness.

2.2 Overview of Classification Algorithms for WBANs

Classification algorithms play a pivotal role in ensuring that Wireless Body Area Networks (WBANs) operate securely and efficiently, particularly when it comes to assessing the trustworthiness of individual nodes within the network. Given the sensitive nature of the data WBANs handle, such as health metrics and physical activities, reliable classification of nodes is essential for preventing data breaches, maintaining network integrity, and conserving device resources [27]. Classification algorithms in WBANs generally fall into various categories based on their learning approach, the complexity of the models, and their suitability for different WBAN applications. The following sections provide an overview of the most used classification approaches, including supervised and unsupervised methods, traditional machine learning algorithms, deep learning and hybrid approaches, and trust-based classification techniques tailored to WBAN environments [28]. Table 4 provides a summary of classification algorithms frequently used in WBANs, listing each algorithm's limitations and the performance metrics commonly applied to measure effectiveness. Metrics like accuracy, precision, recall, and F1 score are essential for evaluating classification success, while metrics like latency and power consumption are crucial for real-time, energy-efficient applications [29]. This overview highlights the need to balance algorithm accuracy with computational efficiency in WBANs [30].

Table 4. current classification algorithms used in WBANs

Classification Algorithm	Limitations	Performance Metrics
Decision Trees	Prone to overfitting, limited scalability with large datasets	Accuracy, Precision, Recall, F1 Score
Support Vector Machines (SVM)	High computational cost, less effective with noisy data	Accuracy, Precision, F1 Score, Training Time
K-Nearest Neighbors (KNN)	Computationally expensive with large datasets, sensitive to irrelevant features	Accuracy, Precision, Recall, Latency
Neural Networks	Requires large datasets, high power and memory consumption	Accuracy, Precision, F1 Score, Power Consumption
Convolutional Neural Networks (CNNs)	High computational demands, unsuitable for real-time applications	Accuracy, Processing Time, F1 Score
Naïve Bayes	Assumes feature independence, less accurate with complex data	Accuracy, Precision, Recall
Random Forest	High computational cost, less interpretable, prone to overfitting	Accuracy, Precision, F1 Score, Latency
Genetic Algorithms	Computationally intensive, sensitive to parameter settings	Convergence Time, Accuracy
Reinforcement Learning	Requires extensive training, complex to implement	Convergence Rate, Accuracy, Latency
K-Means Clustering	Sensitive to initial conditions, limited interpretability	Cluster Purity, Inertia, Silhouette Score
Principal Component Analysis (PCA)	Reduces dimensionality but may lose important data features	Explained Variance, Reconstruction Error
Trust-Based Algorithms	High complexity in maintaining trust scores, computational overhead	Trust Score Accuracy, False Positive Rate, False Negative Rate

In the context of WBANs, classification methods can broadly be categorized into supervised and unsupervised learning approaches. Supervised learning involves training a model on labeled data, where the input data is paired with the correct output or classification, which helps the model learn to predict outcomes for new, unseen data [31]. In WBANs, supervised methods are often used when ample labeled data is available, allowing the system to classify nodes into trusted and untrusted categories based on historical data patterns [32]. Supervised learning can improve the accuracy of WBAN classification by effectively distinguishing between normal and suspicious activity. On the other hand,

unsupervised learning operates without labeled data, making it suitable for scenarios where data is less predictable or labeled data is scarce [33]. Instead of using predefined categories, unsupervised algorithms identify patterns and groupings based on data similarities and anomalies. In WBANs, unsupervised methods are useful for anomaly detection, identifying potential threats or compromised nodes that behave differently from others. This approach can be particularly valuable in dynamic environments where the system must adapt to new, unforeseen behavior without retraining on labeled data [34].

2.3 Traditional Machine Learning Algorithms

Traditional machine learning algorithms, including decision trees, support vector machines (SVM), and k-nearest neighbors (KNN), are widely used for node classification in WBANs due to their interpretability and relatively low computational cost. Decision trees are a popular choice because they are intuitive and allow the WBAN system to make decisions based on a series of simple rules, which makes them both efficient and suitable for real-time applications. Decision trees are often used in scenarios where WBAN systems need to classify nodes quickly with minimal processing power, making them ideal for wearable devices with limited resources [35].

Support Vector Machines (SVM) are another effective algorithm for WBAN classification, especially when dealing with high-dimensional data. SVMs create a boundary, or "hyperplane," that separates different classes, allowing the WBAN system to differentiate between trusted and untrusted nodes based on their feature vectors. This algorithm is beneficial for WBAN applications that require high accuracy, as SVMs can manage complex data patterns, though they are typically more computationally intensive than decision trees [36].

K-nearest neighbors (KNN) is a simple yet powerful algorithm that classifies nodes based on the "distance" between data points, which makes it effective for WBANs that have spatial or proximity-based data. KNN is useful in situations where WBAN nodes are grouped closely together and can be classified based on the similarity to their nearest neighbors. However, KNN can be computationally expensive as the dataset grows, making it better suited for smaller networks or cases where speed is not the primary concern [37].

2.4 Deep Learning and Hybrid Approaches

As WBAN applications become more complex, deep learning algorithms are increasingly being employed to handle sophisticated classification tasks. Techniques such as neural networks and convolutional neural networks (CNNs) are now used to analyze complex data patterns and improve the accuracy of node classification within WBANs. Neural networks are particularly suited for handling non-linear relationships in data, which is common in WBAN environments where node behavior may be unpredictable or vary based on multiple factors. CNNs are especially beneficial when analyzing spatial data or data with hierarchical structures, as they can extract features through layered processing. In WBANs, CNNs are sometimes applied in gesture recognition and activity monitoring applications, where they can recognize patterns across multiple layers of data. Hybrid approaches combine the strengths of traditional and deep learning algorithms, creating models that balance accuracy with computational efficiency. For example, hybrid models may use decision trees to preprocess and filter data before feeding it into a deep learning model, optimizing the balance between accuracy and speed. Hybrid approaches are well-suited to WBANs that need to conserve power and processing resources but still demand high classification accuracy for secure and reliable performance [38].

2.5 Trust-Based Classification Techniques

Given the importance of security and reliability in WBANs, trust-based classification techniques have been specifically developed to assess and classify node trustworthiness. These algorithms evaluate the behavior of each node and assign a trust level, which helps the WBAN system determine whether to include or exclude a node's data in network operations.

Trust-based algorithms often monitor factors such as data consistency, frequency of communication, and historical reliability to assign a trust score to each node. Nodes that consistently provide accurate data are classified as trusted, while nodes exhibiting unusual or inconsistent behavior are flagged as untrusted [39].

Trust-based classification techniques are particularly useful in WBANs where security is critical, as they enable the system to isolate compromised nodes without disrupting the entire network. For example, a node that has been compromised by a cyberattack may begin sending incorrect or harmful data; by detecting these deviations, trust-based algorithms can prevent the network from acting on compromised information. These techniques are instrumental in applications like medical monitoring, where trustworthy data is essential for patient safety.

The choice of the "best" classification algorithm for Wireless Body Area Networks (WBANs) largely depends on the specific needs and constraints of the application, such as energy efficiency, computational power, and real-time processing requirements. Here are three leading algorithms that are commonly considered effective for different WBAN scenarios, each with unique strengths and limitations:

Random Forest is an ensemble learning technique that builds multiple decision trees and aggregates their results to improve classification accuracy and reduce the likelihood of overfitting. This makes it highly suitable for applications where high accuracy is a priority, such as healthcare monitoring. In WBANs, where data may be complex or noisy, Random Forest is particularly effective as it can handle a diverse set of features and variations in data. By combining multiple decision trees, the algorithm creates a robust model that often outperforms simpler models in terms of accuracy [40].

However, Random Forest has limitations, particularly in WBAN applications where power and memory are constrained, as it is computationally intensive and requires substantial resources. Additionally, because Random Forest is an ensemble method, it can be challenging to interpret, which limits its application in real-time monitoring where speed and simplicity are essential. Despite these limitations, Random Forest remains an excellent choice for scenarios where accuracy is crucial, and energy constraints are manageable, such as in healthcare monitoring systems where data can be processed off-body.

Support Vector Machines (SVMs) are known for their high accuracy, especially in high-dimensional spaces where there is a clear margin of separation between classes. This makes SVMs ideal for applications that require precise classification, such as differentiating between trusted and untrusted nodes or recognizing specific activities in WBANs. The strength of SVM lies in its ability to create a decision boundary, or hyperplane, that maximizes the separation between different classes. This capability makes it a reliable option for applications with small to medium datasets, which are often found in WBAN environments [41].

However, SVM has its limitations, as it is computationally demanding, particularly when using complex kernels or when working with larger datasets. This requirement for computational resources may impact its suitability for real-time processing in WBANs, where resources are limited. Additionally, SVM is sensitive to noise in the data, which can affect classification accuracy. Despite these limitations, SVM remains a strong choice for applications where accurate node classification is vital, provided that sufficient computational resources are available.

Naïve Bayes is a probabilistic algorithm known for its simplicity and computational efficiency, making it well-suited for real-time WBAN applications where power consumption is a critical constraint. This algorithm is particularly useful in wearable and implantable WBAN devices, as it requires minimal computational resources and works effectively with small datasets. Naïve Bayes assumes feature independence, which may not always be accurate in real-world WBAN scenarios, yet this assumption simplifies computations,

making it suitable for low-power applications [42].

While Naïve Bayes is generally less accurate than more complex models like SVM or Random Forest, its fast processing and low resource demands make it ideal for lightweight WBAN applications, such as basic health monitoring in wearables. For these applications, Naïve Bayes is often preferred, as it strikes a good balance between efficiency and simplicity, allowing real-time monitoring with minimal impact on battery life [43].

Each of these algorithms performs well under specific conditions, and the best choice depends on the unique requirements of the WBAN application. For applications where accuracy is paramount, such as in healthcare diagnostics, Random Forest or SVM is often the preferred option due to their ability to handle complex and noisy data. In contrast, Naïve Bayes is well-suited for real-time and power-sensitive applications like wearable health monitoring, where quick, low-power classification is prioritized over absolute accuracy. For applications that require a balance between accuracy and power consumption, a hybrid approach may be beneficial. Combining simpler preprocessing techniques, such as Naïve Bayes or KNN, with more accurate models like SVM or Random Forest can optimize classification in WBANs [45].

Trust-based classification techniques in Wireless Body Area Networks (WBANs) use a variety of parameters to assess and classify nodes as "trusted" or "untrusted." The following are some common parameters and their associated equations that can be used to calculate trust scores and classify nodes based on their behavior and reliability.

1. Direct Trust (DT): Direct trust between nodes is often calculated based on successful interactions or positive data exchanges over a period. It combines factors such as successful interactions (e.g., data accuracy) and communication frequency.

$$DT_{i,j} = \frac{\text{Successful Interactions}_{i,j}}{\text{Total Interactions}_{i,j}}$$

where:

- $DT_{i,j}$ is the direct trust of node i in node j.
- **Successful Interactions** is the count of positive, reliable interactions between nodes i and j.
- **Total Interactions** is the total count of interactions between nodes i and j.

2. Indirect Trust (IT): Indirect trust is derived from recommendations or observations by neighboring nodes that have interactions with the target node. This value is aggregated based on the trust ratings provided by other nodes about the target node.

$$IT_{i,j} = \sum_{k \in N(i)} \left(\frac{DT_{k,j} \times DT_{i,k}}{|N(i)|} \right)$$

where:

- $IT_{i,j}$ is the indirect trust of node i in node j.
- $N(i)$ is the set of neighbors of node i.
- $DT_{k,j}$ is the direct trust of a neighboring node k in node j.
- $DT_{i,k}$ is the direct trust of node i in its neighboring node k.

3. Total Trust (TT) : Total trust is a combination of direct and indirect trust, often weighted to prioritize either direct or indirect trust based on the application requirements.

$$TT_{i,j} = \alpha \cdot DT_{i,j} + \beta \cdot IT_{i,j}$$

where:

- $TT_{i,j}$ is the total trust value of node i in node j.
- α and β are weight coefficients for direct and indirect trust, respectively, with $\alpha + \beta = 1$.

4. Trust Decay Factor (TDF): Trust in nodes can decay over time if there is no continuous interaction, reflecting the idea that trust needs to be maintained. The decay factor can be applied to reduce the trust score over time if interactions become infrequent.

$$TDF = e^{-\lambda t}$$

where:

- TDF is the trust decay factor.
- λ is the decay constant (a parameter that determines how quickly trust decays).
- t is the time elapsed since the last successful interaction.

The decayed trust can then be calculated as:

$$DT_{\text{decayed}} = DT \times TDF$$

5. Reputation Score (RS): Reputation in trust-based systems is often calculated by aggregating trust ratings from multiple nodes. It represents the reliability of a node as perceived by its neighbors.

$$RS_j = \frac{\sum_{i \in N(j)} TT_{i,j}}{|N(j)|}$$

where:

- RS_j is the reputation score of node j.
- $N(j)$ is the set of neighboring nodes that interact with node j.
- $TT_{i,j}$ is the total trust of each neighbor i in node j.

6. Trust Threshold (TT_threshold): To classify nodes as trusted or untrusted, a threshold value is often used. Nodes with a total trust score above this threshold are classified as trusted, while those below are classified as untrusted.

$$\text{Classification} = \begin{cases} \text{Trusted} & \text{if } TT_{i,j} \geq TT\_threshold \\ \text{Untrusted} & \text{if } TT_{i,j} < TT\_threshold \end{cases}$$

where:

- $TT\_threshold$ is the predefined trust threshold value for classification.
- $TT_{i,j}$ is the total trust of node i in node j.

7. Trust Aggregation: In cases where multiple trust factors are involved (such as direct trust, indirect trust, and reputation), a weighted aggregation approach can be used:

$$T_{i,j} = w_1 \cdot DT_{i,j} + w_2 \cdot IT_{i,j} + w_3 \cdot RS_j$$

where:

- $T_{i,j}$ is the aggregated trust score of node i in node j.
- w_1, w_2, and w_3 are weights assigned to direct trust, indirect trust, and reputation, respectively, with $w_1 + w_2 + w_3 = 1$.

These equations provide a structured approach to trust-based classification in WBANs, allowing nodes to be evaluated based on both direct experiences and reputational input from neighboring nodes. By combining these factors, WBAN systems can achieve a more comprehensive and reliable classification of nodes, supporting both security and network efficiency.

3. Advanced Techniques for Node Classification in WBANs

As Wireless Body Area Networks (WBANs) continue to evolve, more advanced classification techniques are being applied to enhance the accuracy, security, and reliability of node classification within these networks. Traditional classification algorithms can be limited in handling the complex, high-dimensional, and sometimes dynamic data encountered in WBANs. To address these challenges, advanced techniques such as artificial intelligence (AI), spatiotemporal modeling, metaheuristic algorithms, and ensemble learning have been introduced. Each approach brings specific benefits to WBAN node classification, supporting a range of applications from healthcare to security-sensitive environments [46].

Artificial Intelligence (AI)-based techniques, particularly those leveraging deep learning and reinforcement learning, have become central to advancing node classification in WBANs. Deep learning algorithms, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have shown a remarkable ability to analyze complex, non-linear patterns in data. This makes them well-suited for WBAN applications, where data from nodes can vary significantly based on user behavior, environmental factors, and the specifics of physiological monitoring. CNNs, for instance, are effective in identifying spatial patterns in sensor data, which can help classify nodes based on their reliability. Meanwhile, RNNs, with their ability to analyze sequential data, are particularly valuable in applications that track changes over time, such as activity monitoring or anomaly detection.

Reinforcement learning introduces a different paradigm, where nodes learn to classify behavior based on reward feedback mechanisms. This approach is beneficial for WBANs that operate in changing environments, allowing the system to adapt classification rules dynamically based on new input data. For example, reinforcement learning could enable a WBAN system to detect and classify new types of threats or abnormal behavior that may not have been anticipated during initial training. While deep learning and reinforcement learning require substantial computational power, they contribute to enhanced classification accuracy and real-time adaptability, making them suitable for WBANs that prioritize security and reliability [47].

Spatial and temporal models leverage the spatiotemporal characteristics of data collected from WBAN nodes to improve classification accuracy in real-time environments. In WBANs, data from sensors are often affected by the position of the node on the body and the time-dependent nature of physiological changes. Spatial models focus on analyzing the location-based data, recognizing patterns based on where the node is located and how it interacts with other nodes. This is especially valuable in applications like gait analysis, posture recognition, and fall detection, where spatial relationships among nodes (e.g., on the wrist, chest, or ankle) contribute to accurate classification.

Temporal models, on the other hand, analyze time-series data to identify trends or

abnormalities over time. This approach is beneficial in WBANs where node behavior may change gradually or suddenly, such as in monitoring heart rate variability or respiratory patterns. Combining spatial and temporal models allows WBANs to capture a more comprehensive view of the data, helping to differentiate between trusted and untrusted nodes based on both the physical location and time-based behavior. Such models can significantly improve the real-time responsiveness and reliability of WBAN node classification, especially in applications requiring continuous monitoring, like healthcare and emergency response systems [48].

Metaheuristic algorithms, including genetic algorithms and particle swarm optimization (PSO), offer advanced optimization techniques for node classification in WBANs, addressing challenges where traditional algorithms may fall short. These algorithms are designed to search for large solution spaces and find optimal or near-optimal solutions by simulating natural processes. Genetic algorithms work by mimicking the process of natural selection, evolving a population of solutions over time to improve classification accuracy. This approach is beneficial in WBANs where the best classification parameters may not be known in advance, as genetic algorithms can dynamically adjust parameters to enhance accuracy and efficiency [49].

Particle swarm optimization simulates the social behavior of birds or fish to optimize classification. In WBANs, PSO can be used to improve the clustering or grouping of nodes, helping to identify which nodes are likely to be trustworthy based on their behavior and interactions with neighboring nodes. Both genetic algorithms and PSO are flexible and adaptable, making them effective for WBAN applications that require adaptive classification techniques to respond to changing network conditions. However, these algorithms can be computationally intensive, so their use may be best suited for systems with moderate-to-high processing capabilities or for classification tasks where optimization is performed periodically rather than in real time.

Ensemble and hybrid techniques combine multiple algorithms to improve the robustness and accuracy of classification in WBANs. Ensemble learning uses multiple classifiers to create a combined model that often outperforms individual algorithms. Techniques like bagging (bootstrap aggregating), boosting, and stacking are popular ensemble methods that aggregate predictions from several algorithms, reducing the likelihood of misclassification and increasing reliability. For example, an ensemble of decision trees (known as a random forest) can provide high accuracy while managing the complexity of WBAN data. This approach is especially effective in WBANs where individual nodes may experience variable conditions, as ensemble learning can compensate for these fluctuations by aggregating diverse predictions.

Hybrid techniques take ensemble learning further by combining different types of algorithms, such as pairing a traditional machine learning model with a deep learning model, to benefit from the strengths of each. For instance, a hybrid system might use Naïve Bayes to perform preliminary filtering of nodes before applying a more complex algorithm like CNN for final classification. This combination allows WBANs to achieve a balance between speed and accuracy, making hybrid approaches ideal for applications where power efficiency and high classification accuracy are both priorities. Hybrid and ensemble methods are particularly useful in WBANs deployed in healthcare settings, where accuracy is paramount, but resource constraints are also a consideration [50].

4. Comparative Analysis of Classification Algorithms

Comparing classification algorithms is essential to determine which approach is most suitable for Wireless Body Area Networks (WBANs). Each algorithm has distinct strengths and limitations that make it more or less appropriate for specific WBAN applications, such as real-time health monitoring, activity recognition, or security assurance. This section presents a detailed analysis of the performance metrics used to

evaluate classification algorithms, an in-depth comparison of the strengths and weaknesses of each algorithm, and a comparative summary table that consolidates these findings for easy reference. In WBANs, the performance of classification algorithms is evaluated using several key metrics that address both accuracy and operational efficiency. Accuracy is one of the most fundamental metrics, representing the proportion of correctly classified instances out of the total instances. High accuracy is critical for applications where misclassification could lead to serious consequences, such as in medical monitoring. Precision and recall provide a more nuanced view of accuracy, focusing specifically on the rate of true positive classifications among all positive predictions and the rate of true positive classifications among actual positive cases, respectively. These metrics are particularly valuable in trust-based WBAN applications where false positives (e.g., classifying an untrusted node as trusted) or false negatives (e.g., classifying a trusted node as untrusted) could compromise data integrity and network security [51].

The F1 score is the harmonic meaning of precision and recall, providing a balanced measure that takes both metrics into account. This is especially important in WBANs where false positives and negatives are both costly, making it a preferred metric for algorithms used in security-focused WBAN systems. Latency is another crucial metric, particularly in real-time applications where data must be processed quickly. High latency can disrupt continuous monitoring, so algorithms with lower latency are favored in applications like real-time health monitoring or emergency response. Energy efficiency is also essential for WBANs, as many devices are battery-powered. Energy-intensive algorithms can drain battery life quickly, making them less practical for wearable or implantable WBAN devices. Thus, algorithms must balance high accuracy with low energy consumption to be effective in long-term WBAN applications.

Each classification algorithm comes with unique strengths and weaknesses, which must be carefully considered in the context of WBAN systems. **Decision trees**, for example, are simple to understand and interpret, making them a suitable choice for WBANs with limited computational capacity. They are quick and efficient, which makes them well-suited for real-time applications where interpretability is essential. However, decision trees are prone to overfitting, particularly with complex data, which can compromise their generalizability and accuracy [52].

Support Vector Machines (SVM) excel in accuracy, particularly in high-dimensional data spaces where there is a clear margin of separation between classes. This makes SVMs a strong choice for WBAN applications that require precise node classification, such as distinguishing between trusted and untrusted nodes. However, SVMs are computationally intensive and require significant processing power, which limits their suitability for real-time applications or energy-constrained WBAN devices. **K-Nearest Neighbors (KNN)** is another algorithm known for its high accuracy, especially when the dataset is small and straightforward. It is effective in applications where node classification can rely on proximity-based clustering. However, KNN's computational cost increases with larger datasets, making it less efficient for real-time or large-scale WBANs [53].

Neural networks and **convolutional neural networks (CNNs)** provide exceptional accuracy and are highly effective in handling complex and non-linear relationships in data, which makes them ideal for WBANs that handle diverse physiological data. However, they are resource-intensive, requiring substantial power and memory, which limits their practical use in small, low-power WBAN devices. On the other hand, **Naïve Bayes** offers a fast and efficient classification option with minimal computational demand, making it suitable for lightweight WBAN applications. Its simplicity, however, comes at the cost of accuracy in complex datasets, especially when the assumption of feature independence is violated.

Ensemble methods, such as **Random Forest**, combine multiple algorithms to improve classification, accuracy and robustness. They are generally more resilient to overfitting than

individual decision trees and offer higher accuracy, making them effective in WBAN applications with moderate computational resources. However, ensemble methods require more processing power than single algorithms, which can be challenging for energy-constrained WBAN devices [54]. Lastly, **metaheuristic algorithms** like genetic algorithms and particle swarm optimization are powerful for optimizing classification in dynamic environments, but they require significant computational power and are more suited to periodic optimization tasks rather than continuous real-time classification as shown in table 5.

Table 5 compares classification algorithms based on key performance metrics and attributes, highlighting their suitability for different WBAN applications.

Algorithm	Accuracy	Precision & Recall	F1 Score	Latency	Energy Efficiency	Strengths	Weaknesses
Decision Tree	Moderate	Moderate	Moderate	Low	High	Simple, interpretable, suitable for real-time	Prone to overfitting, less effective with complex data
Support Vector Machine (SVM)	High	High	High	Moderate	Moderate	Accurate in high-dimensional spaces	Computationally intensive, sensitive to noise
K-Nearest Neighbors (KNN)	Moderate-High	High	Moderate	High	Low	Effective for small datasets and proximity-based	High computational cost with large datasets
Neural Network	High	High	High	Moderate-High	Low	Excellent for complex, non-linear relationships	Resource-intensive, not suitable for low-power devices
Convolutional Neural Network (CNN)	Very High	Very High	Very High	High	Low	Effective for spatial data and complex patterns	High computational demand, unsuitable for real-time
Naïve Bayes	Moderate	Moderate	Moderate	Low	Very High	Fast, low power, suitable for lightweight WBANs	Assumes feature independence, less accurate with complex data
Random Forest	High	High	High	Moderate	Moderate	High accuracy, robust to overfitting	High computational cost, less interpretable
Genetic Algorithm	Moderate-High	Moderate	Moderate	High	Low	Adaptable, suitable for optimization tasks	Computationally intensive, sensitive to parameter settings
Particle Swarm Optimization (PSO)	Moderate	Moderate	Moderate	High	Low	Effective for dynamic environments	Computationally demanding, less suited for real-time

This comparative summary table provides a quick overview of the strengths and weaknesses of each classification algorithm in the context of WBANs. It allows for easier selection based on the desired balance of accuracy, efficiency, and computational demands. While some algorithms like Random Forest and SVM offer high accuracy and are well-suited for trusted node classification, others like Naïve Bayes and Decision Tree provide efficient, low-power alternatives for real-time, low-complexity applications. This analysis underscores the need for careful algorithm selection based on the specific requirements of each WBAN system [55].

5. Challenges and Future Directions

Wireless Body Area Networks (WBANs) are rapidly advancing, and with their growth come new challenges and opportunities for innovation, particularly in classification techniques. As WBANs are deployed in increasingly complex and diverse environments, ensuring that classification algorithms remain effective, secure, and adaptable is essential [56]. This section explores some of the key challenges and future directions for WBAN classification, focusing on scalability, security, privacy, advanced machine learning models, and the challenges of real-world implementation. One of the primary challenges in WBAN classification is achieving scalability and adaptability in classification methods to accommodate large and diverse networks. WBANs are often deployed across multiple nodes, each collecting different types of data, from physiological metrics to movement patterns [57]. In large-scale WBAN applications, such as monitoring patient groups in hospitals or athletes in training camps, classification algorithms must be able to handle high data volumes and ensure accurate

classification across a range of environments and contexts. This demands that algorithms be highly adaptable, dynamically adjusting to variations in user behavior, device types, and environmental conditions [58]. Future directions may involve the development of adaptive algorithms capable of learning and recalibrating in real-time based on user patterns, which would help to scale WBANs effectively without compromising performance or accuracy. As WBANs increasingly integrate with the broader Internet of Things (IoT) ecosystem, ensuring secure classification becomes a significant challenge. WBANs connected to IoT networks often interact with various other devices and systems, from cloud servers to smartphones and medical equipment [59]. This connectivity introduces additional security risks, as it creates more entry points for potential attackers. Securing WBANs in an IoT-integrated environment will require advanced authentication and encryption protocols that can safeguard data as it moves through different networks. Additionally, secure data-sharing frameworks will be essential to maintain trust in connected WBAN devices, especially in healthcare, where patient data privacy is a primary concern. Future solutions may include blockchain-based systems for secure data sharing and zero-trust architectures that verify each device interaction to prevent unauthorized access [60].

Privacy and data protection remain central to the ethical deployment of WBANs, particularly as these networks handle sensitive personal data. Classification algorithms in WBANs must be designed to protect user privacy without compromising on classification accuracy. This is particularly challenging because effective classification often requires detailed data, which can inadvertently reveal more about a user's personal health or behavior than intended. Techniques like differential privacy, which adds controlled noise to data to mask individual identities, are gaining attention as a potential solution for WBAN privacy protection. Federated learning, which trains algorithms across decentralized devices without centralizing raw data, also holds promises for protecting user privacy while maintaining the performance of classification algorithms. Balancing data protection with classification efficiency will be a key focus for future WBAN developments. As the complexity of WBAN data and applications increases, there is a growing interest in leveraging advanced machine learning models such as reinforcement learning, federated learning, and other AI approaches to enhance classification. Reinforcement learning can be applied to create adaptive classification models that learn from ongoing data and adjust their parameters based on user feedback. This is particularly useful in dynamic environments where user behavior is variable, such as in sports training or rehabilitation applications. Federated learning offers the potential to improve classification accuracy while maintaining data privacy, as it allows WBAN devices to learn collaboratively without sharing raw data. Other advanced AI models, such as self-supervised learning, could further enhance classification by using unlabeled data more effectively. These emerging approaches open new possibilities for WBANs, allowing classification algorithms to become more sophisticated, personalized, and effective. While many classification algorithms show promise in controlled environments, deploying them in real-world WBAN applications presents unique challenges. Factors like sensor placement, environmental interference, device durability, and user movement variability can all affect the performance of classification algorithms in practical settings. For example, wearable sensors may produce different results depending on how securely they are attached or where on the body they are located, which can complicate classification. Additionally, the need for regular maintenance and updates can create logistical challenges, particularly for systems deployed on a large scale, such as in hospitals or remote monitoring programs. Real-world testing and validation of these algorithms under diverse conditions are essential to ensure they can deliver reliable performance outside of lab environments. Future research should focus on developing testing frameworks that replicate real-world conditions and assess

algorithm resilience to common challenges in WBAN deployment [61].

6. Conclusion

The analysis of classification algorithms for Wireless Body Area Networks (WBANs) reveals several important insights. Key findings indicate that while traditional algorithms like decision trees and Naïve Bayes provide efficiency and simplicity, more advanced methods such as support vector machines, neural networks, and ensemble techniques offer higher accuracy, which is essential in applications that require precise, reliable data. Furthermore, security-enhanced techniques, power-efficient optimizations, and latency reduction methods are necessary to ensure WBANs function effectively in real-time and resource-constrained environments. Addressing the unique challenges of node classification in WBANs—such as power constraints, data privacy, and environmental variability—requires a balance between accuracy, efficiency, and security. The implications of using effective classification algorithms in WBANs extend beyond performance; they enhance network trustworthiness and operational reliability. Accurate classification bolsters WBAN security by distinguishing between trusted and untrusted nodes, reducing the risk of data breaches or compromised health monitoring. Efficient and secure classification algorithms help ensure that WBANs can function continuously, especially in healthcare applications where real-time, reliable data is critical. By incorporating robust classification models, WBANs can maintain high standards of security and data integrity while minimizing power consumption, an essential factor for wearable devices that rely on limited battery life. Looking ahead, the future of WBANs will likely involve an increased focus on advanced machine learning and AI-driven techniques to improve both the accuracy and adaptability of node classification. As WBANs become increasingly integrated with the Internet of Things (IoT), addressing data privacy and security challenges will be paramount. Trustworthy node classification will continue to be a cornerstone of effective WBAN performance, ensuring these networks can safely and reliably support healthcare, fitness, and other critical applications.

References

[1] I. I. Al Barazanchi, W. Hashim, R. Thabit, R. Sekhar, P. Shah, and H. R. Penubadi, "Secure Trust Node Acquisition and Access Control for Privacy-Preserving Expertise Trust in WBAN Networks," in *Forthcoming Networks and Sustainability in the AIoT Era*, 2024, pp. 265–275.

[2] I. I. Al Barazanchi, W. Hashim, R. Thabit, R. Sekhar, P. Shah, and H. R. Penubadi, "Secure and Efficient Classification of Trusted and Untrusted Nodes in Wireless Body Area Networks: A Survey of Techniques and Applications," in *Forthcoming Networks and Sustainability in the AIoT Era*, 2024, pp. 254–264.

[3] H. H. Mahmoud *et al.*, "Eco-friendly and Secure Data Center to Detection Compromised Devices Utilizing Swarm Approach," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 3, pp. 102–115, 2024, doi: 10.22266/ijies2024.0630.09.

[4] A. Korneev *et al.*, "Experimental Research in Frequency and Time Domain for Electromechanical System with Distributed Parameters in Mechanical Part," *Math. Model. Eng. Probl.*, vol. 11, no. 4, pp. 1107–1114, 2024, doi: 10.18280/mmep.110429.

[5] H. R. Abdulshaheed, M. M. Abdulrahman, I. Ibraheem, A. Barazanchi, and J. F. Tawfeq, "Identification of Faulty Sensor Nodes in WBAN Using Genetically Linked Artificial Neural Network," *Iraqi J. Comput. Sci. Math.*, pp. 48–58, 2024.

[6] A. L. Khalaf *et al.*, "Real time pedestrian and objects detection using enhanced YOLO integrated with learning complexity-aware cascades," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 22, no. 2, pp. 362–371, 2024, doi: 10.12928/TELKOMNIKA.v22i2.24854.

[7] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al_Barazanchi, "Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach," *Sensors*, vol. 23, no. 3, p. 2023, 2023, doi: 10.3390/s23031431.

[8] A. Ibrahim *et al.*, "Evaluating the Impact of Emotions and Awareness on User Experience in Virtual Learning Environments for Sustainable Development Education," *Ingénierie des systèmes d Inf.*, vol. 29, no. 1, pp. 65–73, 2024, doi: 10.18280/isi.290108.

[9] A. M. Ali, M. A. Ngadi, I. I. Al Barazanchi, and P. S. JosephNg, "Intelligent Traffic Model for Unmanned Ground Vehicles Based on DSDV-AODV Protocol," *Sensors (Basel).*, vol. 23, no. 14, pp. 1–13, 2023, doi: 10.3390/s23146426.

[10] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al Barazanchi, "Enhanced QoS Routing Protocol for an Unmanned Ground Vehicle, Based on the ACO Approach," *Sensors (Basel).*, vol. 23, no. 3, 2023, doi: 10.3390/s23031431.

[11] A. H. Hamad, A. Y. Dawod, and M. F. Abdulqader, "A secure sharing control framework supporting elastic mobile cloud computing," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 2270–2277, 2023, doi: 10.11591/ijece.v13i2.pp2270-2277.

[12] Y. Niu, I. A. M. Al Sayed, A. R. Ali, I. Al Barazanchi, and P. S. Josephng, "Research on fault adaptive fault tolerant control of distributed wind solar hybrid generator," *Bull. Electr. Eng. Informatics*, vol. 12, no. 2, pp. 1029–1040, 2023, doi: 10.11591/eei.v12i2.4242.

[13] A. A. Al-fatlawi and I. Al-barazanchi, "A novel approach for new architecture for green data centre," *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 411–417, 2023, doi: 10.11591/eei.v12i1.4421.

[14] S. A. Sahy, S. H. Mahdi, H. M. Gheni, and I. Al-Barazanchi, "Detection of the patient with COVID-19 relying on ML technology and FAST algorithms to extract the features," *Bull. Electr. Eng. Informatics*, vol. 11, no. 5, pp. 2886–2894, 2022, doi: 10.11591/eei.v11i5.4355.

[15] S. A. Shawkat, B. A. Tuama, and I. Al Barazanchi, "Proposed system for data security in distributed computing in using triple data encryption standard and Rivest Shamir Adlemen," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 6, pp. 6496–6505, 2022, doi: 10.11591/ijece.v12i6.pp6496-6505.

[16] I. Al-Barazanchi *et al.*, "Remote Monitoring of COVID-19 Patients Using Multisensor Body Area Network Innovative System," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–14, Sep. 2022, doi: 10.1155/2022/9879259.

[17] Y. Niu, S. I. Kadhem, I. A. M. Al Sayed, Z. A. Jaaz, H. M. Gheni, and I. Al Barazanchi, "Energy-Saving Analysis of Wireless Body Area Network Based on Structural Analysis," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Jun. 2022, pp. 1–6, doi: 10.1109/HORA55278.2022.9799972.

[18] I. Al Barazanchi *et al.*, "Blockchain: The Next Direction of Digital Payment in Drug Purchase," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Jun. 2022, pp. 1–7, doi: 10.1109/HORA55278.2022.9799993.

[19] I. Al-Barazanchi, H. R. Abdulshaheed, and M. S. Binti Sidek, "A survey: Issues and challenges of communication technologies in WBAN," *Sustain. Eng. Innov.*, vol. 1, no. 2, pp. 84–97, Dec. 2019, doi: 10.37868/sei.v1i2.85.

[20] S. A. Shawkat and I. Al-Barazanchi, "A proposed model for text and image encryption using different techniques," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 20, no. 4, p. 858, Aug. 2022, doi: 10.12928/telkomnika.v20i4.23367.

[21] S. Widadi, S. Al Badrun Munir, N. Shahu, I. Ahmad, and I. Al Barazanchi, "Automatic wireless nurse caller," *J. Robot. Control*, vol. 2, no. 5, pp. 380–384, 2021, doi: 10.18196/jrc.25111.

[22] I. Al_Barazanchi *et al.*, "Proposed New Framework Scheme for Path Loss in Wireless Body Area Network," *Iraqi J. Comput. Sci. Math.*, vol. 3, no. 1, pp. 11–21, 2022, doi: 10.52866/ijcsm.2022.01.01.002.

[23] H. R. Abdulshaheed, H. H. Abbas, E. Q. Ahmed, and I. Al-Barazanchi, "Big Data Analytics for Large Scale Wireless Body Area Networks; Challenges, and Applications," 2022, pp. 423–434.

[24] S. S. Oleiwi, G. N. Mohammed, and I. Al-Barazanchi, "Mitigation of packet loss with end-to-end delay in wireless body area network applications," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 1, pp. 460–470, 2022, doi: 10.11591/ijece.v12i1.pp460-470.

[25] S. A. Shawkat and I. Al-barazanchi, "A proposed model for text and image encryption using different techniques," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 20, no. 4, pp. 858–866, 2022, doi: 10.12928/TELKOMNIKA.v20i4.23367.

[26] I. Al Barazanchi *et al.*, "WBAN System Organization, Network Performance and Access Control: A Review," *7th Int. Conf. Eng. Emerg. Technol. ICEET 2021*, no. October, pp. 27–28, 2021, doi: 10.1109/ICEET53442.2021.9659564.

[27] Z. A. Jaaz, M. E. Rusli, N. A. Rahmat, I. Y. Khudhair, I. Al Barazanchi, and H. S. Mehdy, "A Review on Energy-Efficient Smart Home Load Forecasting Techniques," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2021-Octob, no. October, pp. 233–240, 2021, doi: 10.23919/EECSI53397.2021.9624274.

[28] I. Al_barazanchi, Z. A. Jaaz, H. H. Abbas, and H. R. Abdulshaheed, "Practical application of iot and its implications on the existing software," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2020-Octob, no. October, pp. 10–14, 2020, doi: 10.23919/EECSI50503.2020.9251302.

[29] Z. A. Jaaz, I. Y. Khudhair, H. S. Mehdy, and I. Al Barazanchi, "Imparting Full-Duplex Wireless Cellular Communication in 5G Network Using Apache Spark Engine," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 2021-Octob, no. October, pp. 123–129, 2021, doi: 10.23919/EECSI53397.2021.9624283.

[30] M. H. Ali, A. Ibrahim, H. Wahbah, and I. Al_Barazanchi, "Survey on encode biometric data for transmission in wireless communication networks," *Period. Eng. Nat. Sci.*, vol. 9, no. 4, pp. 1038–1055, 2021, doi: 10.21533/pen.v9i4.2570.

[31] I. Al Barazanchi, W. Hashim, A. A. Alkahtani, H. H. Abbas, and H. R. Abdulshaheed, "Overview of WBAN from Literature Survey to Application

Implementation," *2021 8th Int. Conf. Electr. Eng. Comput. Sci. Informatics*, no. October, pp. 16–21, 2021, doi: 10.23919/eecsi53397.2021.9624301.

[32] I. Al Barazanchi *et al.*, "Proposed a New Framework Scheme for the PATH LOSS in Wireless Body Area Network," *Iraqi J. Comput. Sci. Math.*, vol. 3, no. 1, pp. 11–21, 2022.

[33] I. Al Barazanchi, Y. Niu, S. Nazeri, W. Hashim, and A. A. Alkahtani, "A survey on short-range WBAN communication ; technical overview of several standard wireless technologies," *Period. Eng. Nat. Sci.*, vol. 9, no. 4, pp. 877–885, 2021.

[34] I. Al Barazanchi, A. Murthy, A. Abdulqadir, A. Rababah, and G. Khader, "Blockchain Technology - Based Solutions for IOT Security," *Iraqi J. Comput. Sci. Math.*, vol. 3, no. 1, pp. 1–12, 2022.

[35] I. Al Barazanchi, W. Hashim, A. A. Alkahtani, and H. R. Abdulshaheed, "Survey: The impact of the Corona pandemic on people, health care systems, economic: Positive and negative outcomes," in *The Role of Intellectual in Achieving Sustainable Development after the COVID-19 and the Economic Crisis Conference RICSDCO19EC*, 2021, p. 125, doi: ISBN: 978-9922-9455-3-8.

[36] H. H. Abbas, Z. A. Jaaz, I. Al_Barazanchi, and H. R. Abdulshaheed, "Survey on Enhanced Security Control measures in Cloud Computing systems," *J. Phys. Conf. Ser.*, vol. 1878, no. 1, p. 012004, 2021, doi: 10.1088/1742-6596/1878/1/012004.

[37] I. Al Barazanchi, S. A. Sahy, and Z. A. Jaaz, "Traffic Management with Deployment of Li-Fi Technology," *J. Phys. Conf. Ser.*, vol. 1804, no. 012141, 2021, doi: 10.1088/1742-6596/1804/1/012141.

[38] H. H. A. and H. R. A. I. Al-Barazanchi, Z. A. Jaaz, "Practical application of IOT and its implications on the existing software," *2020 7th Int. Conf. Electr. Eng. Comput. Sci. Informatics (EECSI), Yogyakarta, Indones.*, no. October, pp. 10–14, 2020, doi: 10.23919/EECSI50503.2020.9251302.

[39] S. A. Shawkat, K. S. L. Al-Badri, and I. Al Barazanchi, "Three band absorber design and optimization by neural network algorithm," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020, doi: 10.1088/1742-6596/1530/1/012129.

[40] Z. A. Jaaz, S. S. Oleiwi, S. A. Sahy, and I. Albarazanchi, "Database techniques for resilient network monitoring and inspection," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 18, no. 5, pp. 2412–2420, 2020, doi: 10.12928/TELKOMNIKA.v18i5.14305.

[41] I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, "A Survey : Issues and challenges of communication technologies in WBAN," *Sustain. Eng. Innov.*, vol. 1, no. 2, pp. 84–97, 2020.

[42] I. Al Barazanchi, H. R. Abdulshaheed, M. Safiah, and B. Sidek, "Innovative technologies of wireless sensor network : The applications of WBAN system and environment," *Sustain. Eng. Innov.*, vol. 1, no. 2, pp. 98–105, 2020.

[43] H. R. Abdulshaheed, I. Al Barazanchi, M. Safiah, and B. Sidek, "Survey : Benefits of integrating both wireless sensors networks and cloud computing infrastructure," *Sustain. Eng. Innov.*, vol. 1, no. 2, pp. 67–83, 2020.

[44] I. A. B. Sawsan Ali Hamid , Rana Alauldeen Abdalrahman , Inam Abdullah Lafta, "Web Services Architecture Model to Support Distributed Systems," *J. SOUTHWEST JIAOTONG Univ. Vol.*, vol. 54, no. December, pp. 52–57, 2019, doi: 10.4018/978-1-60960-192-8.ch011.

[45] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 6, pp. 2818–2825, 2019, doi: 10.12928/TELKOMNIKA.v17i6.13201.

[46] H. R. Abdulshaheed, I. Al Barazanchi, H. T. Jaya, and D. Tunggal, "Smart Solutions Based-On Cloud Computing and Wireless Sensing," *Int. J. Adv. Sci. Technol.*, vol. 28, no. 8, pp. 526–542, 2019.

[47] I. Al Barazanchi, H. R. Abdulshaheed, and A. Shibghatullah, "The Communication Technologies in WBAN," *Int. J. Adv. Sci. Technol.*, vol. 28, no. 8, pp. 543–549, 2019.

[48] N. J. Qasim, S. M. Mohammed, A. S. Sosa, and I. Al Barazanchi, "Reactive protocols for unified user profiling for anomaly detection in mobile Ad Hoc networks," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 843–852, 2019.

[49] I. Al Barazanchi, "An Analysis of the Requirements for Efficient Protocols in WBAN," *J. Telecommun. Electron. Comput. Eng.*, vol. 6, no. July, p. 43, 2014.

[50] H. R. Bdulshaheed, Z. T. Yaseen, and I. I. Al-barazanchi, "New approach for Big Data Analysis using Clustering Algorithms in Information," *Jour Adv Res. Dyn. Control Syst.*, vol. 2, no. 4, pp. 1194–1197, 2019.

[51] I. Al Barazanchi and H. R. Abdulshaheed, "Adaptive Illumination Normalization Framework based on Decrease Light Effect for Face Recognition," *Jour Adv Res. Dyn. Control Syst.*, vol. 11, no. 01, pp. 1741–1747, 2019.

[52] A. S. Abdullah, M. A. Abed, and I. Al Barazanchi, "Improving face recognition by elman neural network using curvelet transform and HSI color space," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 430–437, 2019.

[53] S. Rashid, A. Ahmed, I. Al Barazanchi, and Z. A. Jaaz, "Clustering algorithms subjected to K-mean and gaussian mixture model on multidimensional data set," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 448–457, 2019.

[54] S. Rashid, A. Ahmed, I. Al Barazanchi, A. Mhana, and H. Rasheed, "Lung cancer classification using data mining and supervised learning algorithms on multi-dimensional data set," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 438–447, 2019.

[55] I. Al Barazanchi, S. A. Hamid, R. A. Abdulrahman, and H. Rasheed, "Automated telemedicine and diagnosis system (ATDS) in diagnosing ailments and prescribing drugs," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 888–894, 2019.

[56] I. Al Barazanchi, H. R. Abdulshaheed, S. A. Shawkat, and S. R. Binti, "Identification key scheme to enhance network performance in wireless body area network," *Period. Eng. Nat. Sci.*, vol. 7, no. 2, pp. 895–906, 2019.

[57] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, "Proposed a Smart Solutions Based-on Cloud Computing and Wireless Sensing," *Int. J. Pure Appl. Math.*, vol. 119, no. 18, pp. 427–449, 2018.

[58] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, "A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing," *Int. J. Pure Appl. Math.*, vol. 119, no. 18, pp. 461–486, 2018.

[59] I. Al Barazanchi, A. S. Shibghatullah, and S. R. Selamat, "A New Routing Protocols for Reducing Path Loss in Wireless Body Area Network (WBAN)," *J. Telecommun. Electron. Comput. Eng. Model*, vol. 9, no. 1, pp. 1–5, 2017.

[60] A. Shibghatullah and I. Al Barazanchi, "A survey on Central Control Unit (CCU) in WBAN," *Int. Symp. Res. Innov. Sustain. 2014 (ISoRIS '14) 15-16 Oct. 2014, Malacca, Malaysia*, vol. 14, no. October, pp. 15–16, 2014.

[61] A. S. Shibghatullah and I. Al Barazanchi, "An Analysis of the Requirements for Efficient Protocols in WBAN," *J. Telecommun. Electron. Comput. Eng.*, vol. 6, no. 2, pp. 19–22, 2014.