Security Issues and Research Opportunities in Wireless Body Area Networks

Qazi Ejaz Ali[1*], Abdul Haseeb Malik[1], Waheed Ur Rehman[1], Muhammad Haseeb[1], Tabinda Salam[2]

[1]Department of Computer Science, University of Peshawar 25120, Pakistan.

[2]Department of Computer Science, SBBWU, Peshawar, Pakistan.

*****Correspondence**: qaziejazali@uop.edu.pk

Citation | Ali. Q. E, Malik. A. H, Rehman. W. U, Haseeb. M, Salam. T, "Security Issues and Research Opportunities in Wireless Body Area Networks", IJIST, Vol. 07 Issue. 03 pp 1881-1894, August 2025

DOI | https://doi.org/10.33411/ijist/20257318811894

Received | July 28, 2025 **Revised |** August 09, 2025 **Accepted |** August 11, 2025 **Published |** August 12, 2025.

Wireless Sensor Networks (WSNs) have found application in diverse fields, one of is Wireless Body Area Networks (WBANs). WBANs are essential networks for fitness diagnostics, observation, and flexible actuators, which rely on data gathered from numerous wireless sensors installed in or above the human body. Due to the Ad hoc nature of WBANs, there are security concerns, which can affect the confidentiality, authenticity, and integrity of data. Security and privacy play a critical role in ensuring secure communication by helping networks prevent unauthorized access and avoid fraudulent activities. Despite its significance, no survey has been conducted in WBANs in terms of computation and communication overheads, Man in the Middle attack (MIMA), Denial of Service (DoS), and Spoofing attacks. This paper helps the new researcher in WBANs security to better understand the area and the need for designing new schemes that focus on the aforementioned parameters.

Keywords: WBAN, Security, MIMA, DoS, Spoofing

Introduction:

Wireless Sensor Networks (WSNs) have undergone a significant transformation through the integration of wireless communications, microelectronics, distributed processing systems, ad hoc networks, sensor applications, and implantable technologies. WSNs consist of multiple distributed sensors that are designed to monitor and record environmental conditions, with the collected data subsequently transmitted to a base station [1]. Wireless Sensor Networks (WSNs) have been applied in various fields, including healthcare monitoring. The significance of medical observing has increased due to its capability of providing real-time data and communication. The use of WSNs in healthcare is known as Wireless Body Area Networks (WBANs). WBANs represent a specialized category of sensor networks that leverage the Internet to connect patients with healthcare providers, facilitating the transmission of critical health information [2]. WBANs are essential networks for fitness diagnostics, observation, and flexible actuators, which rely on data gathered from numerous wireless sensors installed in or above the human body. There are numerous returns of WBAN, such as locality independent checking, no disruption to patients' movement, timely detection and stoppage of diseases, and distant patient assistance, amongst others. Therefore, it is highly suitable for continuous monitoring, enabling accurate analysis and providing on-time response to health professionals [3].

In [4], the authors highlighted that WBANs are a key application of the Internet of Things (IoT), aimed at enhancing the quality of patient care. The IoT market is projected to exceed 19 trillion USD in the coming years [5]. Therefore, it is expected that by 2025, more than 100 billion IoT devices will be functioning worldwide, with an estimated monetary value of more than $11 trillion USD [6]. Among the most influential wireless sensor tools for healthcare, WBANs allow healthcare system users to access real-time statistics for critical uses like inaccessible health observing, sports, home-based patient care, substitute comeback, and timely disturbance revealing [7][8][9][10]. Nonetheless, the absence of robust information protection mechanisms in such a networking model renders sensitive medical data vulnerable to illegitimate access by malicious actors. This puts the security and privacy of users' data at risk, with potential adverse effects proceeding patients. Such as, if a patient experiences a heart attack, wireless sensors installed in or above their body can detect the event. Therefore, within a public network, it is vital to ensure user and data protection to enable doctors to initiate treatment quickly [11][12].

Ensuring the security of WBANs requires a strong protective framework. Authentication and confidentiality are two primary concerns that need attention, typically addressed through the use of encryption and digital signatures [13]. When both encryption and signing are necessary simultaneously, the sign-then-encrypt method is commonly employed. However, due to the severe restrictions linked with low-end WBANs detecting procedures, such as inadequate committed energy and CPU competencies, complicated cryptographic procedures are not feasible. To address this challenge, an integrated approach called signcryption is employed [14]. Additionally, signcryption is more suitable for resource-constrained scenarios like WBANs than using signatures based on encryption, primarily due to its lower cost.

Considering the entire WBAN environment, data communication can be organized into multiple layers. It is important to note that as a person moves, the positions of the sensors attached to their body may also change. Therefore, WBANs are inherently dynamic. According to the WBAN standards [15][16][17], communication is generally classified into three levels: Tier-1 of WBANs refers to Intra-BAN Communications, which can be either wired or wireless. The authors in [18] proposed a communication scheme in which only the sink and sensors are connected, focusing on intra-BAN communication [19]. The communication range of this tier is approximately two meters in and around the body. For instance, the sensors are placed in the link range; this tier is crucial. Therefore, the mode of communication is narrow in range. The communication technologies, which are ZigBee and Bluetooth, are used in this layer [20][21]. The sensors monitor physiological parameters and transmit the data to a sink located at the boundary of Tier-1. The sink then processes this information and forwards it to the next level, Tier-2 [17][22][23]. In addition to facilitating inter-network connectivity, Tier-2 is responsible for routing data between the access points and the corresponding sinks in Tier-1. The communication range of this tier is usually up to a few hundred meters, which is significantly larger than Tier-1. However, due to the limited communication range, access points must be strategically positioned to ensure reliable data transfer between Tier-1 and Tier-3. Access points can be connected to the Internet, enabling remote access to the data collected by WBANs and allowing for the monitoring and management of patients' health from a distance. Tier-3 connects WBANs to the Internet or other wide area networks, enabling healthcare providers to remotely access and manage patient data. This layer ensures global connectivity, supporting continuous monitoring of patient health. The communication technologies employed in this layer are typically based on the Internet Protocol (IP), such as Wi-Fi, WiMAX, and cellular networks. This layer provides a wide range of services, including telemedicine, remote patient monitoring, and emergency response services, among others. It allows healthcare providers to remotely access patient data and provides patients with the ability to communicate with healthcare professionals regardless of their location [23]. The database in Tier-3 is a critical component in WBANs as it stores the patient's profile, medical history, and other relevant information. Medical professionals can access the database to remotely monitor and assess a patient's health status. When the patient's condition deteriorates, the system can generate an alert or notification to the concerned healthcare providers to take immediate action based on the patient's medical history and real-time data collected from the WBAN sensors. This approach can potentially save lives by enabling timely medical intervention and treatment [17][24]. In practice, the sink in Tier-1 can connect to an Access Point (AP) via 4G, 5G, or 6G, which forms part of Tier-2's communication technologies. This setup enables a more direct connection to the Internet or other networks for data transmission and retrieval, eliminating the need to rely on Tier-2's inter-BAN communications. However, this approach demands higher power and may not be suitable for all WBAN applications. It is common in the first-tier communication to have 2 BANs depicted, through the body nodes and fixed nodes range all over the body, as shown in Figure 1. The nodes can either be directly connected to the center or by the relay nodes.

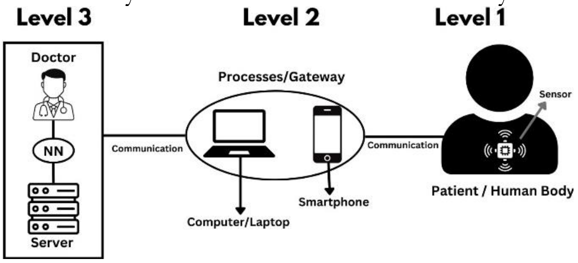

Figure 1. WBAN level of communication

Table 1 shows a comparative summary for Tier 1, Tier 2, and Tier 3 with respect to communication types, range, technology, and purpose.

Table 1. WBAN Communication Tiers

Tier	Communication Type	Range	Technologies	Purpose
Tier-1 (Intra-BAN)	Intra-body communication (wired or wireless) between sensors and sink	Up to 2 meters (in and around the body)	ZigBee, Bluetooth, UWB	- Monitors physiological signals (e.g., heart rate, temperature) - Transmits data from body sensors to the sink

				- Narrow, energy-efficient communication
Tier-2 (Inter-BAN / Personal Network)	Communication between sinks and access points	Up to a hundred meters	Wi-Fi, LTE, 4G/5G/6G, ZigBee gateway, Bluetooth	- Aggregates data from Tier-1 sinks - Routes data to Tier-3 (Internet/cloud) - Enables remote access to WBAN data
Tier-3 (Beyond BAN / Wide Area Network)	WBAN-to-Internet or WAN communication	Beyond a hundred meters to global connectivity	Internet Protocol (IP) based: Wi-Fi, WiMAX, 4G/5G/6G, Satellite, Cloud services	- Provides global connectivity - Supports telemedicine, emergency response, and remote monitoring. Stores medical history, profiles, and real-time health data

As reported in [23], WBANs are being applied across diverse domains, including healthcare, entertainment, defense, and sports. As noted in [25], WBANs play a crucial role in healthcare by facilitating the transmission of patient information during emergencies, thereby contributing to the preservation of life. According to [26], WBANs involve the placement of the sensors on the human body, which persistently observe in real time the patient's health. Slightly anomalous fluctuations in the patients' healthiness, for example, low heart rate, high temperature, or supplementary indications, are communicated to the physician through the internet, enabling quick and timely intervention. In [27], the authors categorize WBAN applications into two types: implantable sensors and wearable sensors. An implantable sensor, which is surgically placed inside the human body and not intended for removal, is used for continuous patient monitoring. On the other hand, a wearable sensor is utilized when patients need to be monitored and can be removed at any time. The wearable sensor node is designed to detect patient movements and unusual positions. For example, wearable devices like personal digital assistants can help monitor various health parameters, including blood glucose, body temperature, SpO_2, heart function, and blood pressure [28].

Figure 2 illustrates the diverse range of applications that are being developed using WBANs, comprising remote healthcare, local aided active, and worker-centric uses, such as smart households and gaming. While human activity recognition has gained considerable attention in recent years, WBANs are increasingly being applied in healthcare, particularly for remote monitoring, early diagnosis, and the management of chronic diseases in eldercare. Ambient assisted living applications can also help older adults maintain their independence in their daily routines. Moreover, WBANs are also useful in the entertainment industry as they facilitate data streaming operations.

Furthermore, WBANs have applications in tracking an athlete's training regime and physical health in various sports such as swimming, hammer throwing, volleyball, football, cricket, and related events. By analyzing the sensory data collected, customized metrics can be developed to improve performance while also maintaining user comfort [29]. Wearable sensors can detect body movements in water sports such as swimming and water volleyball, and are capable of adapting communication mediums between water and air. These applications require water-resistant sensor enclosures and intelligent Media Access Control (MAC) protocols that can dynamically switch communication mediums as needed. Additionally, in military settings, WBANs play a crucial role in enabling medical personnel to monitor the health of soldiers and locate them in emergencies.

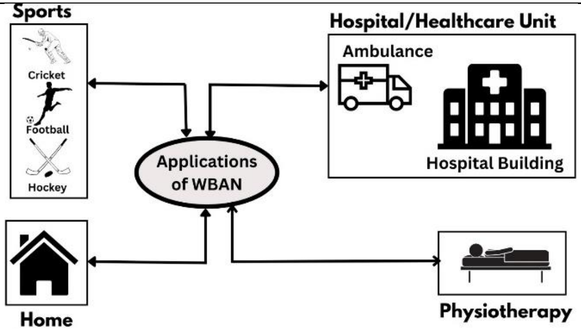

Figure 2. WBAN Applications

WBANs are anticipated to be employed in the future for emergency response and disaster relief situations, for instance, flood and fire rescues [30]. Once body sensors are utilized in disaster relief operations, ache signals are directed, which can be selected by rescue apparatus or transmitted via nearby BANs [31]. Consequently, WBAN applications have acquired a significant new aspect that demands communication capabilities not only within the same Body Area Network (BAN) but also across different BANs in a heterogeneous environment. A wide range of sensors, such as temperature and multimedia sensors, are used in combination with GPS for these applications, with the volume of transmitted data varying depending on the sensor type employed. The ability of flood rescue sensors to send statistics through both air and water forces the use of intelligent MAC procedures.

Sensors are utilized in all of these applications either on, in, or around the human body, and they gather data on the user's behavior. Consequently, the close integration of humans with the system raises concerns about its overall security and reliability. Maintaining the integrity of data is a crucial prerequisite for WBANs' uses, for the reason that inaccurate statistics regarding one's body vitals could lead to improper treatment and potentially deadly outcomes. Moreover, safeguarding the confidentiality of user data is critical, as these applications may expose sensitive details about daily activities and behavior, potentially affecting an individual's social well-being. Even a small piece of evidence or fabrication regarding a participant's qualification could harm their reputation. Therefore, it is imperative to continuously enhance the security of WBAN applications to ensure the accuracy and long-term sustainability of the observing applications they are intended for. As more events become integrated with such applications, it becomes increasingly important to establish rigorous security requirements. In recent years, there has been growing interest in authentication research within the field of WBAN security. To strengthen WBAN security, several comprehensive surveys and analyses of state-of-the-art authentication methods have been presented in the literature. Though both security and privacy are vital components of WBANs safety, and regrettably, nobody in the current reviews examines security and privacy solutions critically.

Objectives of this research:

This paper provides readers with a summary of WBANs technology, security needs, and architecture, aiming to give them a fundamental comprehension of the research field.

This study comprehensively reviews the security and privacy methods suggested to safeguard the infrastructure of WBANs.

Apart from providing a comprehensive analysis of the current security schemes for securing WBANs in terms of security and privacy, this survey also includes comprehensive explanations of the threats that aim to exploit these techniques.

An investigation of interrelated studies has been conducted to establish the novelty of the proposed review in terms of computational and communication overheads, Man in the Middle (MIM), DoS, and Spoofing attacks.

This study presents the future research opportunities and the issues in the subject domain, providing potential avenues for further investigation and exploration.

The remainder of this paper is distributed into different sections, which are the following:

Related security and privacy Survey Presented for WBANs:

The primary objective of this review study is to offer a summation of the most recent research papers on security and privacy, and future developments in the security of WBANs. Relevant information on the research topic is scattered across numerous previously published papers. To gather these resources, widely used online databases such as IEEE Xplore, Springer, and ScienceDirect were consulted. As a second step, a guided search was conducted in the relevant area. Furthermore, efforts were made to review all security and privacy studies in the field of WBANs. In [32], researchers stressed the primary security necessities and concerns related to Denial of Service (DoS) attacks in WBANs. The authors also provided a comprehensive overview of key security features and identified prevalent attacks on WBANs across different layers. Lastly, they conducted an in-depth evaluation of the prevailing security protocols.

In 2011, the researchers in [33] conducted a study to examine potential attacks on resource-constrained WBANs and analyzed communication protocols, cryptographic techniques, and key management methods relevant to WBAN security and privacy. The researchers also examined the flaws of existing solutions and identified potential research areas in WBANs security that could be explored in the future.

In [34], the authors provided an acute investigation of possible authentication methods for WBANs. The discussion and reviews were guided by the IEEE 802.15.6 standard. In [35], the researchers investigated major security and privacy issues as well as potential attacks in WBANs. The authors also highlighted an unresolved Quality of Service (QoS) issue in WBANs, which may give rise to significant security challenges. Lastly, the novelists outlined forthcoming research guidelines that could be explored in the field of WBANs.

The researchers in [36] provided an overview of the current state of security aspects in existing WBANs. In addition, the researchers highlighted several significant security challenges. In [37], the authors gave an overview of WBANs and allied experiments with a specific emphasis on safety issues. They discussed WBANs' security attacks, WBANs' security requirements, and vulnerability assessments.

In [34], the authors proposed a taxonomy of attacks in WBANs, categorized as physical, link, network, transport, and application layer attacks. The authors also examined existing weaknesses and potential security issues and further provided recommendations for enhancing WBAN security. In [38], the researchers presented a comprehensive overview of existing security and privacy mechanisms in WBANs is presented. In addition, the authors highlighted the potential security threats and challenges that WBANs face. Finally, the authors suggest possible future research directions in this field.

The authors of [39] conducted a survey of WBANs' security protocols and techniques, including authentication, confidentiality, integrity, and availability. The authors also examine existing security and privacy challenges and propose potential solutions. Lastly, the writers suggest possible future research directions in this field.

In [38], the authors also examined potential attacks and defenses, as well as future research areas that can be pursued in the domain of WBAN security. The authors of [39] examined the security of healthcare information systems, including WBANs, discussing various security challenges and potential attacks, along with existing solutions and future research directions. Lastly, the writers provide a comparative analysis of the present WBAN security procedures.

In [40], a comprehensive survey of the recent advancements in security and privacy issues of WBANs, with a focus on the authentication and key management schemes, is presented. The authors also discussed the emerging technologies and standards related to WBANs' security and privacy. Similarly, a survey in [41] provides a comprehensive review of WBANs' security requirements, attacks, and existing security protocols, as well as the gains and restrictions of these protocols. Finally, the authors outlined potential future research directions for enhancing WBAN security.

The study in [40] investigated the suitability of various secure communication technologies for use within WBANs, as well as for external communication between WBANs and other organizations. They also highlighted the crucial security requirements that must be met for secure transmission at both levels. Meanwhile, in [41], the authors provided an in-depth review of key research on mobile, ubiquitous, and WBANs, with a specific focus on the challenges related to routing and security. However, they did not critically analyze the security and privacy attacks.

In [42], the authors showed a broad analysis of several authentication approaches. They evaluated the techniques based on factors such as security threats, safety features, and additional relevant issues. Meanwhile, in [43], the researchers provided a concise summary of WBAN security, proposing a classification to categorize entities involved in healthcare systems. The authors identified important topics and potential research directions related to security issues at all layers of WBANs.

In [44], the researchers presented a comprehensive outline of the main security necessities and potential threats in WBANs across the various communication layers. The authors first provided a summary of WBANs for healthcare observing, followed by a discussion of cryptographic explanations for solving the security and privacy concerns. In [45], the authors focused on the security and key management of intra-BAN communication. They analyzed existing key agreement methods, but did not consider the potential threats properly. In [46] the researchers proposed multiple design solutions for WBANs, accompanied by a thorough analysis of security facilities. The main objective of the survey was to provide a comprehensive overview of the security aspects of the entire WBAN system. Similarly, in [47], the authors provided an overall summary of WBANs, their uses, and safety apprehensions based on recent research.

The authors of [48] presented a methodical literature review of the security and privacy concerns of E-healthcare schemes in WBANs. Meanwhile, the authors of [49] identified design issues in WBANs' authentication protocols. Furthermore, the authors suggested significant research prospects for the communities in this field. In [50], the researchers investigated the security and privacy challenges of WBANs, proposed solutions, and described the category of authentication methods used. Similarly, in [51], the researchers provided a summary of WBANs and their belongings, including a classification of several authentication schemes. The study also compared numerous verification techniques, highlighted their pros and cons, performance assessment, and strengths against numerous security threats. Lastly, the researchers sketched upcoming guidelines, which could be followed in the area. The authors of [52] provided a comprehensive evaluation of the issues in WBANs concerning communication and security. However, the authors' review of major security concerns was found to be lacking. On the other hand, the researchers in [53] conducted a study on WBANs that focused on significant security requirements and concerns regarding Denial of Service attacks.

In [54], the researchers conducted a detailed analysis of the security and privacy challenges of both WSNs and WBANs. The study examined the features, architecture, management measures, and uses of both systems, followed by a comparative analysis. The authors also identified exposed research challenges for future studies. In contrast, the researchers of [55] on evaluating the routing, security, energy, and cost-cutting issues of WBANs.

The authors of [56] provided a comprehensive outline of the technology involved in WBANs with a particular emphasis on security and privacy apprehensions, proposed solutions, research guidelines, and open problems. However, the authors' focus is solely on authentication schemes. On the other hand, the researchers of [57] covered several security processes and routing questions, which WBANs encounter, as well as potential attacks on the network and the mechanisms in place to prevent them. The researchers also examined the security of different attack scenarios and summarized the main challenges faced by users when creating a WBAN network, which has become a new area. This appears to be a comprehensive and valuable study, as reviewing and evaluating existing security approaches is essential for identifying potential weaknesses and enhancing the protection of sensitive data in healthcare systems. Using quality assessment criteria and considering recent work can help ensure that the identified techniques are relevant and effective. Implementing strong encryption algorithms, such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), can significantly enhance data security and privacy. Equally important is the evaluation of these security measures against diverse attack scenarios to ensure their robustness and effectiveness. In [58], the authors presented a comprehensive review of security and authentication schemes and solutions in WBANs. Unlike previous surveys that addressed these issues in a fragmented way, this study adopts a holistic perspective by examining key aspects of security, including risks, potential attackers, and countermeasures. They provided a detailed explanation of security techniques in WBANs along with their functionality, technology, and building blocks. Moreover, the study discusses the applications of WBANs, investigation challenges, endorsements, and future guidelines. Generally, this review offers a broader understanding of WBANs' security and authentication, and suggests potential avenues for further exploration. Author [59] designed a good technique to address certain issues of WBANs security, but prone to DoS, MIMA, and Spoofing attacks. The researchers [60] designed an approach using a blockchain technique to address security issues. However, it introduces high computation and communication costs. Similarly, author [61] designed a good approach, but prone to MIMA and Spoofing Attacks. Author [62] introduced a good approach, but prone to DoS and MIMA attacks.

WBANs have been a well-established topic of research for a significant period, leading to the publication of several survey and technical papers that compile research on different features of the domain. The investigations discussed above mainly focus on topics such as authentication, architecture, security, and challenges. The papers under discussion contributed to the literature by covering security requirements, applications, security methods, and the organization of existing security structures based on cryptography and algorithms. The study also provides an overview of recently presented techniques, a collected list of the security and privacy properties of these schemes, and a discussion of approaches for evaluating the security and privacy, and performance of WBANs. The main objective of this survey is to provide a comprehensive organization, different types of attacks, analysis, and comparison of security and privacy methods for WBANs, which is given in Table 2.

Taxonomy and Security Requirements:

Depending on the form of cryptographic approach used, the security and privacy schemes for WBANs can be broadly classified into 3 categories:

Symmetric Key Schemes: In this category, the same secret key is used for both encryption and decryption of messages. Symmetric key algorithms are faster than asymmetric key algorithms and require less computational overhead. Symmetric key schemes such as CLEFIA-SC, PRESENT-SC, and HIGHT-SC have been applied in WBANs; however, their functionality is largely limited to ensuring confidentiality, without adequately addressing other security needs.

Asymmetric Key Schemes: In this category, two different keys, namely the public key and the private key, are used for encryption and decryption of messages, respectively. Asymmetric key algorithms provide better security and key management than symmetric key algorithms. Examples of asymmetric key schemes for WBANs include RSA-SC, ECC-SC, and NTRU-SC. However, the computational costs of these schemes are high in general.

Hybrid schemes: These techniques combine both the symmetric key and asymmetric key cryptographic concepts to address the security and privacy of WBANs efficiently. Examples of hybrid schemes include AES-SC, RSA-SC, and ECC-SC. However, there are different types of attacks, which should be avoided.

Based on the security requirements of WBANs, security and privacy schemes can be classified as follows:

Confidentiality: This requirement ensures that the data transmitted over the WBANs is protected from unauthorized access and interception.

Integrity: This requirement ensures that the data transmitted over the WBANs is not tampered with or altered during transmission.

Authentication: This requirement ensures that the sender and receiver of the data transmitted over the WBANs are verified and authenticated.

Non-repudiation: This requirement ensures that the sender of the information cannot deny that he/she sent it, and the receiver of the data cannot deny having received it.

Key Management: This requirement ensures that the secret keys used for encryption and decryption of messages are properly managed, distributed, and updated.

These are the main categories for the classification of security and privacy techniques for WBANs based on the type of cryptography used and WBAN's security requirements.

Comparison of Security schemes and Research opportunities:

Based on the literature, Table 2 provides a comparison of the security schemes in WBANs that give direction to the researchers to remove the shortcomings of the schemes and develop their own schemes. In WBANs, if the computational cost of the message generation and verification is more than 1 second, it is considered high, if more than 100ms and less than 1 second, it is considered moderate, and if less than 100ms, it is considered low [63][64].

Table 2. Comparison of the security schemes and their shortcomings

Research paper	Computational cost	Communication overheads	Man In the Middle Attack	DoS Attack	Spoofing Attack
[5]	Low	High	Yes	No	Yes
[6]	High	Moderate	No	Yes	Yes
[8]	Low	Low	Yes	Yes	Yes
[9]	Moderate	Low	Yes	Yes	No
[12]	High	High	No	Yes	No
[14]	High	High	Yes	No	Yes
[25]	Moderate	Moderate	No	Yes	No
[26]	Moderate	Moderate	Yes	No	Yes
[29]	High	Moderate	Yes	Yes	N0
[31]	High	High	Yes	No	Yes
[49]	Moderate	Moderate	Yes	No	No
[59]	Moderate	Moderate	Yes	Yes	Yes
[60]	High	High	No	Yes	No
[61]	Low	Low	No	Yes	Yes
[62]	Moderate	Moderate	Yes	Yes	No

Conclusion:

Security and privacy play a critical role in ensuring secure communication by helping networks prevent unauthorized access and avoid fraudulent activities. Despite its significance, no comprehensive survey has been conducted in WBANs on security, privacy, and privacy procedures till now. This paper fills this gap by providing a detailed analysis of various security and privacy techniques in WBANs. In this paper, useful information and features of these techniques are presented in tabular form and developed diagrams to showcase their architecture, taxonomy, and analysis in a presentable way. The survey begins by introducing WBAN's basic information, including its architecture, applications, and requirements related to security and privacy. This information is decisive for researchers to increase WBANs' better understanding and to develop efficient security and privacy techniques. This review classified different WBANs security and privacy schemes with computational and communication overheads, MIMA, DoS, and spoofing attacks. This research is expected to be useful for researchers interested in this specialized area. With WBANs being one of the utmost favorable technologies in e-health, they are poised to modernize healthcare by providing numerous services and reducing the need for traditional hospitals. However, due to wireless communication, WBANs face several security risks, making secure, security and privacy a critical issue. Efficient security and privacy solutions are necessary to prevent illegal activities and unwanted users in the network.

Future Recommendations:

Future research in this area should focus on developing lightweight, energy-efficient mechanisms with enhanced security and privacy features to ensure secure communication in WBANs efficiently.

References:

[1] V. D. Gaikwad and S. Ananthakumaran, “A Review: Security and Privacy for Health Care Application in Wireless Body Area Networks,” *Wirel. Pers. Commun.*, vol. 130, no. 1, pp. 673–691, May 2023, doi: 10.1007/S11277-023-10305-7/METRICS.

[2] M. Seyedi, B. Kibret, D. T. H. Lai, and M. Faulkner, “A survey on intrabody communications for body area network applications,” *IEEE Trans. Biomed. Eng.*, vol. 60, no. 8, pp. 2067–2079, 2013, doi: 10.1109/TBME.2013.2254714,.

[3] M. Z. K. Farman Ullah, “Energy Efficiency and Reliability Considerations in Wireless Body Area Networks: A Survey,” *Comput. Math. Methods Med.*, p. 1090131, 2022, doi: 10.1155/2022/1090131.

[4] C. C. Sobin, “A Survey on Architecture, Protocols and Challenges in IoT,” *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1383–1429, Jun. 2020, doi: 10.1007/S11277-020-07108-5/METRICS.

[5] M. Soni and D. K. Singh, “LAKA: Lightweight Authentication and Key Agreement Protocol for Internet of Things Based Wireless Body Area Network,” *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1067–1084, Nov. 2022, doi: 10.1007/S11277-021-08565-2/METRICS.

[6] T. Limbasiya and A. Karati, “Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things,” *Int. Conf. Inf. Netw.*, vol. 2018-January, pp. 168–173, Apr. 2018, doi: 10.1109/ICOIN.2018.8343105.

[7] G. Aceto, V. Persico, and Antonio Pescapé, “Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0,” *J. Ind. Inf. Integr.*, vol. 18, p. 100129, 2020, doi: https://doi.org/10.1016/j.jii.2020.100129.

[8] A. Arif, M. Zubair, M. Ali, M. U. Khan, and M. Q. Mehmood, “A Compact, Low-Profile Fractal Antenna for Wearable On-Body WBAN Applications,” *IEEE Antennas Wirel. Propag. Lett.*, vol. 18, no. 5, pp. 981–985, May 2019, doi: 10.1109/LAWP.2019.2906829.

[9] A. Sharma and R. Kumar, “A constrained framework for context-aware remote E-

healthcare (CARE) services," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 8, p. e3649, Aug. 2022, doi: 10.1002/ETT.3649;WGROUP:STRING:PUBLICATION.

[10] M. Haghi Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *J. Netw. Comput. Appl.*, vol. 192, p. 103164, Oct. 2021, doi: 10.1016/J.JNCA.2021.103164.

[11] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, "Privacy in the Internet of Things for Smart Healthcare," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 38–44, Apr. 2018, doi: 10.1109/MCOM.2018.1700809.

[12] M. Shingala, C. Patel, and N. Doshi, "An Improve Three Factor Remote User Authentication Scheme Using Smart Card," *Wirel. Pers. Commun.*, vol. 99, no. 1, pp. 227–251, Mar. 2018, doi: 10.1007/S11277-017-5055-9.

[13] A. H. El-Kady, S. Halim, and F. K. , Mahmoud M. El-Halwagi, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Saf. Environ. Prot.*, vol. 173, pp. 384–413, 2023, doi: https://doi.org/10.1016/j.psep.2023.03.012.

[14] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)," *Adv. Cryptol. — CRYPTO '97*, pp. 165–179, 2006, doi: https://doi.org/10.1007/BFb0052234.

[15] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Networks*, vol. 17, no. 1, pp. 1–18, Jan. 2011, doi: 10.1007/S11276-010-0252-4/METRICS.

[16] R. Punj and R. Kumar, "Technological aspects of WBANs for health monitoring: a comprehensive review," *Wirel. Networks*, vol. 25, no. 3, pp. 1125–1157, Apr. 2019, doi: 10.1007/S11276-018-1694-3/METRICS.

[17] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014, doi: 10.1109/SURV.2013.121313.00064.

[18] T. Zimmerman, "Personal Area Networks (PAN): Near-Field Intra-Body Communication," *Thesis MASTERS Sci. MEDIA ARTS Sci. Neil Gershenfeld*, 1995, [Online]. Available: http://researchgate.net/publication/371667121_Personal_Area_Networks_PAN_Near-Field_Intra-Body_Communication

[19] W. A. N. Wan Abdullah, N. Yaakob, M. E. Elobaid, M. N. Mohd Warip, and S. A. Yah, "Energy-efficient remote healthcare monitoring using IoT: A review of trends and challenges," *ACM Int. Conf. Proceeding Ser.*, vol. 22-23-March-2016, Mar. 2016, doi: 10.1145/2896387.2896414;WGROUP:STRING:ACM.

[20] "What is the ZigBee Alliance? | DigiCert FAQ." Accessed: Sep. 02, 2025. [Online]. Available: https://www.digicert.com/faq/industry-standards-for-security-and-trust/what-is-the-zigbee-alliance

[21] "Bluetooth® Technology Website." Accessed: Sep. 02, 2025. [Online]. Available: https://www.bluetooth.com/

[22] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," *Mob. Networks Appl.*, vol. 16, no. 2, pp. 171–193, 2011, doi: 10.1007/s11036-010-0260-8.

[23] R. Negra, I. Jemili, and A. Belghith, "Wireless Body Area Networks: Applications and Technologies," *Procedia Comput. Sci.*, vol. 83, pp. 1274–1281, 2016, doi: 10.1016/j.procs.2016.04.266.

[24] K. C. D. Sharma, "Body area networks: A survey".

[25] M. A. D. Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, "A lightweight and secure two-factor authentication scheme

for wireless body area networks in health-care IoT," *Comput. Networks*, vol. 177, p. 107333, 2020, doi: https://doi.org/10.1016/j.comnet.2020.107333.

[26] K. Chen, X. Lu, R. Chen, and J. Liu, "Wireless wearable biosensor smart physiological monitoring system for risk avoidance and rescue," *Math. Biosci. Eng.*, vol. 19, no. 2, pp. 1496–1514, 2022, doi: 10.3934/MBE.2022069,.

[27] J. V. Ananthi and P. S. H. Jose, "A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications," *Int. J. Wirel. Inf. Networks*, vol. 28, no. 4, pp. 451–466, Dec. 2021, doi: 10.1007/S10776-021-00538-3/METRICS.

[28] T. H. H. A. Carlos A. Tavera, Jesús H. Ortiz, Osamah I. Khalaf, Diego F. Saavedra, "Wearable Wireless Body Area Networks for Medical Applications," *Comput. Math. Methods Med.*, 2021, doi: https://doi.org/10.1155/2021/5574376.

[29] Y. Fu and J. Liu, "Monitoring system for sports activities using body area networks," *BODYNETS 2013 - 8th Int. Conf. Body Area Networks*, pp. 408–413, Oct. 2013, doi: 10.4108/ICST.BODYNETS.2013.253675.

[30] S. Maitra, T.; Roy, "Research challenges in BAN due to the mixed WSN features: Some perspectives and future directions," *IEEE Sens. J*, vol. 17, pp. 5759–5766, 2017.

[31] L. Huang, R.; Chu, "Disaster rescue mode for body area networks," *US Pat.*, 2016, [Online]. Available: https://patents.google.com/patent/US9247375B2/en

[32] Sana Ullah, "On the Security Issues in Wireless Body Area Networks. | Request PDF," DBLP. Accessed: Sep. 02, 2025. [Online]. Available: https://www.researchgate.net/publication/220670178_On_the_Security_Issues_in_Wireless_Body_Area_Networks

[33] C. C. Y. P. Guang He Zhang, "A Review on Body Area Networks Security for Healthcare," *ISRN Commun. Netw.*, 2011, doi: 10.5402/2011/692592.

[34] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016, doi: 10.1002/SEC.1642;REQUESTEDJOURNAL:JOURNAL:19390122;PAGE:STRING:ARTICLE/CHAPTER.

[35] S. S. Javadi and M. A. Razzaque, "Security and Privacy in Wireless Body Area Networks for Health Care Applications," *Wirel. Networks Secur.* , pp. 165–187, 2013, doi: 10.1007/978-3-642-36169-2_6.

[36] D. D. . Saha, M.S.; Anvekar, "State of the art in WBAN security and open research issues," *Int. J. Recent Innov. Trends Comput. Commun*, vol. 2, pp. 1958–1964, 2014.

[37] B. Chandra and S. Kanaga Suba Raja, "Security In Wireless Body Area Network (WBAN) Using Blockchain," *IETE J. Res.*, vol. 70, no. 1, pp. 487–498, Jan. 2024, doi: 10.1080/03772063.2023.2233472;SUBPAGE:STRING:ACCESS.

[38] P. Naik, M.R.K.; Samundiswary, "Wireless body area network security issues—Survey," *Proc. 2016 Int. Conf. Control. Instrumentation, Commun. Comput. Technol. (ICCICCT), Kumaracoil, India*, pp. 190–194, 2016.

[39] I. A.-S. Samaher Al-Janabi, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egypt. Informatics J.*, vol. 18, no. 2, 2016, doi: 10.1016/j.eij.2016.11.001.

[40] B. H. Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, Shanzhi Chen, "A Survey on Secure Wireless Body Area Networks," *Secur. Commun. Networks*, 2017, doi: https://doi.org/10.1155/2017/3721234.

[41] A. S. S. Jawad Ahmad Aman, "Routing and Security Issues in U-Healthcare Mobile, Ubiquitous and Wireless Body Area Network (WBAN)," *Int. J. Adv. Sci. Technol.*, vol. 109, 2017, doi: 10.14257/ijast.2017.109.03.

[42] B. Narwal and A. K. Mohapatra, "A review on authentication protocols in wireless

body area networks (WBAN)," *Proc. 3rd Int. Conf. Contemp. Comput. Informatics, IC3I 2018*, pp. 227–232, Oct. 2018, doi: 10.1109/IC3I44769.2018.9007303.

[43] M. Usman, Muhammad; Asghar, Muhammad Rizwan; Ansari, Imran Shafique; Qaraqe, "Security in wireless body area networks: from in-body to off-body communications," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2873825.

[44] M. A. Muhammad Sheraz Arshad Malik, "Wireless Body Area Network Security and Privacy Issue in E-Healthcare," *Int. J. Adv. Comput. Sci. Appl.*, 2018, doi: 10.14569/IJACSA.2018.090433.

[45] M. Kompara and M. Hölbl, "Survey on security in intra-body area network communication," *Ad Hoc Networks*, vol. 70, pp. 23–43, 2018, doi: https://doi.org/10.1016/j.adhoc.2017.11.006.

[46] S. . Morales, L.V.; Delgado-Ruiz, D.; Rueda, "Comprehensive Security for Body Area Networks: A Survey," *Int. J. Netw. Secur*, vol. 21, pp. 342–354, 2019.

[47] K. R. S. Bharathi and R. Venkateswari, "Security Challenges and Solutions for Wireless Body Area Networks," *Adv. Intell. Syst. Comput.*, vol. 810, pp. 275–283, 2019, doi: 10.1007/978-981-13-1513-8_29.

[48] R. Nidhya and S. Karthik, "Security and Privacy Issues in Remote Healthcare Systems Using Wireless Body Area Networks," *EAI/Springer Innov. Commun. Comput.*, pp. 37–53, 2019, doi: 10.1007/978-3-030-00865-9_3.

[49] A. Joshi and A. K. Mohapatra, "Authentication protocols for wireless body area network with key management approach," *J. Discret. Math. Sci. Cryptogr.*, vol. 22, no. 2, pp. 219–240, Feb. 2019, doi: 10.1080/09720529.2019.1582869;WGROUP:STRING:PUBLICATION.

[50] K. C. Shubhankar Chaudhary, Ashish Singh, "Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey," *Int. J. Comput. Intell. IoT, Vol. 2, No. 2, 2019*, 2019, doi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355560.

[51] M. Altaf, "A Survey on Authentication Techniques for Wireless Body Area Networks," *J. Syst. Archit.*, vol. 101, no. 2, p. 101655, 2019, doi: 10.1016/j.sysarc.2019.101655.

[52] M. Asam, M.; Ajaz, A.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Gulzar, "Challenges in wireless body area network," *Int. J. Adv. Comput. Sci. Appl*, vol. 10, pp. 336–341, 2019.

[53] M. Sen Sagarika Karchowdhury, "Survey on Attacks on Wireless Body Area Network," *Int. J. Comput. Intell. IoT, Forthcom.*, 2019, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3358378

[54] K. K. Moshaddique Al Ameen, Jingwei Liu, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, p. 2, 2012, doi: 10.1007/s10916-010-9449-4.

[55] S. . Sharma, R.; Kang, "Wban for healthcare applications: A survey of current challenges and research opportunities," *J. Crit. Rev*, vol. 7, pp. 2444–2453, 2020.

[56] M. S. Hajar, M. O. Al-Kadri, and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Comput. Secur.*, vol. 104, p. 102211, 2021, doi: https://doi.org/10.1016/j.cose.2021.102211.

[57] T. C. Samaneh Madanian, "Health IoT Threats: Survey of Risks and Vulnerabilities," *Futur. Internet*, vol. 16, no. 11, p. 389, 2024, doi: https://doi.org/10.3390/fi16110389.

[58] M. A. Naser, A. A. Majeed, M. Alsabah, T. R. Al-Shaikhli, and K. M. Kaky, "A Review of Machine Learning's Role in Cardiovascular Disease Prediction: Recent Advances and Future Challenges," *Algorithms 2024, Vol. 17, Page 78*, vol. 17, no. 2, p. 78, Feb. 2024, doi: 10.3390/A17020078.

[59] C. Li *et al.*, "Efficient Medical Big Data Management With Keyword-Searchable

Encryption in Healthchain," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5521–5532, Dec. 2022, doi: 10.1109/JSYST.2022.3173538.

[60] A. Aldweesh, "Blockchain-Based Secure Firmware Updates for Electric Vehicle Charging Stations in Web of Things Environments," *World Electr. Veh. J.*, vol. 16, no. 4, p. 226, 2025, doi: https://doi.org/10.3390/wevj16040226.

[61] H. Zhu, C. Jin, Y. Xu, G. Chen, and L. Chen, "Efficient and secure heterogeneous online/offline signcryption for wireless body area network," *Pervasive Mob. Comput.*, vol. 99, p. 101893, 2024, doi: https://doi.org/10.1016/j.pmcj.2024.101893.

[62] S. K. Anuj Kumar Singh, "An efficient and secure CLAKA protocol for blockchain-aided wireless body area networks," *Expert Syst. Appl.*, vol. 242, p. 122740, 2024, doi: https://doi.org/10.1016/j.eswa.2023.122740.

[63] S. H. Lisha Zhong, "Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey," *Sensors*, 2022, doi: 10.3390/s22093539.

[64] A. A.-M. Damilola D. Olatinwo, "A Survey on LPWAN Technologies in WBAN for Remote Health-Care Monitoring," *Sensors*, vol. 19, no. 23, p. 5268, 2019, doi: 10.3390/s19235268.

Copyright © by authors and 50Sea. This work is licensed under the Creative Commons Attribution 4.0 International License.