Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Security in Wireless Body Area Networks for Healthcare Applications: Current Trends and Future Directions

Raju Sharma[a,d*], Urvashi Chaudhary[b,e], Samikannu Rajkumar[c].

[a]*Centre of Excellence in Informatics, Electronics and Transmission (CIET), Faculty of Engineering, Sri Lanka*

[b]*Institute of Information Technology, Malabe 10115, Sri Lanka.*

[c]*Chennai Institute of Technology, India*

[d]*Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib 140407, India*

[e]*COPELABS, Lusofona University, Lisbon, Portugal*

[a]*Email: raju.sharma63@gmail.com*

[b]*Email: Urvashi.c@sliit.lk*

[c]*Email: rajkumars.ece@citcehnnai.net*

Abstract

The emergence of wireless body area networks is revolutionizing patient care through non-invasive and unobtrusive monitoring of patients, increasing the efficiency of remote management of patients, assistance in times of crisis, and monitoring chronic conditions of patients. Still, on account of the confidentiality of the health information and the delicate function of WBANs, the need for reasonable security measures is clear. In this survey, the authors assess the security of WBANs with a focus on data confidentiality, integrity, authentication, and availability as well as regulatory requirements. The latest some improvements like use lightweight encryption mechanisms, machine learning-based anomaly detection for attacks, biometric methods for authentication, and using block chains solutions appeared in improving the WBAN systems security are encouraging. Energy constraints, issues of scaling of devices and requirements of standardization, however, remain obstacles. Significant existing solutions and future directions including the use of quantum cryptography, AI-based protection and privacy sensitive data technology are discussed. The survey is expected to provide the WBAN security context while addressing its several challenges and offer a roadmap for future research and development for better and safe WBAN use in the medical field

Keywords: Security, privacy, Wireless Body Network, Healthcare, Attacks, Threats

Citation: R. Sharma, U. Chaudhary, and S. Rajkumar, "Security in Wireless Body Area Networks for Healthcare Applications: Current Trends and Future Directions", ARIS2-Journal, vol. 4, no. 2, pp. 57–74, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.51

---

* Corresponding author. Email address: raju.sharma63@gmail.com

1. Introduction

Wireless body area networks or WBANs have been a game-changer for healthcare systems allowing for round-the-clock patient monitoring without any invasion using voice and vision-based wearable and implantable wireless sensor node networks. They are powerful tools for improving the quality and accessibility of health care by allowing remote patient control, an early diagnosis, and appropriate treatment in a timely manner since WBANs collect data in passive obtaining heart rate, blood pressure, glucose, and a number of other important statistics in real-time [1]. These systems are indispensable for clinical situations requiring constant surveillance, such as management of chronic disease patients, post-surgical monitoring, and emergency situations.

At first glance, though there's no simple justification for the implementation of preventive measures and strictly regulated protocols, however it is the inherent feature of the collected data especially the depth of surveillance and critical operating functions that leaves no room for doubt. Health data succinctness is crucial so that any individual cannot gain unwarranted access to unauthorized personnel, data inconsistency, and unavailability are essential for the purpose of risk-free monitoring [2]. Security transgressions of such systems, compromise patient safety, data integrity and violate the governing laws. Therefore, in order for WBAN technology to deliver its intended benefits, it is necessary to implement a secure and fault-tolerant WBAN system.

The scope of this paper is to assess the current security realm of WBANs in healthcare by evaluating modern practices, methods and technologies. This paper attempts as well to investigate the main difficulties in securing WBANs, especially in resource-constrained environments and to suggest future lines of research aimed to improve security, efficiency and scalability of these systems in healthcare context. Structure of the paper shown in Figure 1.

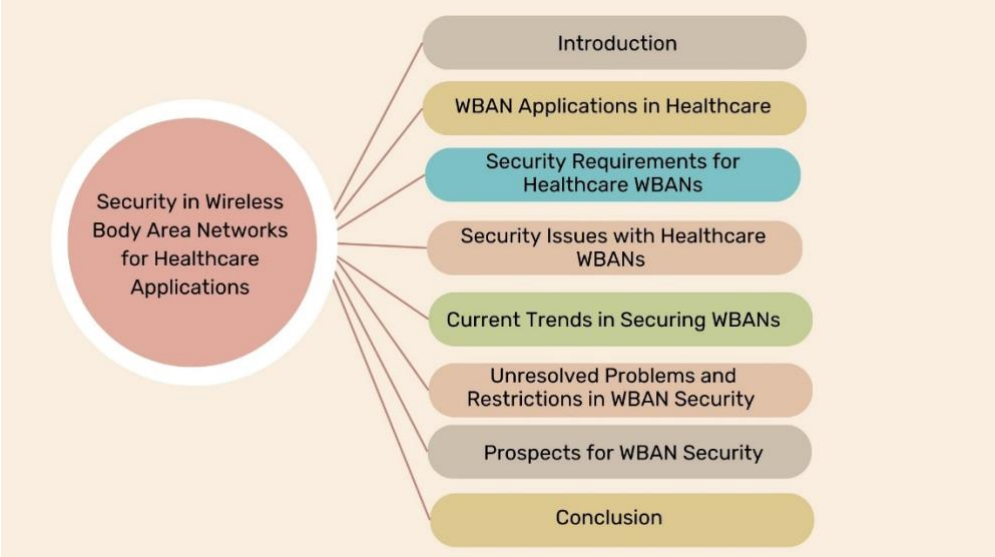

Figure 1: Structure of the paper

2. Literature Review

The literature review is Given in following Table 1.

Table 1: Literature Review

Authors	Year	Parameters/Technique Used	Key Findings	Gap
Moses Blessing [3]	2024	Encryption, Secure Routing	Highlighted encryption and secure routing as key solutions for WBAN communication challenges.	Limited focus on specific encryption algorithms or energy efficiency.
Alte, Bhavana, and Amarsinh V. Vidhate. [4]	2024	Hybrid cryptographic model (AES and ECC)	Optimized energy efficiency in WBANs.	No discussion of scalability or specific attack resilience.
Singla, Ripty, et al [5].	2022	AES-based encryption with adaptive security	Proposed encryption with variable security levels based on data sensitivity.	Energy consumption and real-time performance were not analyzed.
Hajar, Muhammad Shadi [6]	2022	High entropy EKG signals	Mitigated DoS, replay, and MITM attacks in WBANs.	Limited validation in diverse WBAN environments and with multiple data types.
Zhang, Jianhong, and Chenghe Dong [7]	2022	Low computational cost cryptographic solution	Enhanced data protection with minimal	Did not address adaptive security levels

			computational overhead.	for varied data sensitivity.
Izza, Sarah, Mustapha Benssalah, and Karim Drouiche [8]	2021	Fast cryptographic operation	Achieved shorter encryption times to meet real-time requirements in WBANs.	Lack of integration with existing WBAN frameworks for testing scalability and security.
Taleb, Houssein, et al. [9]	2021	Survey of WBAN security challenges	Reviewed security and privacy issues in healthcare applications of WBANs.	Lacked practical implementation or suggested solutions.
Newaz et al. [10]	2020	HEKA (Intrusion Detection System)	High accuracy in detecting attacks on personal medical devices.	Did not address scalability and energy constraints for continuous monitoring.
Hussain, Munir, et al. [11]	2019	Hybrid cryptography	Suggested benefits of combining symmetric and asymmetric methods for WBANs.	No practical implementation or performance evaluation for the proposed approach.
Basnet, A., et al.	2019	HMAC, RSA, AES	Developed a secure health telemonitoring system with high data security.	Did not optimize energy consumption for continuous monitoring.
Chatterjee, K.[13]	2019	Improved authentication protocol	Enhanced security for WBANs in healthcare applications.	Lacked performance metrics for computational efficiency and energy usage.
Alaparthy and Morgera [14]	2018	Multi-level intrusion detection based on immune theory	Proposed an immune-based intrusion detection for WBANs.	Limited focus on real-time implementation in constrained environments.
Odesile and Thamilarasu [15]	2017	Distributed IDS using mobile agents and ML algorithms	Used machine learning for intrusion detection in WBANs.	Computational overhead of ML algorithms in resource-constrained WBANs.
Thamilarasu [16]	2016	iDetect (Intelligent IDS using genetic algorithms)	Improved detection accuracy for WBANs.	Did not address deployment challenges in dynamic WBAN environments.
Tewari and Verma [17]	2016	Critical review	Identified gaps in security and privacy in WBAN-based e-healthcare.	Lack of new methods or tools proposed to fill identified gaps.
Kargar et al. [18]	2013	Security analysis from e-health perspective	Identified key vulnerabilities in WBANs.	Did not propose specific countermeasures or solutions.

Ullah et al. [19]	2012	Survey on WBAN characteristics and challenges	Provided a comprehensive overview of WBAN vulnerabilities.	Lack of targeted solutions to address identified security gaps.
Huang and Lee [20]	2003	Cooperative IDS using mobile agents	Applied mobile agent technology for intrusion detection in ad hoc networks.	Did not specifically address WBAN constraints or healthcare applications.

3. WBAN Applications in Healthcare

In the Healthcare sector, the role of the WBAN is becoming very important. Additionally, the Wireless Body Area Network supports various types of applications that can provide patient welfare and real-time insights on health status. There are some applications such as remote patient monitoring. fitness tracking, emergency response, and chronic disease management that can be treated without any physical contact with the help of a WBAN [21].

With the help of WBANs practitioners monitor the patient's vital signs from a distance and it makes it possible for the practitioners to follow up the cardiac patients, diabetes patients, and also the post-surgical patient to check their recovery [22]. For cardiac patients, wearable sensors constantly monitor the patient's heart rate or blood pressure and update the doctors if an arrhythmia occurs in cardiac patients. Continuous Glucose Monitors enabled by WBAN for Diabetes Management, deliver data based on glucose levels in real-time and help healthcare providers to decide whether insulin injections of carbohydrates are required or not. Real-Time Monitoring with the help of WBAN enables the patients to record and monitor the important data from a distance without any touch. This provides tailored and active medical care to patients. Figure 2. Shows the WBAN applications in healthcare.

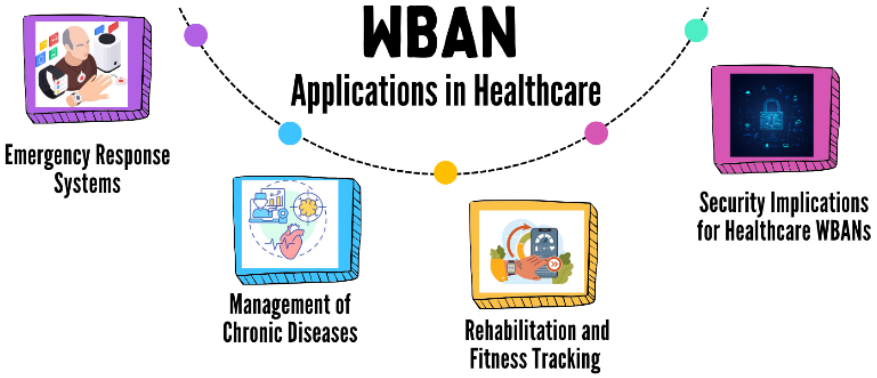

Figure 2: WBAN Applications in Healthcare

3.1. Emergency Response Systems

Emergency Response Systems are also called Real-Time Systems which makes possible for the doctors or emergency room teams to receive real-time information regarding patients [23]. This can be done by using wearables WBAN devices that sense the data such as oxygen saturation, ECE readings or respiration rate and send this information to the doctors that take decisions according to the information. In Heart Attacks or in several allergic reactions, real-time data transmission is very important to affect he patients' life and recovery [24].

3.2. Management of Chronic Diseases

For treating chronic illness including Parkinson's disease, asthma and hypertension, WBANs are very helpful when timely information and ongoing monitoring is required. In asthma, sensors deployed on patients track the breathing pattern of patient and alert them and their relatives to early signs of an attack. From Customized therapy modifications, Patients with Parkinson's disease takes benefit to improve their quality of life by using wearable devices to detect and monitor tremor balance, intensity and movement alterations [25].

3.3. Rehabilitation and Fitness Tracking

In addition to acute and chronic illness applications, WBANs are used in preventive healthcare and rehabilitation. In physical therapy and rehabilitation, WBANs are used to give information regarding posture, joint movements and muscle activity. This information helps the doctors to access the patient's progress remotely and adjust treatment as required. In preventative healthcare, WBAN enabled fitness trackers are used to monitor the parameters like heart rate variability and step count. These fitness trackers are helped to monitor the warning signs and motivates the users to maintain the healthy life activity [26]

3.4. Security Implications for Healthcare WBANs

Security in WBAMs' applications are very important. Security flaws in WBAN systems may lead to major consequences like inaccurate diagnosis, delayed treatment or illegal access to private patient data. Change in health data may lead to inaccurate dosage recommendations for diabetic patients and violations of data privacy may expose the medical history of the patient that result to stigmatizations and prejudice. Therefore, to ensure the effective and safe integration of WBAN technology in healthcare sector, strong security measure is required to maintain the confidentiality, integrity and availability of WBAN data [26].

4. Security Requirements for Healthcare Wireless Body Area Networks (WBANs)

WBANs are essential for patient health monitoring systems to collect and transmit real-time health data to doctors. The protection of privacy and security of the patient's health data is also very important. The Security Requirement for Healthcare Wireless Body Area Networks (WBANs) shown in Figure 3. To deploy the WBANs effectively and securely, the following standards must be met:

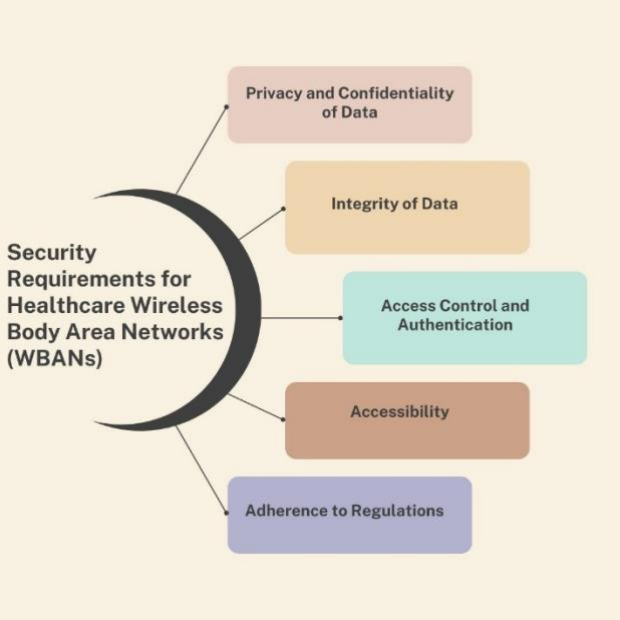

Figure 3: Security Requirements for Healthcare Wireless Body Area Networks (WBANs)

4.1. Privacy and Confidentiality of Data

To avoid any unauthorized access, the privacy of personal health information (PHI) must be protected. Privacy of personal health information (PHI) must be protected to avoid any unauthorized access. Sensitive information like glucose levels, heart rate, and blood pressure should be encrypted during transmission and storage. AES (Advanced Encryption Standard) is an improved encryption that should be developed to ensure that the data is only accessible by authorized persons or systems. Furthermore, methods for anonymization and deidentifying data might help to safeguard the patient's privacy, especially when sharing the data with other members for research analysis [27].

4.2. Integrity of Data

To provide the reliability of the health data it should be guaranteed that the data accumulated by the WBAN is correct, dependable, and unaltered during transmission. Digital signatures and cryptographic hash function procedures are used to identify unauthorized data change. Keeping data integrity is very significant for real-time monitoring because any change to the data could lead to incorrect diagnoses or treatment decisions [28].

4.3. Access Control and Authentication

Use of medical data and equipment, effective access control and authentication protocols are essential to prohibit unauthorized access. To verify the individuality of patients, medical personnel and other users interacting with system, Robust multi-factor authentication (MFA) methods should be used. To ensure that only permitted persons

have access to specific types of data or equipment. Role-based access control of RRAC can be used. By preventing the unauthorized access to the vital monitoring of patients' health records, reduces the likelihood of breaches [29]

4.4. Accessibility

In critical situations where patient safety needs real-time monitoring, used in healthcare sector must ensure the uninterrupted access to health data. It is important to implement fault-tolerant systems, redundancy and fail over strategies to provide continuous data accessibility for authorized users despite network issues, hardware failure or cyberattacks. Healthcare professionals and patients must trust that the monitoring system will operate continuously, to provide continuous health monitoring and timely interventions [30].

4.5. Adherence to Regulations

When managing health data, WBAN must adhere to the General Data Protection Regulation (GDPR), the Health Insurance Probability and Accountability Act (HIPAA) in the United States, and other regional or national standards that are very few laws and regulations. To safeguard patient health data, uphold the rights of data subjects, and offer audit trails for data access and change, healthcare institutes must put in place particular security measures by these guidelines. To guarantee the authenticity of healthcare WBAN deployment and build confidence among patients, medical professionals, and IT developers, these rules must be followed. By attending to these security needs, guaranteeing patient safety and fulfilling legal obligations, Healthcare WBANs can offer a safe, dependable and privacy-respecting option for ongoing health monitoring [31]

5. Security Issues with Healthcare WBANs

Implementing robust security measures for WBAN in the healthcare sector is very difficult because of intrinsic difficulties. In the specific environment in which WBAN operates and with the nature of medical records, these challenges arise. The following are the primary concerns associated with healthcare WBANs.

5.1. Limitations on Resources

Sensors and Wearable monitors used in WBAN are designed compact, lightweight, and energy-efficient due to processing power, battery life, and storage capacity limitations. Conventional security mechanisms used in WBAN's can rapidly decrease the battery life and affect the performance of the Device; they use most of the power and frequent transmission of data. In resource-constrained environments, lightweight encryption methods and improved security protocols are designed to handle these issues [32].

5.2. Scalability and Mobility

Patients move within and outside of the healthcare facilities, to handle this mobility. WBANs use a network of mobile sensors that continuously collect and transmit data. Since sensors may switch between networks or briefly lose access to a network. This is very difficult to ensure the connectivity of these mobile and scattered devices. When installations are expanded to cover more patients or handle more devices, it can be difficult to provide

secure communication. To maintain confidentiality, data availability, and integrity while adjusting to the dynamic topologies, the security measures must be flexible enough to cope with the frequent changes in the network configurations [33]

5.3. Real-Time Requirement

To provide treatment on time or alerts, many WBAN-based applications like heart monitoring and glucose monitoring require real-time data processing and analysis. Security solutions that are used to protect data without increasing latency are implemented because any delay could affect patient care. The need of real-time response conflicts with the computational needs of data validation, encryption, and authentication. Creative Security mechanisms that minimize the processing overhead and preserve WBAN responsiveness are required to handle this challenge [34].

5.4. Interoperability

WBAN healthcare system mostly uses devices from different manufacturers with different security standards, measures, and communication protocols. It is a challenging task to present secure interoperability among these devices due to diverse security levels and inappropriate protocols that cause network vulnerabilities. It requires close cooperation between healthcare providers, regulatory bodies, and manufacturers. These problems can be solved by establishing industry-wide compatibility for WBAN via the development of protocols and common security standards.

5.5. Privacy Issue

Privacy is a primary concern in WBAN applications due to the sensitivity of the healthcare data. If the patient's health information is available to unauthorized people or organizations that is collected by WBAN devices, can be misused. To safeguard patient privacy, strict access control encryption and compliance with laws like GDPR and HIPPA are all required. Since WBAN devices are portable and mobile, there are additional privacy issues, and they are more susceptible to illegal data leaks and interception [35].

6. Current Trends in WBAN Security

WBANs are designed for healthcare systems that need to implement advanced security techniques so that it can work perfectly within the limitations of these system resources. Nowadays most of the research is focused on

developing lightweight, scalable, and privacy-preserving security solutions so that the demand of the healthcare sector can be achieved. Current trends in WBAN security are shown in Figure 4.

Figure 4: Current Trends in WBAN Security

6.1 Protocols for Lightweight Encryption

Due to the very limited processing power of WBAN devices, lightweight encryption methods are an effective and rational alternative to protect confidential health information with little computational overhead. Protocols in wide use include elliptic curve cryptography (ECC) based protocols, generalized to work within the Advanced Encryption Standard (AES). Although ECC assures a high level of security with much smaller key size than classical cryptographic techniques, lightweight AES-based encryption ensures a high degree of data confidentiality while requiring comparatively lower power and computational requirements. Which make sure to store and transfer data without letting it affect the battery or real-time performance severely [36].

6.2 Techniques for Key Management

To provide secure communication, efficient key management is crucial where numerous devices must connect dynamically and safely. Modern key management techniques include pre-distributed keys, pairwise keys, and dynamic key management. Pre-distributed keys are an efficient way to allocate keys in advance. It saves energy, removing the need for real-time key creation. Pairwise key configuration ensures that keys are unique to each device pair, enhancing security and reducing the possibility of key compromise. Dynamic key management allows

keys to be updated often to maintain security over time. These methods increase the integrity and confidentiality of WBAN interactions by ensuring secure key exchange and storage [37].

6.3 Authentication Through Biometrics

A WBAN is a biometric authentication, which uses unique physiological characteristics to access. ECG-based authentication, for instance, verifies a user's identity by unique biometric signals produced by the heart. Since such physiological data, including ECG patterns, is extremely unique and hard to replicate, authentication based on biometrics provides a secure and convenient approach compared to the traditional password-based methods. This would restrict the access of authorized users to WBAN devices and information thereby enhancing patient privacy and preventing unauthorized access to critical health information [37].

6.4 Integration of Blockchain

A blockchain is a decentralized, secure data management system for WBAN information. Such a system would support the audibility and tamper-proof storage of data due to its decentralized structure, thereby maintaining the accuracy and traceability of medical records in WBANs. In addition, it can permit several healthcare providers to exchange data securely while preserving access control and data provenance. Through smart contracts, it can automate access rights and ensure that only authorized parties can view or modify health information. This could dramatically enhance both the security and integrity of WBAN data while providing a clear framework for patient consent along with the management of that data.[38]

6.5 Integration of Blockchain

Privacy-preserving data aggregation techniques can collect and analyze health data without revealing sensitive personal information [39]. By employing strategies like homomorphic encryption, differential privacy, and secure multi-party computation (SMPC), healthcare practitioners can safely aggregate data from many WBANs, reducing privacy risks. For example, because homomorphic encryption allows computations on encrypted data, sensitive health information is never revealed during analysis. These techniques allow for extracting significant health insights from aggregated data while protecting patient privacy.

In addition to addressing the particular security and privacy issues raised by these systems, these trends mark important developments in the security of WBANs for the healthcare industry and allow for the safe and effective use of WBANs in clinical and remote health monitoring applications.

7. Current Unresolved Problems and Restrictions in WBAN Security

Security of WBANs in the healthcare sector has advanced significantly. However, there are still several limitations and issues that impact the effectiveness and deployment of these system. Significant difficulties are shown in Figure 5.

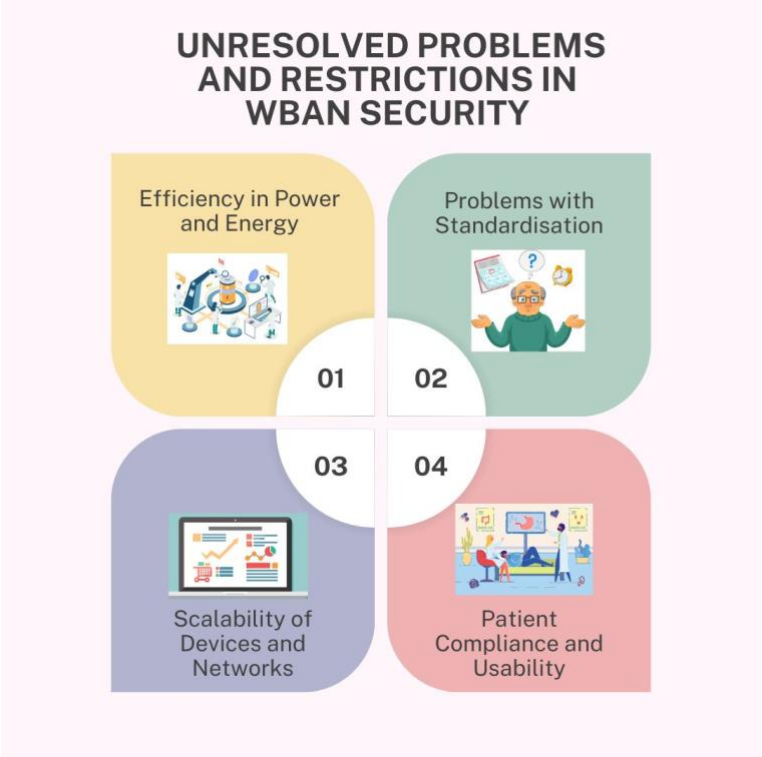

Figure 5: Unresolved Problems and Restrictions in WBAN Security

7.1 Efficiency in Power and Energy

Strong security measures result, in higher energy usage, and lower lifespans, because WBAN devices are usually battery-operated. Reasons of the quick drain of power of these limited power devices are regular authentication processes, continuous data monitoring, and intricate encryption techniques. There is a trade-off between battery life and security level because high energy requirements, need charging of devices more frequently or replacement, which is not suitable for continuous health monitoring. To increase the battery life without compromising security, energy-efficient security features are required [40].

7.2 Problems with Standardization

One major limitation of WBAN security is the lack of unified standards for healthcare applications. The absence of standards hinders interoperability and standardized security practices especially in multi-vendor environments when devices are from multiple manufacturers. If clear standards are not implemented, healthcare providers can find it difficult to enforce security norms and methods that could make security vulnerable. Standardization efforts are required to establish consistent security mechanisms across WBANs to support regulatory compliance, integration with existing healthcare information systems, and interoperability [41].

7.3 Scalability of Devices and Networks

Adding more devices and connecting with other networks, WBAN becomes more complex. Each additional device increases the possibility of unauthorized access or data breaches. Since it needs to ensure that the data is secure while it is going across different devices and infrastructures, communication between the bigger networks

and WBANs becomes difficult to manage. The implementation of scalability solutions that can handle a large number of devices and enable secure connections with larger healthcare networks is required to provide suitable support for the deployment of WBAN at scale [42]

7.4 Patient Compliance and Usability

A balance of robust security features and usability is required to ensure patient compliance, particularly for those using WBANs for long-term monitoring. As WBANs use difficult authentication techniques or frequent security disruptions occur, patients may feel annoyed and less likely to adhere to device protocols. Security techniques must be simple to use and invasive to encourage regular use while preserving security.

There is a necessity for the advancement of WBAN security to address the practical constraints and changing needs of healthcare applications, the reason for this is the existing unresolved problems. To optimize WBAN in healthcare it is essential to build a system that prioritizes standardization, scalability, usability, and energy efficiency [43].

8. Current Unresolved Problems and Restrictions in WBAN Security

Innovative approaches to resolving security concerns and enhancing data protection are being researched and the usage of WBANs in the healthcare sector grows. Here are some potential paths for WBAN security.

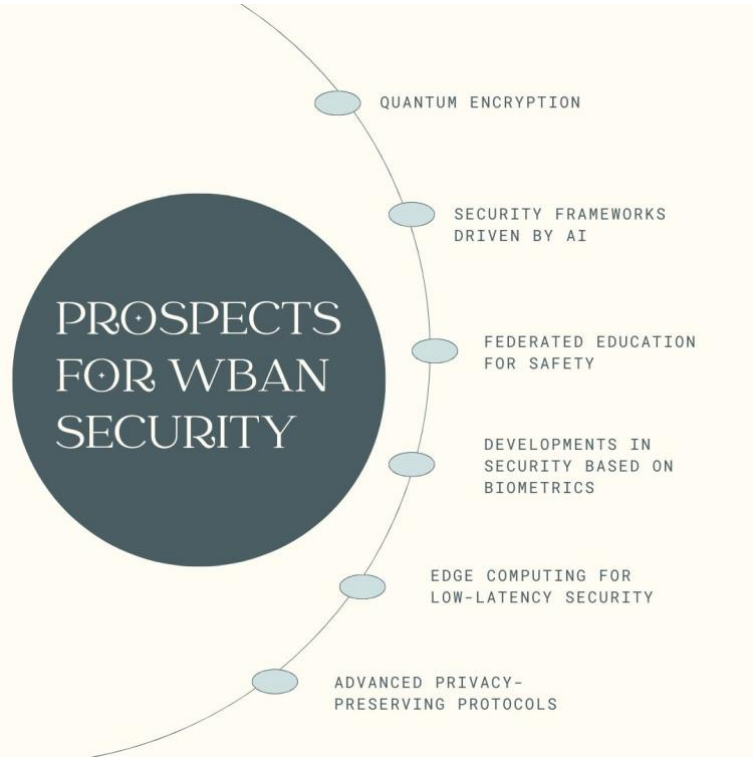

Figure 6: Prospects For WBAN Security

8.1 Patient Compliance and Usability

Quantum key distribution utilizes the ideas of quantum mechanics to offer the potential for almost unbreakable encryption, and cryptographic keying material using special-purpose technology. In Quantum key distribution, two devices can share encryption keys and make any attempt at eavesdropping instantly detectable, which is not possible with conventional encryption methods. The use of QKD plays an important role in protecting sensitive health data in WBAN even in the situation of advanced cyberthreats. Even while practical applications of quantum cryptography are still in their infancy, they have the potential to completely revolutionize WBAN security [44].

8.2 Patient Compliance and Usability

WBAN security can be improved with the use of real-time threat identification and mitigation, AI has a great potential to provide this. AI-driven frameworks continuously keep track on the device behaviors and network patterns to point out the irregularities that indicate security breaches. AI can provide context-aware and tailored protection. it can also lower the security risks without requiring persistent annual improvement by just changing the security rules. This is a promising approach because cyber threats point to healthcare data in WBAN and are dynamic [45]

8.3 Federated Education for Safety

The federated learning process preserves privacy and improves security by enabling the WBAN devices to learn collectively from the aggregated data without integrating sensitive patient data. With the help of federated learning methods, WBAN devices can improve their threat detection capability and response abilities to learn from regionalized data patterns across several devices. This technique ensures data privacy and increases device-level security due to raw data does not leave individual devices. For deploying regionalized, privacy-preserving security solutions in WBAN, Federated Learning can be a powerful tool [46].

8.4 Developments in Security Based on Biometrics

To enhance the accuracy and security of biometric authentication procedures, multimodal biometrics are used. Physiological information consisting of movement patterns, body temperature and electrocardiograms are combined by using these biometrics. By integrating these unique characteristics WBAN can reduce unauthorized access while simultaneously providing more access control. Two outcomes that can be achieved are improved authentication and user convenience. By gathering real-time data from a wide variety of sensors. Secure and hassle-free WBA authentication can be achieved with this approach [47].

8.5 Edge Computing for Low-Latency Security

Now researchers of large amounts are interested in computing to process data close to WBANs. This technique helps WBANs gain the ability to quickly detect and respond to threats while reducing reliance

on central servers. WBANs can decrease the probability of security breaches by carrying out security activities close to the network edge, where they can counter more quickly to threats and send less data to remote servers. Edge computing allows for immediate threat detection and data analysis at the souse in healthcare applications where latency is important and requires that security techniques remain effective [47].

8.6 Advanced Privacy-Preserving Protocols

While retaining raw health information, enhanced privacy-preserving techniques contain homomorphic encryption and differential privacy support to enable safe data handling. Without compromising patient privacy, Homomorphic encryption allows computations to be conducted on encrypted data. And enabling analysis and information aggregation. Differential privacy techniques, however, include noise in datasets such that individual data points cannot be found back to individual individuals and yet allow for large analytical results. These techniques allow healthcare professionals to safeguard patient privacy and extract valuable information from WBAN data, thus confirming safe and privacy-respecting data management in WBAN applications [47].

By applying a forward-looking approach to expand the security of WBANs addresses current issues, thus addressing existing vulnerabilities and adjusting to the evolving threat environment. These technologies have great potential to transform WBAN security as they grow, thus creating a more secure and effective framework for use in the healthcare industry.

9. Conclusion

WBANs offer a substantial opportunity for healthcare advancement by enabling real-time and continuous monitoring of patient health information. In this paper, several factors related to WBAN security have been discussed like a need for data confidentiality, integrity of data, and compliance with legal requirements. The factors like mobility, resource restrictions, and privacy issues are still to be overcome. These factors make difficult to implement standard security measures to meet the requirements of WBAN security.

To protect the WBAN from unauthorized access, prompt advancements in the field like biometric authentication, lightweight encryption and AI-enhanced security methods are going to support recent research. For the development of scalable and energy-efficient security solutions, future reach should be the top priority that can be adapted to the particular needs of healthcare applications. Edge computing, federated learning and quantum cryptography are the methods that can be used to reduce the power usage and increasing the security of WBNs.

This paper concludes that the realization of the full capabilities of the WBAN healthcare system requires robust security techniques. There is need that the healthcare providers, technology developers and regulatory bodies works together to improve the security protocols to protect the patient healthcare data along with this also preserve the usability in order to meet the WBAN security criteria.

References

1. Sharma, S., Tripathi, M. M., & Mishra, V. M. (2022, February). Comparative analysis of routing protocols in wireless body area network (wban). In *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)* (Vol. 2, pp. 703-706). IEEE.
2. Saxena, D., & Patel, P. (2023). Energy-efficient clustering and cooperative routing protocol for wireless body area networks (WBAN). *Sādhanā*, *48*(2), 71.
3. Blessing, M. (2024). Challenges and Solutions in Implementing Secure Communication in WBANs.
4. Alte, B., & Vidhate, A. V. (2024, June). A Hybrid Cryptographic Protocol for Secure and Efficient Data Transmission for Wireless Body Area Network. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
5. Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Personal Communications, 1-40.
6. Hajar, M. S. (2022). A reliable trust-aware reinforcement learning based routing protocol for wireless medical sensor networks (Doctoral dissertation).
7. Zhang, J., & Dong, C. (2022). Secure and lightweight data aggregation scheme for anonymous multi-receivers in WBAN. *IEEE Transactions on Network Science and Engineering*, *10*(1), 81-91.
8. Izza, S., Benssalah, M., & Drouiche, K. (2021). An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *Journal of Information Security and Applications*, *58*, 102705.
9. Taleb, H., Nasser, A., Andrieux, G., Charara, N., & Motta Cruz, E. (2021). Wireless technologies, medical applications and future challenges in WBAN: A survey. *Wireless Networks*, *27*(8), 5271-5295.
10. Newaz, A. I., Sikder, A. K., Babun, L., & Uluagac, A. S. (2020, June). Heka: A novel intrusion detection system for attacks to personal medical devices. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.
11. Hussain, M., Mehmood, A., Khan, S., Khan, M. A., & Iqbal, Z. (2019). Authentication techniques and methodologies used in wireless body area networks. *Journal of Systems Architecture*, *101*, 101655.
12. Basnet, A., Alsadoon, A., Prasad, P. W. C., Alsadoon, O. H., Pham, L., & Elchouemi, A. (2019). A novel secure patient data transmission through wireless body area network: Health tele-monitoring. *International Journal of Communication Networks and Information Security*, *11*(1), 93-104.
13. Alte, B., & Vidhate, A. V. (2024, June). A Hybrid Cryptographic Protocol for Secure and Efficient Data Transmission for Wireless Body Area Network. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
14. Alaparthy, V. T., & Morgera, S. D. (2018). A multi-level intrusion detection system for wireless sensor networks based on immune theory. *IEEE Access*, *6*, 47364-47373.
15. Odesile, A., & Thamilarasu, G. (2017, September). Distributed intrusion detection using mobile agents in wireless body area networks. In *2017 Seventh International Conference on Emerging Security Technologies (EST)* (pp. 144-149). IEEE.
16. Thamilarasu, G. (2016). iDetect: an intelligent intrusion detection system for wireless body area networks. *International Journal of Security and Networks*, *11*(1-2), 82-93.
17. Tewari, A., & Verma, P. (2016). Security and privacy in e-healthcare monitoring with WBAN: a critical review. *International Journal of Computer Applications*, *136*(11).
18. Kargar, M. J., Ghasemi, S., & Rahimi, O. (2013). Wireless body area network: from electronic health security perspective. *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, *2*(4), 38-47.
19. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., ... & Kwak, K. S. (2012). A comprehensive survey of wireless body area networks: On PHY, MAC, and network layers solutions. *Journal of medical systems*, *36*, 1065-1094.
20. Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (pp. 135-147).
21. Blessing, M. (2024). Challenges and Solutions in Implementing Secure Communication in WBANs.

22. Sharma, R., Ryait, H. S., & Gupta, A. K. (2015). Performance analysis of ATTEMPT, SIMPLE and DEEC routing protocols in WBAN. *Int J Latest Trends Eng Tech*, *6*(2), 133-39.
23. Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. *Wireless Personal Communications*, 1-40.
24. Sharma, R., Ryait, H. S., & Gupta, A. K. (2016). Analysing the effect of posture mobility and sink node placement on the performance of routing protocols in WBAN. *Indian Journal of Science and Technology*, *9*(40), 1-11.
25. Tan, H., & Chung, I. (2019). Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. *IEEE Access*, *7*, 151459-151474.
26. Tan, H., & Chung, I. (2019). Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. *IEEE Access*, *7*, 151459-151474.
27. Olatinwo, D. D., Abu-Mahfouz, A., & Hancke, G. (2019). A survey on LPWAN technologies in WBAN for remote health-care monitoring. *Sensors*, *19*(23), 5268.
28. Malik, M. S. A., Ahmed, M., Abdullah, T., Kousar, N., Shumaila, M. N., & Awais, M. (2018). Wireless body area network security and privacy issue in e-healthcare. *International Journal of Advanced Computer Science and Applications*, *9*(4).
29. Javadi, S. S., & Razzaque, M. A. (2013). Security and privacy in wireless body area networks for health care applications. *Wireless Networks and Security: Issues, Challenges and Research Trends*, 165-187.
30. Karmakar, K., Saif, S., Biswas, S., & Neogy, S. (2018, January). WBAN Security: study and implementation of a biological key based framework. In *2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT)* (pp. 1-6). IEEE.
31. Asam, M., Jamal, T., Ajaz, A., Haider, Z., & Butt, S. A. (2019). Security Issues in WBANs. *arXiv preprint arXiv:1911.04330*.
32. Tewari, A., & Verma, P. (2016). Security and privacy in e-healthcare monitoring with WBAN: a critical review. *International Journal of Computer Applications*, *136*(11).
33. Taleb, H., Nasser, A., Andrieux, G., Charara, N., & Motta Cruz, E. (2021). Wireless technologies, medical applications and future challenges in WBAN: A survey. *Wireless Networks*, *27*(8), 5271-5295.
34. Paul, P. C., Loane, J., McCaffery, F., & Regan, G. (2021). Towards design and development of a data security and privacy risk management framework for WBAN based healthcare applications. *Applied System Innovation*, *4*(4), 76.
35. Soni, M., & Singh, D. K. (2023). New directions for security attacks, privacy, and malware detection in WBAN. *Evolutionary Intelligence*, *16*(6), 1917-1934.
36. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727-1765.
37. Narwal, B., & Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. *Journal of Systems Architecture*, *113*, 101883.
38. Bouazzi, I., Zaidi, M., Usman, M., Shamim, M. Z. M., Gunjan, V. K., & Singh, N. (2022). Future Trends for Healthcare Monitoring System in Smart Cities Using LoRaWAN-Based WBAN. *Mobile Information Systems*, *2022*(1), 1526021.
39. Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless communications*, *17*(1), 51-58.
40. Javadi, S. S., & Razzaque, M. A. (2013). Security and privacy in wireless body area networks for health care applications. *Wireless Networks and Security: Issues, Challenges and Research Trends*, 165-187.
41. Kaur, R., Shahrestani, S., & Ruan, C. (2024). Security and Privacy of Wearable Wireless Sensors in Healthcare: A Systematic Review. *Computer Networks and Communications*, 24-48.
42. Kumaran, S., Samyuktha, P. M., & Bhavyashree, M. R. (2024, July). Deep Learning Enhanced Signal Processing Techniques for WBAN-Enabled Telemedicine Applications. In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)* (pp. 1010-1015). IEEE.
43. Ullah, S., Li, J., Chen, J., ALI, I., Khan, S., Ahad, A., ... & Leung, V. (2024). A Survey on Emerging Trends and Applications of 5G and 6G to Healthcare Environments. *ACM Computing Surveys*.

44. Alawadhi, A., Almogahed, A., Mohammed, F., Ba-Quttayyan, B., & Hussein, A. (2024). Improving performance metrics in WBANs with a dynamic next beacon interval and superframe duration scheme. *Heliyon*, *10*(5).
45. Nissar, G., Khan, R. A., Mushtaq, S., Lone, S. A., & Moon, A. H. (2024). IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends. *Multimedia Tools and Applications*, 1-62.
46. Radha, M., & Murugan, K. (2024, February). Monitoring and Storage of Health Data in Secured Cloud Environment: A Detailed Survey. In *2024 2nd International Conference on Computer, Communication and Control (IC4)* (pp. 1-6). IEEE.
47. Chen, Y. (2024). Adversarial Models and Game Theoretic Logic Related to Online Security. *Arts, Culture and Language*, *1*(7).