ISSN: 2831-6789

Research Article

Journal of Robotics and Automation Research

Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare

Kamran Ayub[1*] and Roushdy Alshawa[2]

[1]*Service Mgmt. Office TELUS, Canada*

[2]*Head of Global Service Management New York University - Shanghai, PRC*

[*]Corresponding Author
Kamran Ayub, Service Mgmt. Office TELUS, Canada.

Submitted: 2024, Nov 28; **Accepted:** 2024, Dec 23; **Published:** 2024, Dec 31

Citation: Ayub, K., Alshawa, R. (2024). Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare. *J Robot Auto Res, 5*(3), 01-08.

Abstract

Wireless Body Area Networks (WBANs) are critical components of emerging smart healthcare solutions. Due to the intrinsic nature of wireless communication and the potentially sensitive medical data they carry, such networks are often very vulnerable to many types of security threats. As a result, the security of WBANs becomes a prime concern when they are considered for use in healthcare or medical applications. This text enumerates common security threats that a typical WBAN should prepare for. It also provides a set of enhancement mechanisms and techniques that could be implemented to augment the security of WBANs.

Furthermore, a vital precautionary activity that should be taken in the initial steps towards developing a secure WBAN system—threat modeling—is also described. This text presents two elaborated example cases for the threat modeling technique for WBANs: patrolling and insulin injection WBANs. The cases demonstrate that threats in WBANs are further sources of vulnerabilities, beyond the definition of threats from common knowledge, that should be evaluated and addressed before deployment. Results show that there are plenty of possible problems that threaten the security and privacy of WBAN systems, which should be taken into strong consideration. It is believed that the proposed threat modeling methodology here will significantly contribute to secure designs of WBANs and can also potentially be generalized to other embedded systems as well.

Keywords: Wireless Communication, Correlation, Accuracy, Event Detection, Medical Services, Body Area Networks, Real-Time Systems, Time Factors, Monitoring, Streams, Threat Modelling, Smart Healthcare

The Problem Statement

The integration of ICT in healthcare improves the quality and efficiency of medical treatment while reducing costs. Wireless body area networks (WBANs) offer continuous healthcare and real-time monitoring, potentially saving lives. However, extensive security measures are necessary to protect sensitive medical data. WBAN security can be approached from three angles: communication, application, and network security. Threats can arise from within the network, particularly from the sensor or WBAN node. Implementing security measures within the node-centric approach is challenging due to constraints in system resources. However, this approach is best suited for WBANs as energy-constrained devices. Despite these concerns, there is potential to provide comprehensive security in various applications while safeguarding public information.

1. Introduction

Recently, Wireless Body Area Networks (WBANs) have witnessed a spurt of development, both in terms of research and investment. Wearable WBAN devices communicate with each other through wireless technologies to provide remote monitoring and healthcare services, which is called a smart healthcare system. Such a healthcare system has the potential to improve the effectiveness and efficiency of current medical strategies by providing healthcare services without time and place constraints [1]. However, the possibility of eavesdropping, tampering, and message forgery makes WBANs an easy target for a wide range of security attacks.

To explore the new security challenges presented by WBANs and mitigate their potential risk, we investigate WBANs against a number of well-known security threat modeling techniques from the security engineering domain, discuss several related privacy and security requirements, and present a variety of security enhancements. In this survey, we first briefly introduce smart healthcare and the WBAN technology, then we analyze the security modeling before we identify security enhancements attacking from different networks. In particular, our survey makes the following contributions: 1. Realizing that WBANs have general security requirements, such as confidentiality, integrity, and availability, from a WBAN's intrinsic nature [2]. 2. Revealing

that different application scenarios have significantly different security matching and network topologies, such as single-hop, multiple-hop, and mobile-tomobile networking. 3. Surveying the mapping of security requirements identified in the existing security threat models, followed by discussing how they are concerned with different roles in the network, such as hardware devices, on-body communication, or inter-WBAN. 4. Providing a comprehensive analysis of the security enhancements in WBANs, from the application layer to the physical layer.

2. Security Threats in WBANs

Threat modeling is a way in which a security analyst can assess the security threats and vulnerabilities. These are the few primary goals for which threat analysis has been emphasized. Since wireless body area networks handle personal, sensitive physiological data, they need an immense amount of security-enhanced mechanisms [3]. The risk involved in the WBAN can be classified roughly into low and high. The risk of the patient during their physical activity or events would be considered low, which will result in causing system unavailability for a specific amount of time [4]. Even if the patient is at rest, the system may be exploited, which may cause patient harm intentionally that falls under high risk. They are medical identity theft, unsanctioned disclosure of physiological data, and so on. The protection techniques are designed to focus on satisfying mutual-exclusion properties, which are confidentiality, integrity, data origin authenticity, non-repudiation, and authentication [5].

But in WBAN, they can carefully address data authenticity, integrity, authorization, and confidentiality. The security threats discussed are outlined based on the attack methods, intrusions, type of network access, the susceptibility of the sensors to produce false data, and data quality dependency of mobile nodes [6]. The systems got worse if the user or patient has the capability to intervene with the kind of sensors to generate false data and modify the data. Wearable healthcare users and consumers have a legitimate expectation of the privacy of health information, including personal activity data and physiological sensor data [7]. Public disclosure of this kind of health information without user consent and knowledge violates the privacy of the individual. The WBAN system is considered safe only if there are no violations such as unauthorized access or intrusions.

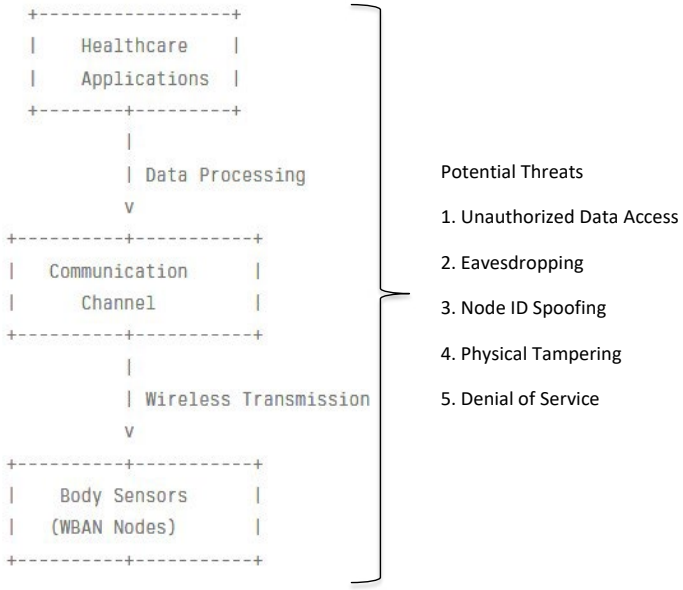

Figure 1: Potential Threats Areas

3. Overview of Threat Landscape

Nowadays, security has become increasingly important in Wireless Body Area Networks (WBAN) because of the information that WBAN carries about the patient's health condition. Malicious entities are mostly interested in exfiltrating this information or even manipulating it. In WBAN, the signal flowing between the sensors is unencrypted [8]. This means that to capture and interpret this signal at the forwarding node, one does not have to be a member of the healthcare team; anyone equipped with the right hardware and software can intrude on the conversation and opportunistically listen to its content without the sensor or forwarding node owner being aware of the privacy breach. An intruder may analyze patterns and steal the user's personal information, posing a threat to their security and privacy. Moreover, an intruder may also inject malicious data, altering the correct operation of the WBAN applications, and as a result, can also threaten a user's life [9].

In the WBAN, patients' critical signs are sent without any protection. Possibly, the captured channel is open, and a third party can monitor the signal, which is sensitive to patients' personal information. The user may also be exposed to physical security threats such as modification of the sensors, which results in data modification, or inference and denial of services, such as modification of the sensor to operate as an active emitter, which exhausts the user's energy [10].

Attack Type	Defense Mechanism	Description
Unauthorized Access	Encryption	Protects sensitive data during transmission
Node ID Spoofing	Signal Authentication	Uses shared Light ID for unicast transfer
Physical Tampering	Tamper-Proof Hardware	Prevents unauthorized physical access to sensors
Eavesdropping	Secure Key Management	Employs dedicated or derived keys for communication
Denial of Service	Traffic Monitoring	Detects and mitigates flood blast attacks

Table 1: Attack-Defense Matrix

For the design of an efficient security scheme, two fundamental steps are followed: threat modeling and security enhancements. In this survey, both aspects are considered. In particular, this section discusses a broader view of possible threats and more specifically in both the a) unique characteristics of WBAN security requirements that derive from its "natural application domain," i.e., the biomedical information that it carries, its structure, and architecture, and b) the implications of these requirements on the technologies that have been selected to secure WBAN communication. UWB is well matched to the ranging challenges posed by WBANs for sensor-to-sensor and sensor-to-station database communications. Then, acknowledging that spectrum overlap strategically benefits cognitive multiple access, it is natural for the cognitive sensor network to utilize the UWB signals of this WBAN for building presence detection [11]. This "in-parallel" design has two important consequences: the first is the potential to minimize any energy consumed by in-band "sniffing" of UWB because the presence detection is driven and performed by the sensor groups through their regular WBAN signaling; the second is a high security assurance level because the sensor and/or forwarding node, already knowing the spectrum "occupation," can restrict downstream transmissions to the guest STIME signal that passed or failed predefined presence/actuation tests. UWB secure WBAN uses channel characteristics and modern encryption techniques to protect Logical Link Control communication streams within the PAN, thus requiring a different kind of patient key for each non-overlapping group of patients for any PAN having more than one patient [12]. UWB secure WBAN does not assume privacy for remote recipients of all embedded patient data other than through WBAN implementation of a "point-to-point" link to the appropriate healthcare device.

4. Common Attack Vectors

The value of data makes them attractive targets for attackers, which can lead to data theft or integrity issues. This data includes positive drug responses or trial results, which can lead to large profits for a person with insider trading knowledge; infection data for viruses and pathogens, which could be leveraged for a variety of hostile capability, exploiting pandemic risk; and rare genetic predispositions in a population, which can lead to sensitive inferences [13]. Individuals who are being experimented on may not yet have personally identifiable information, which causes them to be unaware of being study subjects. There may be a lack of explicit consent from the individuals in such studies, and their options might be limited by involuntary incarceration, human subject tort doctrine, or other factors. A person who either coerces or threatens to coerce another person to participate as a study subject can be considered to be experimenting on that person for the person's own self.

Some researchers have identified systematized hosting in an artificial environment as a possible defense against unethical pursuit of financial or other gains during a disaster or public health emergency, as established by explicit protocols and contracts. Informatics technologies may aid in big data approaches to science, benchmarking, surveillance, and quality improvement activities in public health [14]. Use of individual health data in public-targeted health-related activities, with incentives and opportunities for patient participation in such efforts, can help guard against privacy and security erosion that comes from removal of personally identifiable information from the protections afforded by strict privacy requirements. Nonetheless, there are concerns regarding the sharing of so-called "anonymized" or non-personally identifiable information models derived from clinical sequences, medical imaging data, gene sequencing data and other datasets by third parties. These include concern that proper anonymization and measures to remove potentially identifying information cannot protect the models from such attacks as theory membership or other healthcare data privacy threats. It is important that all threats be considered with the advent of big data and public health and that these issues related to security and privacy be explicitly addressed [15]. It is not sufficient to react to breaches of patient privacy after the fact with notification to the affected stakeholders. There is a need for increased patient data independence based on ownership and ability to control or regulate research and for increased community data ownership and control rights.

5. Threat Modelling in WBANs

In this section, we discuss some of the most prevalent threats in WBANs and healthcare apps. A lack of attention to these threats can have serious implications for patient and healthcare operations in a variety of ways by attacking them. We mainly highlight the impact that potential attackers have on the wireless communication of WBANs [16]. However, one should also understand that in addition to communications, healthcare apps in data processing, and semi-trusted and untrusted people with physical access to body sensors and healthcare apps will also pose a huge threat to body sensor data. The liability of body sensors is enormous because body sensors collect various senior patient data, and their logic is relatively weak.

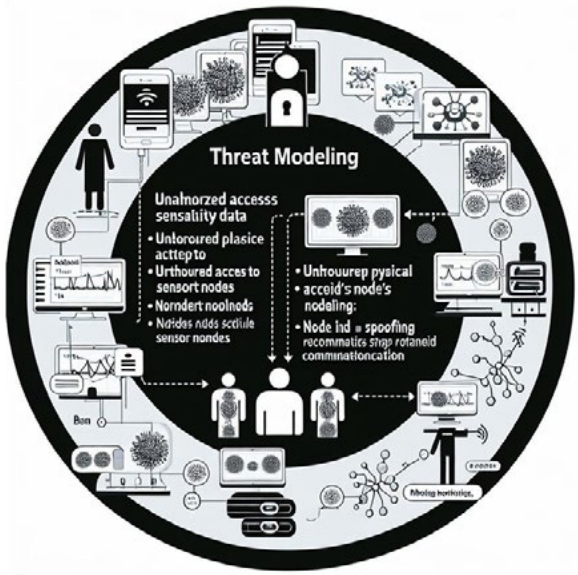

Figure 2: Threat Modelling "High Level Diagram"

Unauthorized access to sensitive data means accessing patient data on their sensor nodes and the communication stream between them to third parties. If transmitting data over untrusted communication channels is not properly encrypted, this can have a significant inadvertent effect [17]. A proper cryptographic method is necessary to ensure that unauthorized third parties cannot decrypt and read data streams. This helps to minimize the risk of data acquisition by any unauthorized attacker. As for a key encryption method for cryptographic communication streams, a dedicated key or a dependent key derived from the application user's access maintenance shall be individually used. Each healthcare app is designed with its own identity and associates with the sensor. In this way, the sensor's data transparency and protection can be achieved in healthcare apps.

The data will be ingested, analyzed, and pushed to the cloud by healthcare apps, so the patient needs to trust the security of the apps they are using [18]. Unauthorized physical access to the patient's sensor nodes/BANs is both affected by privacy and integrity. First, unauthorized physical access to PAN nodes or WBAN sensors is an appropriate invasion of a device and/or its data if some attacker succeeds. Due to sophisticated attackers, unauthorized sensor data collection can lead to an attacker passing themselves off as a legitimate user or another user associating health-related data with a legitimate user [3]. With additional control over sensor data, the sensor data transparency can also allow them to make sensor data stagnant in the desired atmosphere. Second, sensitive data can become entangled and look like medically similar data from other sensor cycles for advanced attackers. This entanglement can confuse the operator, thus leading to an adverse influence on patient health. Data integrity protection needs to be granted by an authorized judicial mandate that spectral measurements from body sensing devices offer guarantees of user privacy and data integrity so that the veracity of the sensed measurements cannot be accurately convinced. Moreover, these devices must be enabled to ensure measurement limitations [19].

Node ID spoofing in communication affects the sensor's trust. Due to this, legitimate sensor nodes cannot be acquired. The pervasive example is an attacker who executes a worn-out attack. This attack involves acquiring node service by exhausting the node battery [20]. It forwards a flood blast message that causes the sensor to consume an unsafe amount of traffic. For security, and to extend the lifetime of body sensor networks, signal authentication can be used on the body for the unicast transfer, using a shared Light ID that is randomly assigned to bodies of the same population. Periodic Light ID replacement without updating the device is necessary. Furthermore, the PAN identifier stays constant across the devices of interest of the same patient. The devices in a PAN form a RAM with the coordinator. The MED can convey via RAM; no frame pronouncements are allowed for data frames. Each MED is then arranged to learn a technique of understanding the additional intellectual condition of the body [21]. Several devices need to possess some basic knowledge of the body in the RAM or appointed RAM devices. Each time a new device joins the RAM, the guarding nurses need to update the teaching available knowledge data of the body.

6. Importance and Benefits

The critical nature of WBAN security in the smart healthcare sector mandates that all types of users, services, and equipment meet the regulatory guidelines. Due to the openness and complexity of the Internet, WBAN systems permit diverse types of threats, including those from insiders, such as medical staff, patients, or other legitimate users, as well as outside attackers using various types of attacks targeting the network infrastructure, sensing data, or privacy information. In a wearable health ecosystem, a gentle movement of the patient can change the nature of woven networked devices [22]. Therefore, unauthorized users may compromise patient medical data to speculatively develop and produce new products faster.

WBAN security is a critical consideration for personal healthcare

devices due to the requirement of data confidentiality during wireless data transfer, and also for intelligent wearable systems such as sensing and digital signal processors of infrastructures such as the cloud. Recently, security research has focused on ensuring authentication, key distribution and revocation, secure localization, and secure information protection [23]. Drug infusion pumps, which form important parts of hospitals' medical infrastructures, were also analyzed for their security flaws. These aspects may be vitally important for patient safety as well. One successful policy could consider the possible types of attackers, attack objectives, attack approaches, threat models, more specific security loading, security architecture, additional system efficiency, and open research issues. In this chapter, we first identify different intelligent sensing forms of patient health aspects and WBANs as standalone, in combination with, or support for a promising smart healthcare market [24]. We also establish threats and mandatory regulatory guidelines from different expert services. We propose a WBAN security modelling and testing structure using a logical attacker test, which is reminiscent of existing WBAN research models.

7. Key Components of Threat Modelling

Threat modelling is an effective tool used to evaluate security problems of resources and defended resources. Threat modelling is defined as an iterative and recursive process that uses models to define security objectives, threats, vulnerabilities, and mitigations. The models used in threat modelling may be expressed as schematics, text narratives, or any other conceptual representation, as long as the resulting model can be used to expose threats [25]. These models must be used to formulate and ask a two-fold question: what are we working to protect, and what are we protecting it from? In other words, threat modelling is useful to understand and prioritize threats in your setting (or settings) and then document available mitigations. Threat modelling may be used in a number of ways to benefit the SMB healthcare community.

An example of its use is to aid in identifying, assessing, and mitigating key privacy and security risks in the design phase or principal reengineering of second-generation EHRs or personal health records. Another use of it is to assist the stratified rapid vulnerability identification and risk assessment of a specific security concern associated with a set of personal health information managed by a third party in the context of EHR system management. In addition, it can help review, evaluate, and prioritize privacy and security requirements, and privacy and security architecture and security policy elements for inclusion in an electronic health care information system [26]. Yet another use of it is to explore potential privacy and security control policies for incorporation in a national health information network within the broader framework of an open network security testing and dissemination community.

8. Security Enhancements for WBANs

Security is an important concern whenever healthcare data is involved. All data, especially health-related data, is personal and highly sensitive in nature, and compliance must be met with strict healthcare regulations. A review of the known security and privacy issues and their consequences in WBANs is provided. In this paper, we present a security framework model that provides ways to ensure security in the context of WBANs for smart Healthcare applications. A security enhancement gained by adding a packet ID to the cross-layer feedback routine and seal handshake into the medium access control protocol is also presented. By realizing that security services provided by the current standard are not sufficient, we are working to propose an addition to the standard through the security framework model we have already proposed.

Wireless Body Area Networks (WBANs) play a crucial role in smart healthcare by enabling continuous monitoring of patients' health status. Threat modeling and security enhancements are essential in ensuring the privacy and integrity of sensitive data transmitted over these networks. This essay will discuss the importance of using the ServiceNow Security Operations platform to enhance security in WBANs. Using the ServiceNow Security Operations platform can help in identifying and mitigating security threats in Wireless Body Area Networks for Smart Healthcare.

We have created a cross-layer secure communication framework that allows identification of potential threats and standard security mechanisms, and how they can be applied to the protocol stack. We therefore review the secure communication services currently provided by the standard and compare them to the ones required by typical applications to highlight any missing features. The secure communication framework we have created consists of a set of security requirements derived from typical applications. These requirements take into account different communication patterns and critical points, as well as attackers and threats. They are then split into six categories: confidentiality, availability, authenticity, message integrity, nonrepudiation, and security management. Finally, we describe the protocol state types and show experimentally how routines can be implemented in a framework.

9. Encryption and Authentication Mechanisms

The role of cryptography in healthcare applications is extremely crucial. Accordingly, suitable encryption mechanisms are required for guaranteeing the related privacy, integrity, and security properties. Additionally, one has to guarantee, using some means, that critical messages (e.g., those regarding medical instructions for a patient) have not been tampered with. Techniques from the field of cryptography provide the required security properties (e.g., confidentiality, integrity, authenticity) that are necessary for Body-BANs healthcare applications [27]. Multi-encryption has to be used in combination with message authentication codes (MACs) in order to provide an additional layer of security that guarantees that message content has not been tampered with.

Noteworthy are the symmetric key encryption algorithms, which are known for their fast processing capabilities. Accordingly, the process of encryption and then decryption can transpire with relatively low time delays. Although encryption with symmetric key algorithms is much faster than public key algorithms and requires fewer computations, the problem with this class of algorithms is that

the key has to be shared secretly among the digital communicators. Public key encryption does not demand beforehand secure sharing of encryption and decryption schemes. Publickey cryptography, in the single direction sense, entails that one person can prepare a message that is secure against eavesdropping while the other person can receive and decrypt it securely. Given the capability of public-key cryptography to authenticate either direction, it is often applied for executing digital signatures. Despite its popularity, the use of public and private key encryptions seems to be unsuitable for healthcare-related wireless BANs, on account of their high processing requirements.

10. Intrusion Detection Systems

In general terms, the aim of an intrusion detection system (IDS) is to prevent unauthorized access or to disable or deter intrusion attacks. An IDS can be designed at different levels, i.e., at a host, networking, or global level, or in a distributed way, which is then defined by the particular requisites of the target network. The functionality of an intrusion detection system may also significantly vary as it can monitor, detect, and then alert, or it can also enforce and implement security policies [28]. The intrusion detection systems are further divided into two categories based on the behavior of the IDS engine, namely misuse IDSs (where already known malicious behavior is evaluated), which could be rule-based or signature-based, and anomaly-based IDSs (these use machine learning techniques to establish baseline performance and detect deviations from what is defined as 'normal operation'). Among these, anomaly-based IDS is defined as one that uses numerous behaviors to define what is considered to be normal, and then catches any behavior that is beyond that normal threshold.

Basically, the anomaly IDS functions by comparing the current performance of the WSN with previously seen behavior or behaviors never seen before, and alerts or logs appropriate information in case of serious deviations. The performance may be evaluated against standard performance/operating metrics, such as power consumption, packet error rate, and radio interferences. Anomaly-based IDSs may be more resilient to previously unknown unusual behavior or novel attacks. They may detect many non-specific attacks unless they operate by creating a profile of ordinary traffic to use as their signature. Such signature-based anomaly detectors have a problem in learning and modeling normal behavior profiles, as well as adapting to different network behaviors depending on specific operating conditions [29]. The tricky part is when the functionality of an IDS is unknown or not clearly specified. In the case of Human Body Area Networks, the devices move with time, which is a characteristic anomaly behavior. The WSNs are typically deployed in regions with inhomogeneous statistics and are expected to continuously adjust their functionality to the instantaneous network state, which, again, is a characteristic anomaly behavior.

11. Case Studies and Practical Implementations

In Section 5, we presented several potential security threats in wireless body area networks for smart healthcare based on the environment, battery energy, and emergency situations, the critical role of the BAN coordinator in the WBAN, nonsecure medical device communication with the sink, and vulnerabilities whenever the BAN is under attack. In this section, we exemplify three case studies of threat models and enhanced security measures in various scenarios such as: (1) a hospital with a medical service communication scenario; (2) a sports exercise or physical workout center that collects exercise data for future physical therapy reference; (3) an implantable or carry-on database storage device and health management scenario for physical fitness and activity collection, reporting, and recommendations. The results demonstrated and ensured that the data could be sent safely. Furthermore, based on the security solutions in a real WBAN system, we presented several common security improvements to resolve WBAN security issues.

Finally, as an addition to this work, we introduced BANMAC enhancements that could improve WBAN security. Most of the proposed solutions in this work depend on the application processor to achieve these benefits. One of the most basic principles in WBAN is that it should have up to seven medical sensors with a 2-Mbps data rate for full use of the channel bandwidth at the same time. It is strongly recommended to use a specific communication protocol for the first stage of the preliminary protocol in many applications, which means the connection setup between any two devices. However, as in other data link layers, the integrity and confidentiality of the data are equally important. At present, there is no protocol that has efficiency and also ensures these factors. Although secure versions of the specified network will soon be proposed, it also achieves data integrity and confidentiality with low computational complexity in this work.

12. Future Research Directions

Multidisciplinary sectors of medicine, computer science, and communication technologies are combined for the development of a WBAN for smart healthcare. Security in all aspects of any communication network for sensitive and important information should be provided. However, securing the WBAN beyond the interdisciplinary fields is also an important task that not only allows our WBAN to be useful but also enhances the system's efficiency. Therefore, mainly in three aspects, future research work should be carried out to further analyze the security issues included within the wide scope of security for the WBAN. To deal with this interdisciplinary research field, we mainly consider first wireless communication technologies, including routing protocols, efficient schemes for bandwidth, considering human factors and different channel scenarios, as well as security issues. Other related challenges are biocompatibility issues, security, and privacy issues. Then, to promote the development of WBANs, further research is imperative to overcome other existing technical, social, and legal limitations for global e-health, especially in rural areas, hospitals, and in emergencies.

Research in designing dedicated security algorithms, as well as implementing them, such as cryptographic functions, hash functions, and pseudorandom number generators, is mainly necessary. These algorithms will have several specific

characteristics, not only due to the on-body and off-body status but also in scenarios with an increasing number of implanted or worn sensors over a patient; different evolution models of system architectures could be considered. Training the medical staff in the use of the easiest WBAN devices is another important challenge in promoting large-scale use. Also, audit and control in the access of information and the privacy of data is at the backbone. The user should clearly be advised when information is gathered and has to know, as soon as he is interested, the information gathered; the safety of the communication link must also be granted. Further studies focusing on the development of WBAN architectures capable of addressing data integrity, authenticity, privacy, and data confidentiality in a secure and efficient way, and legal limitations in e-health, in particular in relation to liability, could be conducted in the field of security and real-time communication and in the power supply management of wearable devices.

13. Conclusion and Recommendations

In this chapter, we started with an introduction to threats and the impact that threats in WBANs expose in smart healthcare, followed by using threat modeling for identifying threats. We then moved to discussing various attacks and security services when seamless support for regular or multimedia data traffic provisioning. First, we developed three traffic models for capturing the data traffic when static health monitoring and regular and multimedia health supervisory services are supported. Based on the models, we identified various multi-level attacks and then classified and showed that keeping a record of open, issued, and sent alarms in an alarm pool could be worthwhile in reducing the attack surface. We then identified the security solutions to address the attacks. Fortunately, many medical bodies, standard organizations, and research institutions are currently working towards identifying mechanisms to secure the data transmitted in medical systems. We demonstrated the solutions and compared them. We then discussed the applicability of the solutions to real-world systems and their performance in terms of signaling, energy, and delay analysis. We followed this with various concluding remarks.

We consider relevant recommendations and conclusions to guide WBAN designers, implementers, and healthcare workers. In smart e-healthcare environments, security is crucial. While research efforts are continuously being made towards the development of security solutions, many of them apply to particular systems and may not scale or apply to newly built ones. In addition, as the number of WBAN systems and the applications they support increases, so do the demands and overload of trusted authority servers used to ensure that deployed systems meet the necessary governing access and power constraints. The respective signaling overhead and the probability of excessive regulation costs and/or reduced resource usage must be studied. Specifically, lightweight security standards must be provided, and energy-efficient security algorithms must be designed. Moreover, since both patients' information and functionality are most pivotal in such systems, new trust management models must be designed to transparently and securely guarantee high interoperability and mutual authentication. Although we have studied the attack surface of threats for three classes of e-healthcare applications, future work may target new technical aspects such as existing threats and the vulnerabilities they expose; the work will typically measure the time taken to reach certain security conditions and obtain the appropriate trade-offs; and the design of a resilient intrusion detection system.

References

1. Javaid, S., Zeadally, S., Fahim, H., & He, B. (2022). Medical sensors and their integration in wireless body area networks for pervasive healthcare delivery: A review. *IEEE Sensors Journal, 22*(5), 3860-3877.
2. Ayub, K., & Alshawa, R. (2024, October). A Novel AI Framework for WBAN Event Correlation in Healthcare: ServiceNow AIOps approach. In *2024 IEEE Workshop on Microwave Theory and Technology in Wireless Communications (MTTW)* (pp. 55-60). IEEE.
3. Roy, M., Chowdhury, C., & Aslam, N. (2020). Security and privacy issues in wireless sensor and body area networks. Handbook of Computer Networks and Cyber Security: *Principles and Paradigms,* 173-200.
4. Niu, Y., Nazeri, S., Hashim, W., Alkahtani, A. A. A., & Abdulshaheed, H. R. (2021). A survey on short-range WBAN communication; technical overview of several standard wireless technologies. *Periodicals of Engineering and Natural Sciences (PEN), 9*(4), 877-885.
5. Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters, 8*(3), 66-77.
6. Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., ... & Duncan, E. (2021). A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures. *Applied Sciences, 11*(16), 7518.
7. Rising, C. J., Gaysynsky, A., Blake, K. D., Jensen, R. E., & Oh, A. (2021). Willingness to share data from wearable health and activity trackers: analysis of the 2019 health information national trends survey data. *JMIR mHealth and uHealth, 9*(12), e29190.
8. Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2021). Performance enhancement in wireless body area networks with secure communication. *Wireless Personal Communications, 116*, 1-22.
9. Sharma, A., Tyagi, A., & Bhardwaj, M. (2022). Analysis of techniques and attacking pattern in cyber security approach: A survey. *International journal of health sciences,* (II), 431188.
10. Billah, M. (2023). Energy-efficient early emergency detection for healthcare monitoring on WBAN platform (Doctoral dissertation, Staffordshire University).
11. Vyas, A., Pal, S., & Saha, B. K. (2021). Relay-based communications in WBANs: A comprehensive survey. *ACM Computing Surveys (CSUR), 54*(1), 1-34.
12. Ahmed, I., Karvonen, H., Kumpuniemi, T., & Katz, M. (2020). Wireless communications for the hospital of the future: requirements, challenges and solutions. *International Journal of Wireless Information Networks, 27*(1), 4-17.

13. Wachter, R. M., & Brynjolfsson, E. (2024). Will generative artificial intelligence deliver on its promise in health care?. *Jama, 331*(1), 65-69.
14. Batko, K., & Ślęzak, A. (2022). The use of Big Data Analytics in healthcare. *Journal of big Data, 9*(1), 3.
15. Onesimu, J. A., Karthikeyan, J., & Sei, Y. (2021). An efficient clustering-based anonymization scheme for privacy-preserving data collection in IoT based healthcare services. *Peer-to-Peer Networking and Applications, 14*(3), 1629-1649.
16. Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems, 44*, 1-9.
17. Ayub, K., & Zagurskis, V. (2016, June). SMART Incubator: Implementation of Impulse Radio Ultra Wideband Based PA-MAC Architecture in Wireless Body Area Network. In *2016 International Conference on Systems Informatics, Modelling and Simulation (SIMS)* (pp. 25-31). IEEE.
18. Heidel, A., & Hagist, C. (2020). Potential benefits and risks resulting from the introduction of health apps and wearables into the German statutory health care system: scoping review. *JMIR mHealth and uHealth, 8*(9), e16444.
19. Sen, S., Maity, S., & Das, D. (2020). The body is the network: To safeguard sensitive data, turn flesh and tissue into a secure wireless channel. *IEEE Spectrum, 57*(12), 44-49.
20. Mannix, K., Gorey, A., O'Shea, D., & Newe, T. (2022). Sensor network environments: A review of the attacks and trust management models for securing them. *Journal of Sensor and Actuator Networks, 11*(3), 43.
21. Keymeulen, B., De Groot, K., Jacobs-Tulleneers-Thevissen, D., Thompson, D. M., Bellin, M. D., Kroon, E. J., ... & Pipeleers, D. (2023). Encapsulated stem cell–derived β cells exert glucose control in patients with type 1 diabetes. *Nature biotechnology,* 1-8.
22. 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.
23. Soni, M., & Singh, D. K. (2023). New directions for security attacks, privacy, and malware detection in WBAN. *Evolutionary Intelligence, 16*(6), 1917-1934.
24. Jose, J. M., Jose, J. V., & Vijaykumar Mahamuni, C. (2020). Multi-biosensor based wireless body area networks (WBAN) for critical health monitoring of patients in mental health care centers: an interdisciplinary study. *International Journal of Research in Engineering, Science and Management, 3.*
25. Lee, C. C., Tan, T. G., Sharma, V., & Zhou, J. (2021). Quantum computing threat modelling on a generic cps setup. In Applied Cryptography and Network Security Workshops: ACNS 2021 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA, Kamakura, Japan, June 21–24, 2021, Proceedings (pp. 171-190). Springer International Publishing.
26. Albahri, A. S., Duhaim, A. M., Fadhel, M. A., Alnoor, A., Baqer, N. S., Alzubaidi, L., ... & Deveci, M. (2023). A systematic review of trustworthy and explainable artificial intelligence in healthcare: Assessment of quality, bias risk, and data fusion. *Information Fusion, 96,* 156-191.
27. Das, M., Tao, X., & Cheng, J. C. (2021). BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in construction, 126,* 103682.
28. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing, 26*(6), 3753-3780.
29. Landril, E., Valente, S., Andersen, G., & Schneider, C. (2024). Ransomware detection through dynamic behavior-based profiling using real-time crypto-anomaly filtering.