Analysis of Attacks and Security Requirements for Wireless Body Area Networks - A Systematic Literature Review

Pangkaj Chandra Paul, John Loane[0000-0002-9285-5019], Gilbert Regan and Fergal McCaffery

Regulated Software Research Centre, Dundalk Institute of Technology
Dundalk, Co. Louth, Ireland

Abstract. Wireless Body Area Networks are gaining popularity in healthcare applications due to recent advances in sensor technology, integrated circuits, and wireless communication. These systems need to ensure that data is protected during collection, transmission, processing and storage. Currently, no complete solution exists for ensuring data is protected while also meeting regulatory security requirements for wireless body area network applications. To develop effective solutions, it is necessary to explore the attacks and security requirements of wireless body area network applications. There is no comprehensive list of attacks and security requirements. This paper will present a systematic literature review of potential attacks and security requirements for ensuring data security in wireless body area networks.

Keywords: wireless body area network, security requirements, security issues, types of attacks, data security.

1 Introduction

Wireless body area network applications (WBANs) can provide long-term health monitoring of patient's physiological states without constraining their normal activities. The latest international standard for WBAN applications, IEEE 802.15.6 [1] divides WBAN applications into two categories 1) Medical applications and 2) Non-medical applications. In a medical application, a WBAN can be used to collect vital patient health record (PHR) data and transmit it to monitoring systems for further analysis. This information can be used to provide real-time monitoring of a patient having various diseases such as cancer, asthma, diabetes and neurological disorders as well as people with physical disabilities.

A WBAN application consists of intelligent, low-powered sensor nodes [2]. These sensor nodes can be placed on different parts of the body and can be wearable or implanted under the skin. These sensor nodes can collect data, perform data processing, store data locally and transmit data to an actuator or a local server. A personal digital assistant device or a computer is commonly used as a local server. This local server will receive all data from the different sensor nodes and transmit it to a central server through a base station using various communication media such as WiMAX, GPRS or GSM. A general architecture for WBAN applications is illustrated in **Fig. 1**.

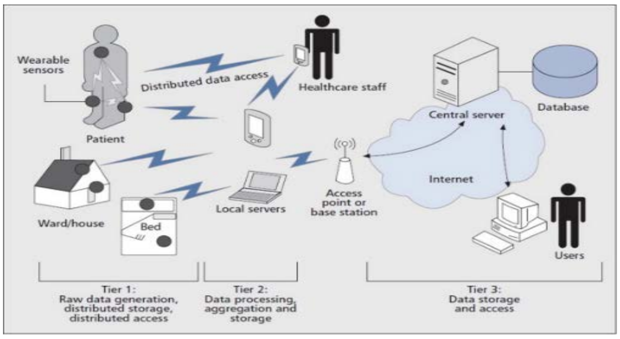
Wearable sensors
Distributed data access
Healthcare staff
Central server
Database
Patient
Internet
Ward/house
Bed
Local servers
Access point or base station
Users
Tier 1: Raw data generation, distributed storage, distributed access
Tier 2: Data processing, aggregation and storage
Tier 3: Data storage and access

Fig. 1. A general architecture of WBAN applications [3]

At present no security framework exists for WBAN. To develop such a framework, we need to understand the current knowledge base for WBAN attack types and security requirements. This paper presents a literature review of these attacks and requirements. The rest of this paper is organised as follows; Section 2 presents the background of this report and Section 3 briefly describes the systematic literature review process. Section 4, details the types of attacks while Section 5 provides the security requirements for WBAN applications. Finally, Section 6 concludes the paper with future work.

2 Background

In [4] the authors state that security is required at four levels in a WBAN application. A WBAN's network and physical level are vulnerable to different types of attack such as eavesdropping, jamming and node capture attack. At the application level, security requirements include confidentiality, integrity, and authentication of the data including proper access control, accountability, and revocability. In [5], the authors detailed similar security requirements to [4], while also including protection against Denial-of-service (DoS) attacks to ensure availability. In [6] the authors added the following attacks: replay attack, man-in-the-middle attack and collision attack for intra-body area network communication. The authors also presented a list of security requirements to develop a secure key management scheme. In [7], the authors illustrated that privacy rules and compliance requirements are needed to ensure data security and privacy in addition to data confidentiality, integrity and authentication. In [8], the authors listed a total of 13 security requirements related to data privacy for cloud assisted WBAN based healthcare applications but did not present any attack types.

After analysing the existing literature, we identified that none of the existing surveys contains a comprehensive list of attack types and/or security requirements for WBAN applications.

3 Systematic literature review process

This literature review uses a systematic approach following the guidelines proposed by Barbara Kitchenham [9]. The following research questions were used to keep the research strongly focused:

RQ 1: What types of attack threaten wireless body area network applications?

RQ 2: What security requirements are needed to secure wireless body area network applications?

To identify the relevant primary literature, the search string below was designed by using keywords from the research questions.

(WBAN OR "wireless body area network" OR "wearable wireless body area network") AND ("security risks" OR "security challenges" OR "security issues" OR "security requirements" OR "types of attack")

In addition to defining search strings, the digital libraries listed in Fig. 2 have been selected for the search process.

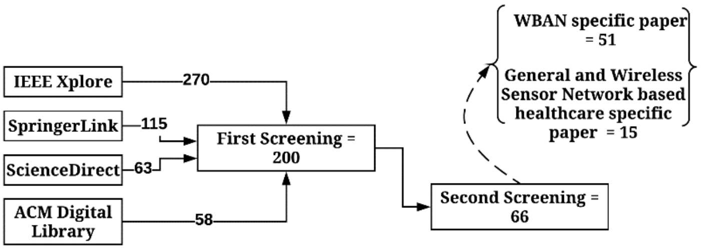

Fig. 2. Paper selection process during the systematic literature review

- **Initial search**

  The initial search was performed using the inclusion and exclusion criteria presented in **Table 1**. This resulted in a total of 506 papers. All search results from each database were recorded into a spreadsheet with a unique number, title, abstract, type of publication, publication date, author's name, and number of citations.

Table 1. Inclusion and Exclusion Criteria

Inclusion	Exclusion
- Publication year: 2008-2018 - Language: English - Full text available	- Literature that neither identifies nor addresses data security challenges or attacks in WBAN applications - Exclude position papers, book reviews, anonymous publications - Exclude duplicate studies - Grey literature sources

- **First screening**

  In the first screening step, each research paper was analysed by reviewing the abstract. If the abstract addressed attacks or security requirements for WBAN or sensor-based healthcare applications, it was selected for a second screening. Otherwise, it was discarded. As indicated in **Fig. 2**, a total of 200 out of 506 papers were selected for second screening.

- **Second screening**
  In the second screening, individual papers were analysed by reading the full text. In this screening process, research papers were selected for further analysis if the paper presented attacks or security requirements for WBAN or sensor-based healthcare applications. Where multiple terms were used to refer to the same attack or security requirement, these are indicated in sections 4 and 5 by separating with a "/". For example, physical attack and node-compromising attack are used interchangeably in the literature, and in this paper referred to as physical attack / node-compromising attack. This was achieved by comparing each author's definition of the term. The second screening resulted in a total of 66 relevant papers. Out of the 66 papers, 51 papers discussed security challenges and attacks related to WBAN applications and the rest discussed security challenges and attacks related to generic and Wireless Sensor Network (WSN) based healthcare applications. Finally, all papers were divided into two categories; 1) papers which addressed security requirements, 2) papers which addressed various attacks on WBAN applications. Some papers, which addressed both requirements and attacks were placed in both categories.

4 Types of attacks

WBAN applications are vulnerable and open to many types of attacks and threats as sensor nodes operate in an environment where the sensor node uses low powered radio signals for communication. The end-user may use open internet access to connect to the application. This open connectivity feature creates a large attack surface. These attacks can affect the performance and availability of the service, sometimes leading to life threating situations or even death [10]. A list of attacks unearthed during the literature review is now presented with the number of references, along with a brief note on how these attack types could affect WBAN applications. For example, in eavesdropping (29), 29 represents the number of references.

Denial of Service (DoS) (26): As WBAN applications use low-frequency wireless mediums, an attacker can transmit noisy signals to interfere with radio signal to drop the traffic [11]. A DoS attack can lead to unavailability of the service for other sensor nodes in the network related to channel access [12]. Referenced in: [3, 6, 7, 13–33].

Eavesdropping (29): By intercepting communications between the sensor node and the base station an attacker can collect PHR data and/or device information. An attacker can use this data to introduce themselves as an authorised member to launch an impersonation attack [6] or break the key exchange technique during the pairing phase [27]. Referenced in: [3, 11–15, 17, 19–21, 23, 25, 28, 30, 32, 34–45].

Man-in-the-middle (9): An attacker can place himself as a relay or proxy into a communication session between sensor nodes and/or end-user applications in WBANs. The attacker can eavesdrop and manipulate the message in real-time without the sender or receiver noticing [6]. Referenced in: [32],[13],[16],[19],[21],[46],[26].

Insider attack (4): In WBAN applications an attacker can launch an insider attack by using a physically compromised node with authorised system access to drop, modify and misroute data packets to harm normal network functionality [8],[13],[15],[34].

Sniffing attack (1): An outside attacker can retrieve vital information including source and destination address, port and protocol type from network data packets using network sniffing tools if not encrypted [29].

Physical attack / node-compromising attack (12): As sensor nodes of a wearable WBAN are placed on the body, they are not tamper proof [3]. By injecting malicious code, an attacker can alter or extract data including the cryptographic key, PHR data and re-engineer the system. This altered health-related data may result in a patient's death [7]. Referenced in: [6],[11],[30],[32],[16],[18],[19],[35],[47],[40].

Sinkhole attack (3): In WBAN, a compromised node can advertise itself as a best possible route to the base station to its neighbouring nodes and subsequently drop or redirect all collected packets which will never reach their destination [6],[11],[30].

Masquerading attack (7): In a WBAN application, an attacker can impersonate or clone an authenticating device to launch a masquerading attack for the purposes of stealing data, injecting false information or getting full access to the healthcare application. With full access to the application, the attacker can modify or delete PHR data from the medical database [34]. Referenced in : [3],[27],[32],[21],[43],[45].

Spoofing and Sybil attack (7): A spoofing attack is when a malicious node masquerades as a legitimate entity of the system to disrupt the network while avoiding detection. In WBAN applications, this attack also facilitates the larger Sybil attack where identities of multiple nodes in the network are compromised [11]. Referenced in: [6],[12],[29],[30],[19],[44].

Data falsification / Data modification (23): An attacker can perform unauthorised modification of data to falsify the information by placing a compromised node nearby which can trigger a false alarm or send unnecessary responses [30]. Referenced in: [3, 6, 11, 14, 15, 17, 18, 20–22, 27, 30, 32, 34–38, 42–44, 46, 48].

Replay attack (23): In a WBAN application, the attacker can collect PHR and continuously retransmit to trick the receiver into causing confusion and errors in the system [28]. Referenced in: [6, 8, 11, 13–17, 20, 21, 26, 27, 30, 31, 37, 38, 43–48].

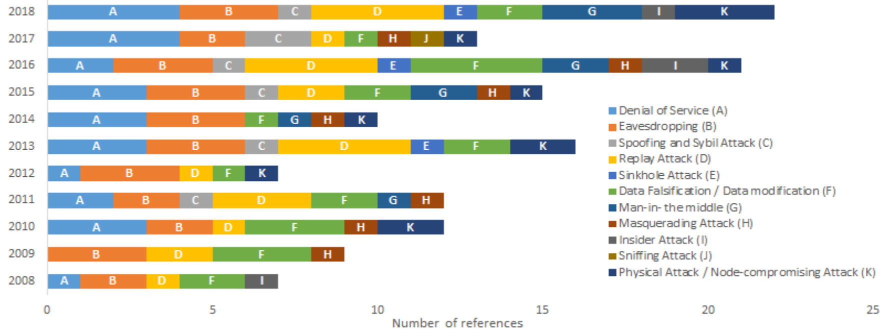

Fig. 3. Attack trends for WBAN applications throughout 2008-2018

The reviewed literature indicates that the most referenced attacks for WBAN application are eavesdropping, DoS, data falsification, replay attack and physical attack, least referenced attacks are sinkhole and sniffing attack. A trend analysis of attacks related to WBAN application from 2008 to 2018 is presented in **Fig. 3**. The number of types of attack gradually increased from five in 2008 to nine in 2018. Authors start discussing spoofing attacks from 2011 onwards and these attacks continue as trending attacks from 2015-2018. Although sniffing attacks are a widely known attack in the context of network security for capturing data packets from the network by using sniffing tools, very few authors have addressed these attacks for WBAN applications.

5 WBAN security requirements

The security of PHR is one of the primary challenges of WBAN systems. The data confidentiality, integrity and availability (CIA) triad is a common concept to ensure data security. To ensure the CIA of data in WBAN applications, there are some other security requirements that need to be taken into account, such as access control, key management and lightweight cryptography algorithms. The literature review conducted as part of this research unearthed 22 security requirements. These 22 security requirements and their relevance to WBAN are now discussed. The number in brackets after each requirement indicates the number of references, for example, data confidentiality was mentioned in 47 of the selected papers.

Data Confidentiality (47): Since WBAN healthcare applications contain sensor nodes that store and transmit PHR data, data confidentiality is one of the most important challenges [49]. PHR data needs to be protected from unauthorised access and leaking while in storage in a sensor node or local server [3]. Referenced in: [6–8, 11, 13–19, 26–33, 35, 36, 41–45, 47, 48, 50–66].

Data Integrity (46): As data confidentiality does not protect data from external modifications, data integrity provides assurances that data is not modified during transmission or while in storage [31]. As WBAN applications contain sensitive PHR, a patient’s life could be in danger without the protection of data integrity [8]. Referenced in: [3, 6, 7, 11, 12, 14–20, 26–28, 30, 32, 33, 35–38, 41, 42, 45, 47, 49–64, 66, 67].

Authentication (48): In WBAN applications, the authentication process will check the identity of a user before allowing access to any PHR data. Both senders and receivers in the network can authenticate each other by a mutual-authentication technique [7]. This will help to mitigate man-in-middle attacks [6]. Referenced in: [3, 7, 8, 12–14, 16–21, 26, 29–33, 35–45, 47, 49–58, 60–64, 66, 68, 69].

Availability (26): In WBAN applications, data availability ensures that data is available to authorised entities whenever it is required [32]. In a medical emergency, the unavailability of PHR data may lead to loss of life of a patient [50]. Referenced in: [3, 7, 11, 13–15, 17–19, 26, 27, 30, 31, 33, 36, 39, 47, 49, 51, 54, 57, 59, 60, 64].

Data Privacy (26): Data privacy ensures that only authorised persons can access the data. In WBAN applications data privacy is a major concern, and it is necessary to ensure that PHR data is not leaked to unauthorised persons [52][53]. Referenced in: [8, 17–19, 26, 29, 31, 33, 36–40, 42, 43, 45, 48–53, 59, 63, 64, 67].

Access Control (19): Access control is also a growing concern for maintaining privacy in WBAN applications due to the sensitivity of the data. This data can be accessible by multiple entities such as doctors, medical staff, pharmacies and other service agencies [3]. In [8], the authors state that a fine-grained access control policy is necessary to ensure that PHR data will not be accessed by an unauthorised entity. Referenced in: [6, 12, 14, 19, 21, 33, 36, 43, 48, 49, 55–57, 60, 64, 66, 68].

Non-repudiation (13): To preserve the privacy of the PHR, the application needs to have the ability to ensure that an entity cannot deny the authenticity of a message which originated from it. It is necessary to keep a constant check on the activity of that authenticated user so that it will be unable to deny that it made certain changes [8]. Referenced in: [3, 14, 19, 31, 33, 36, 49, 52, 56–58, 65].

Encryption / Cryptography (20): As WBAN sensor nodes have limited processing power, and have memory and energy constraints, data encryption is a key challenge. With the help of lightweight and energy efficient cryptography algorithms, data will be encrypted while it resides in storage [53],[51]. Referenced in: [8, 12, 19–21, 26, 29, 33, 37, 38, 40, 42, 43, 45, 48, 50, 60, 64].

Key Management (20): In WBAN applications, key management is constrained by sensors computational power, battery power, memory and transmission range. In [70] the authors present that generating unique cryptographic keys is the most important challenge to ensure data security. Similarly, key revocation and renewal processes need to be in place to revoke a compromised cryptographic key. Referenced in: [7, 16–19, 21, 28, 33, 35, 41, 43, 45, 47, 50, 52, 54, 60, 64, 65, 68].

Data Freshness (20): Data freshness is an important factor in ensuring data integrity and confidentially. It assures that data packets are in the correct format and not previously used [50]. In [7] the authors present that data freshness is required when a sensor node is performing a synchronisation process with the coordinator or a personal server. Referenced in: [6, 7, 14, 17–20, 28, 31, 33, 37, 38, 45, 47, 48, 50, 51, 54, 60, 62].

Firewall (1): In WBAN applications firewalls can be used as the first line of defence to protect sensitive information. The use of firewalls with access control can mitigate different attacks and restrict malicious users from gaining access to the application [12].

Client Platform Security (1): In WBAN applications, the end-user system includes mobile devices, PC and networks which are used for storing or processing data. In [8], the authors state that if these end-user systems are comprised by an attacker, the privacy of stored PHR data may be jeopardised, or it may leave the system open to attacks.

Accountability (7): In WBANs, healthcare providers need to safeguard PHR data by identifying unauthorized actions by users and make the user (both authorised and unauthorised) accountable for their actions [8],[49]. Referenced in: [3, 57, 64, 66].

Revocability (4): In WBAN applications it is necessary to have a fine-grained revocation process to revoke a user's privileges or to revoke a sensor node as soon as they are identified as compromised or behave maliciously [31]. Referenced in: [3] [49, 57].

Forward secrecy / Backward secrecy (3): To preserve data confidentiality and privacy it is necessary to ensure that an attacker cannot trace any data by collecting information from previous and future communication between sensor node and application. Proper key management and cryptographic techniques with forward and backward secrecy are needed to preserve data confidentiality and privacy [35],[52],[13].

Physical Protection (1): In [68], the authors stated that medical backend data servers are one of the most security-critical devices in a WBAN application. The backend server is used to collect and store PHR data from all the sensor nodes. It is necessary to ensure physical security by implementing appropriate access controls.

Auditability (2): Auditability is one of the least addressed security requirements for ensuring data privacy in a healthcare application [8, 66]. In a healthcare application patients might not want to grant access to PHR data to healthcare providers. It is necessary to keep track of access activities to PHR data even if it is by an authorised entity [8]. If anybody tries to misuse the PHR data, it can be tracked through auditing.

Anonymity (4): For a WBAN application, it is necessary to ensure that an adversary cannot trace any user identity by collecting sensor data [13]. Anonymised data will protect users' privacy as a particular individual will not be able to be linked or associated with the data during the transmission or storage processes [8],[16],[66].

Regulations and compliance requirement (1): It is necessary to implement different sets of regulations or policies in WBAN applications to protect the patient's privacy [7]. If any healthcare service provider fails to meet the rules and a data breach happens, the service provider can face civil or criminal consequences, including fines.

Resiliency (5): Resilience is defined as how capable the system is in resisting external and internal failures and how fast the system can recover. To ensure the reliability of WBAN applications, the system needs to have the ability to self-heal if any failures occur regardless the type of failures [18]. Referenced in:[14],[60],[16],[44].

Trust Management (4): In a WBAN based healthcare application trust management is required to verify that data originates from a trusted sensor and not from an attacker. It will help to provide a tamper-proof and efficient service by creating trustworthiness between sensor nodes [7],[60][18]. Without a trust-based security solution in place, cryptographic solutions can become ineffective or useless against an insider attack [30].

Intrusion Detection (4): An intrusion detection system is used a set of rules to identify and block suspicious activity in a network. In [7] the authors present rule and anomaly based intrusion detection systems for a WBAN application to find anomaly against pre-defined attack patterns or profiled behaviours. Referenced in: [30],[18],[19].

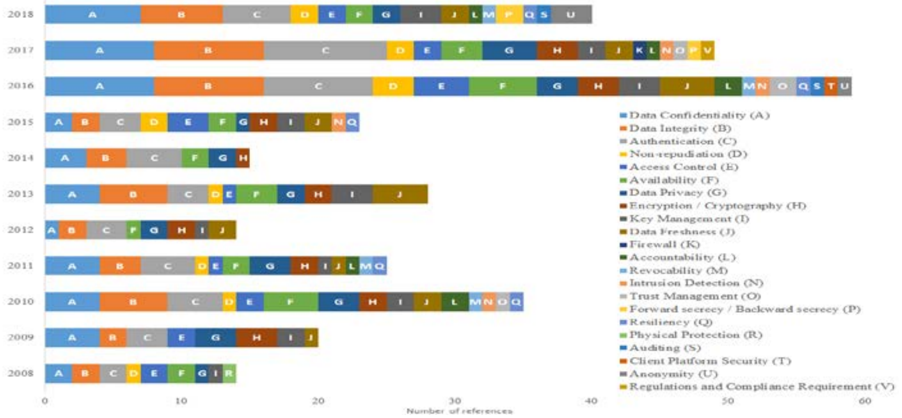

Fig. 4. Security requirements trend for WBAN application throughout 2008-2018

The reviewed literature indicates that the most referenced and trending WBAN security requirements are data confidentially, integrity, availability, authentication and privacy over the last ten years. Trends in security requirements between 2008 and 2018 are presented in **Fig. 4**. It can be seen that the number of security requirements gradually increase over the ten years and almost double from 2008 to 2018. Among them, non-repudiation, access control, key management, encryption and data freshness are the second most referenced security requirements since 2008. Due to easy access to apps installed on mobile devices auditing, client platform security and anonymity have appeared from 2016 onwards. In 2017 onwards firewall, forward and backward secrecy, regulations and compliance requirements have been added. Although firewalls are common in generic web applications, communication between mobile apps and sensor devices also requires a defense system to protect against various attacks such as DoS and spoofing attack. As security and privacy of PHR has become a global concern, WBAN applications need to implement guidelines provided by regulatory compliance bodies.

6 Conclusion and Future work

WBAN applications can now provide health care services with real-time monitoring. However, the characteristics of WBAN applications leave them open to a wide attack surface. Ensuring data security and privacy is a key concern and challenging task for WBAN applications. Currently, no solution exists for ensuring such security and privacy. Furthermore, no comprehensive list of WBAN attack types or security requirements is available.

The goal of this research paper was to perform a systematic literature review to present a holistic view of attack types and security requirements related to WBAN applications. This literature review indicates that WBAN applications are vulnerable to 11 attack types with DoS, eavesdropping and replay attack being the most common. Additionally, this literature review indicates that there are 22 security requirements related to WBAN with data confidentiality, integrity, privacy, fine-grained access control, lightweight cryptography algorithms and key management being the most referenced. The least referenced security requirements are physical protection, intrusion detection, client platform security, auditing, regulation and compliance requirements.

Acknowledgement
This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094. Additionally, this work was partly funded by the DEIS H2020 project (Grant Agreement 732242).

References

1. IEEE802.15.6: IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. (2012).
2. Bouazizi, A., Zaibi, G., Samet, M., Kachouri, A.: Wireless body area network for e-health applications: Overview. In: Int. Conf. on SM2C. pp. 17–19 (2017).
3. Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wirel. Commun. 17, 51–58 (2010).
4. Bharathi, K.R.S., Venkateswari, R.: Security Challenges and Solutions for Wireless Body Area Networks. In: Comp., Comm.. and Signal Proc. Springer Singapore (2018).

5. Zou, S., Xu, Y., Wang, H., Li, Z., Chen, S., Hu, B.: A Survey on Secure Wireless Body Area Networks. Secur. Commun. Networks. 2017, (2017).
6. Kompara, M., Hölbl, M.: Survey on security in intra-body area network communication. Ad Hoc Networks. 70, 23–43 (2018).
7. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., Shamshirband, S.: Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt. Informatics J. 18, 113–122 (2017).
8. Sajid, A., Abbas, H.: Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. J. Med. Syst. (2016).
9. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering. Engineering. 45, 1051 (2007).
10. Kotz, D.: A threat taxonomy for mHealth privacy. In: 3rd International Conference on Communication Systems and Networks, COMSNETS (2011).
11. Partala, J., Keraneny, N., Sarestoniemi, M., Hamalainen, M., Iinatti, J., Jamsa, T., Reponen, J., Seppanen, T.: Security threats against the transmission chain of a medical health monitoring system. 15th Int. Conf. e-Health Net., Appl. Serv. 243–248 (2013).
12. Omoogun, M., Seeam, P., Ramsurrun, V., Bellekens, X., Seeam, A.: When eHealth meets the internet of things: Pervasive security and privacy challenges. 2017 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2017. (2017).
13. Dhillon, P.K., Kalra, S.: Multi-factor user authentication scheme for IoT-based healthcare services. J. Reliab. Intell. Environ. (2018).
14. Islam, S.M.R., Kwak, D., Kabir, H., Hossain, M., Kwak, K.-S.: The internet of things for health care: a comprehensive survey. IEEE Access. 3, 678–708 (2015).
15. Dimitriou, T., Ioannis, K.: Security issues in biomedical wireless sensor networks. 2008 First Int. Symp. Appl. Sci. Biomed. Commun. Technol. 1–5 (2008).
16. Wazid, M., Das, A.K., Kumar, N., Conti, M., Vasilakos, A. V.: A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE J. Biomed. Heal. Informatics. 22, 1299–1309 (2017).
17. Prakash, S., Mamta: An overview of healthcare perspective based security issues in wireless sensor networks. In: Comput. for Sust.Global Dev. pp. 870–875 (2016).
18. Saleem, S., Ullah, S., Kwak, K.S.: Towards security issues and solutions in wireless body area networks. 6th Int. Conf. Networked Comput. 1–4 (2010).
19. Mainanwal, V., Gupta, M., Upadhayay, S.K.: A survey on wireless body area network: Security technology and its design methodology issue. 2015 Int. Conf. Innov. Information, Embed. Commun. Syst. 1–5 (2015).
20. Liu, J.: Hybrid security mechanisms for wireless body area networks. In: Second Int.Conf. on Ubiquitous and Future Networks (ICUFN). pp. 98–103 (2010).
21. Al Alkeem, E., Yeun, C.Y., Zemerly, M.J.: Security and privacy framework for ubiquitous healthcare IoT devices. In: 2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015. pp. 70–75 (2016).
22. Zhang, Z., Zhou, H.: A MAC layer protocol supporting the application of WSNs in medicine and healthcare domains. Proc. - 2011 12th ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel Distrib. Comput. SNPD 2011. 33–37 (2011).
23. Rahman, A.F.A., Ahmad, R., Ramli, S.N.: Forensics readiness for Wireless Body Area Network (WBAN) system. Int. Conf. Adv. Comm. Technol. ICACT. 177–180 (2014).

24. Latif, R., Abbas, H., Assar, S.: Distributed Denial of Service (DDoS) Attack in Cloud-Assisted Wireless Body Area Networks : A Systematic Literature Review. J. Med. Syst. (2014).

25. Ragesh, G.K., Baskaran, K.: CRYPE: Towards Cryptographically Enforced and Privacy Enhanced WBANs. In: Proceedings of the First International Conference on Security of Internet of Things. pp. 204–209. ACM, New York, NY, USA (2012).

26. Hosseini-Khayat, S.: A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices. 5th Int. Symp. Med. Inf. Commun. Technol. ISMICT 2011. 6–9 (2011).

27. Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A.: A survey of wearable devices and challenges. IEEE Commun. Surv. Tutorials. 19, 2573–2620 (2017).

28. Alsadhan, A., Khan, N.: An LBP based key management for secure wireless body area network (WBAN). 2013 14th ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. 85–88 (2013).

29. Langone, M., Setola, R., Lopez, J.: Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method. 2017 IEEE 41st Annu. Comput. Softw. Appl. Conf. 304–309 (2017).

30. Thamilarasu, G., Odesile, A.: Securing wireless body area networks: Challenges, review and recommendations. IEEE Int. Conf. Comput. Intell. Comput. Res. 1–7 (2017).

31. Dodangeh, P., Jahangir, A.H.: A biometric security scheme for wireless body area networks. J. Inf. Secur. Appl. 41, 62–74 (2018).

32. Kyaw, A.K., Cusack, B.: Security challenges in pervasive wireless medical systems and devices. 2014 11th Annu. High Capacit. Opt. Networks Emerging/Enabling Technol. (Photonics Energy), HONET-PfE 2014. 178–185 (2014).

33. Antonescu, B., Basagni, S.: Wireless body area networks: challenges, trends and emerging technologies. In: 8th int. conf. on body area networks. pp. 1–7 (2013).

34. Sherali Zeadally, Jesús Téllez Isaac, Z.B.: Security attacks and solutions in electronic health (e-health) systems. J. Med. Syst. (2016).

35. Challa, S., Wazid, M., Das, A.K., Khan, M.K.: Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions. IEEE Consum. Electron. Mag. 7, 57–65 (2018).

36. Jang, C., Lee, D.-G., Han, J.: A proposal of security framework for wireless body area network. In: 2008 Int.Conference on Security Technology. pp. 202–205 (2008).

37. Javadi, S.S., Razzaque, M.A.: Security and privacy in wireless body area networks for health care applications. Wirel. Networks Secur. 26, 165–187 (2013).

38. Ameen, M. Al, Liu, J.: Security and privacy issues in wireless sensor networks for healthcare applications. J. Med. Syst. 93–101 (2012).

39. Ankaralı, Z.E., Abbasi, Q.H., Demir, a F., Serpedin, E., Qaraqe, K., Arslan, H.: A comparative review on the wireless implantable medical devices privacy and security. 4th Int. Conf. Wirel. Mob. Commun. Healthc. 246–249 (2014).

40. Huang, C., Lee, H., Hoon, D.: A privacy-strengthened scheme for E-healthcare monitoring system. J. Med. Syst. 2959–2971 (2012).

41. Razzi, S.M., Lee, H., Lee, S., Lee, Y.K.: BARI: A biometric based distributed key management approach for wireless body area networks. Sensors. 3911–3933 (2009).

42. Miao, F., Jiang, L., Li, Y., Zhang, Y.T.: A novel biometrics based security solution for body sensor networks. 2nd Int. Conf. Biomed. Eng. Informatics, BMEI. (2009).
43. Zhu, Y., Keoh, S.L., Sloman, M., Lupu, E.C.: A lightweight policy system for body sensor networks. IEEE Trans. Netw. Serv. Manag. 6, 137–148 (2009).
44. Amini, S., Verhoeven, R., Lukkien, J., Chen, S.: Toward a security model for a body sensor platform. Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron. 143–144 (2011).
45. Kumar, P., Lee, S.G., Lee, H.J.: A user authentication for healthcare application using wireless medical sensor networks. IEEE Int. Conf. HPCC. 1, 647–652 (2011).
46. Wu, L., Zhang, Y., Li, L., Shen, J.: Efficient and Anonymous Authentication Scheme for Wireless Body Area Networks. (2016).
47. Ullah, S., Alamri, A.: A secure RFID-based WBAN for healthcare applications. J. Med. Syst. (2013).
48. Zhu, Y., Sloman, M., Lupu, E., Loong Keoh, S.: Vesta: A secure and autonomic system for pervasive healthcare. In: 3rd Int. Conf. on Per. Comp. Tech. for Healthcare (2009).
49. Ramli, S.N., Ahmad, R.: Surveying the Wireless Body Area Network in the realm of wireless communication. 7th Int. Conf. Inf. Assur. Secur. IAS 2011. 58–61 (2011).
50. Naik, M.R.K., Samundiswary, P.: Wireless body area network security issues — Survey. Int. Conf. Control. Instr., Commun. Comput. Technol. 190–194 (2016).
51. Sawaneh, I.A., Sankoh, I., Koroma, D.K.: A survey on security issues and wearable sensors in wireless body area network for healthcare system. In: Wavelet Active Media Technology and Information Processing (ICCWAMTIP). pp. 304–308 (2017).
52. He, D., Zeadally, S., Kumar, N., Lee, J.-H.: Anonymous authentication for wireless body area networks with provable security. IEEE Syst. J. 11, 2590–2601 (2017).
53. Cavallari, R., Martelli, F., Rosini, R., Buratti, C., Verdone, R.: A survey on wireless body area networks: Technologies and design challenges. IEEE Commun. Surv. Tutorials. PP, 1–23 (2014).
54. Venkatasubramanian, S., Jothi, V.: Integrated authentication and security check with CDMA modulation technique in physical layer of Wireless Body Area Network. 2012 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2012. (2012).
55. Yin, L., Zhang, A., Ye, X., Wang, L.: Security-aware attribute-based access control for fog-based eldercare system. In: Com. and Commun. (ICCC). pp. 2680–2684 (2017).
56. Li, F., Hong, J.: Efficient certificateless access control for wireless body area networks. IEEE Sens. J. 16, 5389–5396 (2016).
57. Alshamsi, A.Z., Barka, E.S., Serhani, M.A.: Lightweight encryption algorithm in wireless body area network for e-health monitoring. In: 2016 12th International Conference on Innovations in Information Technology (IIT). pp. 1–7 (2016).
58. Sindhu, K. V: Trustworthy access control for wireless body area networks. In: Information Communication and Embedded Systems (ICICES). pp. 1–5 (2017).
59. Fragopoulos, A.G., Gialelis, J., Serpanos, D.: Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures. 12th IEEE Int. Conf. e-Health Networking, Appl. Serv. (2010).
60. Saleem, K., Zeb, K., Derhab, A., Abbas, H., Al-Muhtadi, J., Orgun, M.A., Gawanmeh, A.: Survey on cybersecurity issues in wireless mesh networks based eHealthcare. IEEE 18th Int. Conf. e-Health Networking, Appl. Serv. (2016).
61. Chukwunonyerem, J., Aibinu, A.M., Onwuka, E.N.: Review on security of wireless

body area sensor network. In: 11th International Conference on Electronics, Computer and Computation (ICECCO). pp. 1–10 (2014).

62. Saarika, U., Sharma, P.K., Sharma, D.: A roadmap to the realization of wireless body area networks: a review. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). pp. 439–443 (2016).

63. Ara, A., Al-Rodhaan, M., Tian, Y., Al-Dhelaan, A.: A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems. IEEE Access. 5, 12601–12617 (2017).

64. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: A survey. Comput. Networks. 54, 2688–2710 (2010).

65. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y.: Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J. Netw. Comput. Appl. 106, 117–123 (2018).

66. Ramu, G.: A secure cloud framework to share EHRs using modified CP-ABE and the attribute bloom filter. Educ. Inf. Technol. (2018).

67. Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., Zhou, F.: Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. Futur. Gener. Comput. Syst. (2018).

68. Singel, D.: A secure cross-layer protocol for multi-hop wireless body area networks. In: International Conference on Ad-Hoc Networks and Wireless. pp. 94–107 (2008).

69. Dharshini, S., Subashini, M.M.: An overview on wireless body area networks. In: Power and Advanced Computing Technologies (i-PACT). pp. 1–10 (2017).

70. Masdari, M., Ahmadzadeh, S., Bidaki, M.: Key management in wireless Body Area Network: Challenges and issues. J. Netw. Comput. Appl. 91, 36–51 (2017).