DOI: https://doi.org/10.24113/ijoscience.v5i11.246

A Review on Security and Privacy Issues in Wireless Body Area Networks for Healthcare Applications

Vineeta Shrivastava
M. Tech. Scholar
Department of Computer Science & Engineering
Sagar Institute of Research & Technology(SIRT)
Bhopal, India
shrivastavavinita21@gmail.com

Mayank Namdev
Assistant Professor
Department of Computer Science & Engineering
Sagar Institute of Research & Technology(SIRT)
Bhopal, India
mayank.namdev@gmail.com

***Abstract*-Wireless Body Area Network (WBAN) is a new trend in the technology that provides remote mechanism to monitor and collect patient's health record data using wearable sensors. It is widely recognized that a high level of system security and privacy play a key role in protecting these data when being used by the healthcare professionals and during storage to ensure that patient's records are kept safe from intruder's danger. It is therefore of great interest to discuss security and privacy issues in WBANs. In this paper, we reviewed WBAN communication architecture, security and privacy requirements and security threats and the primary challenges in WBANs to these systems based on the latest standards and publications. This paper also covers the state-of-art security measures and research in WBAN.**

Keywords: **Wireless Body Area Network, Data sharing, Data confidentiality, Security.**

I. INTRODUCTION

A Body Area Network (BAN) is a short-range wireless network comprised of devices positioned in, on, and around the body. It provides data communication over short distances, limited to ranges of just a few meters. Figure 1 below illustrates the basic concept. This new, inherently personal type of network uses wearable and implanted electronic circuits. It implements highly useful functions and capabilities in convenient, unobtrusive configurations that operate at very low power and deliver superlative security [1].

There has been a noticeable increase in the number of computer products used by an individual person, desktop, laptop, tablet, cell phone and an individual often uses more products regularly. Other products are implanted in people to monitor various bodily functions and conditions as well as the surrounding environment [2].

The sensor nodes are placed directly either on the body or under the skin of a person to compute certain body parameters such as, electro cardio gram (ECG), electroencephalogram (EEG), body movement, temperature, blood pressure, blood glucose, Plasmon Biosensor, heart rate, respiration rate levels [3]. These sensors are designed for specific purposes to meet the requirements of enduses. For example, an EEG sensor was intended to monitor brain electrical activity. Another example is the ECG sensor which was designed for monitoring heart activities.

The IEEE 802.15.6 has suggested taxonomy for WBAN nodes according to the way they are implemented within the body and their role in the network [4].

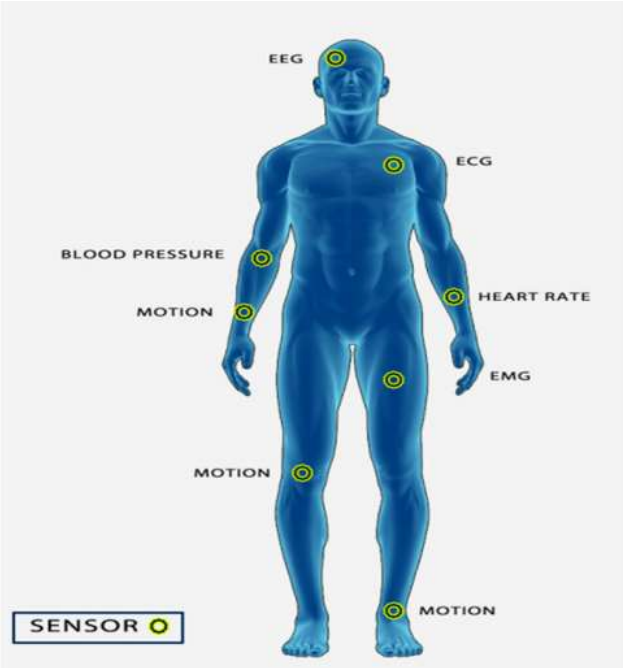

Figure 1: WBAN sensors

The node can be classified based on the way they are implemented into the following:

- Implant Node: This type of node is planted either underneath the skin or inside the body tissue.
- Body Surface Node: It is either placed on the surface or 2 cm away from the human body.
- External Node: It is not in contact with the human body and rather a few centimeters to 5 m away from the human body. There are three types of nodes in WBANs according to their role in the network Coordinator: This node acts as a gateway to the outside world, another WBAN, a trust center or an access coordinator. The PDA is the coordinator of a WBAN in which all other nodes can communicate.
- End Nodes: This type of nodes is restricted to perform their entrenched application but they do not have the capability to transmit messages to other nodes. Relay: These nodes represent intermediate nodes and they are called relays. The relay node consists of a parent and child nodes and relay messages. If a node is at a foot, then it is required for any data sent to be relayed by other nodes before reaching to the PDA. Also these types of nodes can sense data from other nodes.

Fig. 1 typically shows the placement of sensors that communicate by the means of a WBAN [5]. It can be further employed in several other fields and applications such as monitoring pollution levels, physiological and medical monitoring, human computer interaction, education and entertainment [6].

A smart phone can remotely access the information sensed by the sensors or a Personal Digital Assistant (PDA) between the patient and a doctor, nurses, pharmacies who take sensitive decisions or actions depending on the information acquired from those sensors [7]. These critical decisions and medical information must be protected against unauthorized access that could be dangerous to the life of the patient and sometimes lead to death [8], i.e. change of dosage of drugs or treatment procedures, if falls on the wrong hand [9].

Thus, scalable and strict security mechanisms are mandatory and should include secure group management, confidentiality, privacy, integrity, authorization and authentication. A wireless healthcare application offers and brings many benefits and challenges to healthcare sector. These benefits provide a convenient-environment that can monitor the daily lives and medical situations of patients at anytime, anywhere and without limitations [10,11].

On the other hand, one of the most important challenges to these new technologies in healthcare is the security and privacy issues that often makes a patient's privacy more vulnerable [12,13]. The patient's physiological vital signs are very sensitive, especially if a patient is suffering from an embarrassing disease. Such a patient could suffer humiliation at the least or even psychological upset if his or her disease information or low Quality of Service (QoS) were inadvertently communicated.

Also in some instances, disease information could result to a person losing their job. Sometimes the information may make it impossible for the patient to get insurance protection. Medical sensors sense the patient's body conditions and send messages to the doctor or the hospital server while sending of these messages, the sensors may be attacked. For instance, an adversary may capture the data from the wireless channels and modify the results [14,15].

He/She may later pass the attacked data to the doctor or the server. This could imperil the life of the patients. Given the vulnerability of patient privacy, security should be paramount when considering using technology in the healthcare setting [16].

Any patient's vital information should be stored, used and considered sensitive, but it can be especially so for patients with a socially unaccepted disease. Any failure of this type of patient's health information could lead to humiliation, wrong treatments, relationship issues, or even job loss [14,15].

Health information perceived as negative can also hinder an individual's ability to obtain health insurance coverage. Due to this, it is important to make sure that the security and privacy of these data are kept and sent securely.

II. WBAN COMMUNICATION ARCHITECTURE

In order to understand the type of security mechanism to be deployed in a WBAN, we first need to know the structure of the communication within each of these networks as well as their communication to the outside world and with other coexisting WBANs. Therefore, in this section we provide an overview into the communication architecture in WBANs. Fig. 2 depicts that the devices are spread throughout in a network, with the location of the device being tied to a certain application [17]. As the body continuously changes the position so the location of sensors is not fixed. Hence, WBANs, therefore, cannot be classified as a fixed network [3].

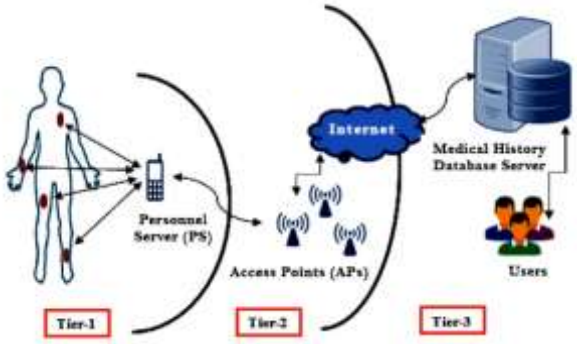

Figure 2: Communication Tiers in Wireless Body Area Network

In most of the WBANs system, the communication design comprised into three separate levels as follows:

A. Tier-1

Intra-WBAN communication: In this level, the interaction of the sensors is confined around the body of the patient. The communication signals within the region use a Personnel Server (PS) that acts as a gateway, to transfer the information to the next level (i.e. access point that is present in Tier 2).

B. Tier-2

Inter-WBAN communication: This level bridge the gap between the PS and the user via access points (APs) that are considered an important part of the network and may be positioned in a way that can allow for emergencies cases. Essentially, communication at this level strives to connect. WBANs with other systems or networks so that information can be easily be retrieved through various mediums, such as the internet [14,15].

The model of inter-WBAN communication is divided into two subgroups as follows:

- Infrastructure based architecture is used in most WBAN applications as shown in Fig. 3. These applications allow for active utilization, even in a restricted space. This type of architecture also provides better control over security and more central management since the AP can perform much like a database server relative to the application [6].

Figure 3: Infrastructure-based Mode Communication

- Ad-hoc based architecture – Fig. 4 illustrates the ability for many APs to relay information in this architecture by forming a lattice that permits more flexible and quick disposition. In this way, more radio coverage can be provided through expansion and non-linear dissemination to more fully support movement. When compared to the infrastructure based coverage, the configuration of the Ad-hoc based architecture is much larger and supports the movement through larger spaces. This type of interconnection extends the coverage area from 2 to 100 m, enabling not only short, but also long term situations [6].

Figure 4: Ad-Hoc based mode communication

C. Tier-3

Beyond-WBAN Communication: This level of communication is ideal for metropolitan areas, as ‘‘gateway.” For example, a Smartphone can become a bridge from Tier 2 and Tier 3. ‘‘Or, from the Internet to the Medical Server (MS) in a specific application” [9]. A medical environment database is an especially crucial part of Tier 3 communication, since it accommodates the medical history and specific profile of the user. This means that the design would necessarily need to be specific to an application; medical providers and/or patients can be alerted to an emergency situation via the Internet or a through Short Message Service (SMS). Tier-3 also allows for the restoration of important patient information that can be crucial to plan for appropriate treatment [14,15]. The PS in Tier-1 could also use GPRS/3G/4G that will directly connect it to tier 3

network, without the need of an AP, depending upon the application.

III. LITERATURE REVIEW

Jiang et al. [1] presented an optimal key agreement scheme based on heartbeat, to ensure secure communication between legitimate devices. The proposed key agreement scheme employs fuzzy commitment with low latency in feature extraction. Moreover, the physiological-distribution-based parameter optimization (PDPO) algorithm is proposed to adaptively determine the optimal protocol parameters for individuals which not only ensures outstanding and stable performance but also guarantee the security of the scheme. Finally, we prototype our protocol and conduct experiments with multiple subjects to evaluate its security and performance. Our results demonstrate that the proposed protocol negotiates the key securely and quickly, has low energy overhead, and is suitable for practical applications.

Ivanciu et al. [2] proposed an original solution for securing the transmission of data gathered by sensors in a Wireless Body Area Network using the Electrocardiogram signal and Named Data Networks. Our contribution is two-fold: first of all, we make use of the inherent features of such networks to securely transmit sensitive, health-related data (of a regular patient or a driver) to the cloud and then disseminate it to interested parties such as physicians. Second, our approach exploits the properties of the Electrocardiogram signal (robustness to attacks, universality and liveness detection) to encrypt this data and provide a simple and fast authentication mechanism between the devices in the Wireless Body Area Network.

Kim et al. [3] proposed a secure and lightweight mutual authentication and key establishment scheme using wearable devices to resolve the security shortcomings of Gupta et al.'s scheme. The proposed scheme can be suitable to resource-limited environments.

Jiang et al. [4] proposed a distributed deep learning optimized system which contains a cloud server and multiple smartphone devices with computation capabilities and each device is served as a personal mobile data hub for enabling mobile computing while preserving data privacy. The proposed system keeps the private data locally in smartphones, shares trained parameters and builds a global consensus model. The feasibility and usability of the proposed system are evaluated by three experiments and related discussion. The experimental results show that the proposed distributed deep learning system can reconstruct the behavior of centralized training. We also measure the cumulative network traffic in different scenarios and show that the partial parameter sharing strategy does not only preserve the performance of the trained model but also can reduce network traffic.

Pandey et al. [5] presented a state-of-art survey about various features of BAN specifically communications, sensors, applications, requirements, standards & protocol, and security aspects.

Meng et al. [6] proposed a new anonymous mutual authentication and key agreement scheme, with untraceability and session key forward secrecy. The scheme uses as few hash functions and XOR operations as possible for authentication and key agreement. It is officially proven to be correct through BAN logic, and its security has been verified by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) as well.

Nezhad et al. [7] proposed an approach for faulty measurements detection in order to make alarming of emergency situations more precisely. The proposed approach is based on decision tree, threshold biasing and linear regression. Our objective is to detect single and multiple faults in order to reduce unnecessary healthcare intervention. The proposed approach has been applied to real healthcare dataset. Experimental results demonstrate the effectiveness of the proposed approach in achieving high Detection Rate and low False Positive Rate. The ability of this algorithm to detect single and multiple anomalies make it more reliable for medical emergency use.

Shim et al. [8] showed that L-OOCLS is entirely broken: anyone can forge certificateless signatures on any messages for any identities from only publicly known information. Thus, the scheme is trivially insecure against the type I adversary who can replace user public keys and the type II adversary who knows the master secret key. Our result shows that their security proofs are also flawed.

Shanthapriya.R et al. [9] ECG-Based Secure Healthcare Monitoring System in Body Area Networks. Polynomial based curve is generated and steganography technique has been used for secure health monitoring which provides data confidentiality and authentication to maintain the privacy of a patient.

Haipeng Peng et al. [10] In this paper, chaotic compressive sensing (CCS) is proposed which uses two encryption mechanisms, confusion and mask, and performs a much better encryption quality.

An intruder can access patient's medical data which is stored in the controller or hack the data when it is transmitted by means of wireless communication, without getting approval from the patients. Intruder can alter the messages (such as time, arrangement, content, request and so on) created inside the BAN before they are carried to a

receiver or - modify the message substance being transmitted from BAN to external entity (e.g., doctor). A third-party A (as an attacker), who is unrelated to this system may try to hamper in the authentication procedure by mounting various attacks. A valid user A (as an attacker), who is a part of the system may try to obtain confidential information of the server so that A can inject several attacks on the authentication system.

To solve the mentioned problems in previous schemes, an algorithm is proposed for secure authentication system for WBAN/IOT.

- A secure authentication and key agreement scheme for cloud-assisted WBAN/IOT system is proposed. Therefore, only authorized users have ability to access information and the proposed system can ensure user's privacy and data integrity.
- From the execution of the proposed procedures, the system reduces the burden on some computations and is suitable for implementation in the current mobile environment.
-

IV. BAN APPLICATIONS

A. User authentication for notebook computers

To protect property and privacy, a BAN can be used to authenticate the user of a notebook computer. The operator wears a " smart watch" a small device with a built-in BAN function. When the user touches the computer's touchpad, a controller embedded in the touchpad picks up the ID data and verifies the requisite access-control information, enabling login.

B. Room entry control

No key or pass code is needed to enter a controlled access area if the person is wearing a BAN communication device. When their hand is placed near the doorknob or touches it, the BAN transmits the individual's ID information to a network bridge connected to the knob. From there that data goes to the access controller and authentication server, where authentication is completed. The system then releases the door lock, allowing the properly authorized individual to enter the room.

C. Fitness monitoring

Health and safety are increased when a Body Area Network serves as a pulse monitor during exercise workouts. A sensor near the skin tracks the person's pulse and transmits the data to the smart watch worn on a wrist. The user can check the pulse rate in real time by viewing the watch display.

V. SECURITY ISSUES IN WBAN

The major security and privacy requirements to ensure the safety of a WBAN system and its extensive acceptance by its users are outlined as follows:

A. Data Confidentiality

Data confidentiality denotes the protection of a confidential data from exposure that is considered as the vital issue in a WBAN. Since WBAN nodes applied in medical situations are expected and relied upon to transmit delicate and private information about the status of a patient's well-being, hence their data must be protected from unauthorized access that could be hazardous to the patient's life. This important, transported data can be ''overheard" during transmission that can either damage the patient, the provider, or the system itself. Encryption can provide better confidentiality for this sensitive data by providing a shared key on a secured communication channel between secured WBAN nodes and their coordinators [2].

B. Data Integrity

Data integrity refers to the measures taken to protect the content of a message, its accuracy and consistency. It applies to both single messages as well as streams of messages [14,15]. However, data confidentiality does not protect data from external modifications, as information can be illicitly changed when data is transmitted to an insecure WBAN as an adversary that can easily moderate the patient's information before reaching to the network coordinator.

More specifically, modifications can be simply made by integrating some fragments, manipulating data within a packet, and then forwarding the packet to the PS. This interception and modification can lead to serious health concerns and even death in extreme cases. Consequently, it is imperative that the information not be accessible and altered by a potential adversary by applying authentication protocols [3].

C. Data Freshness

Data freshness techniques can effectively make certain that the integrity and confidentiality of data are protected from recording and replaying older data by an adversary and confuse the WBAN coordinator. It ensures that old data is not recycled and that its frames are correct. There are two types of data freshness are currently in use: Strong freshness promises delay in addition to frame ordering; and weak freshness which is limited to frame ordering, but does not provides any delay guarantees. Strong freshness is required for synchronization when a beacon is being conveyed to the WBAN coordinator and weak freshness is used for WBAN nodes with a low-duty cycle [14].

D. Availability of the network

It insinuates a medical practitioner with efficient access to a patient's information. Since such a system carries important, highly sensitive and potentially lifesaving information, it is paramount that the network is available at all the times for patients' usage in case of an emergency [4,5,8]. For this, it is essential to switch the operations to another WBAN in case of availability loss occurs.

E. Data Authentication

Medical and non-medical applications may require data authentication. Thus, nodes within a WBAN must be capable to verify that the information is sent from a known trust centre and not an imposter. Therefore, the network and coordinator-nodes for all data calculate Message Authentication Code (MAC) by sharing an undisclosed key. Accurate calculation of a MAC code, assures the network coordinator that the message is being conducted by a trustworthy node [12].

F. Secure Management

To deliver key distribution to a WBAN, the decryption and encryption operation requires secure control by the coordinator. The coordinator role is to add and remove WBAN nodes in a secure way during node association and disassociation [4].

G. Secure Localization

Most WBAN applications need correct estimation of the patient's location. Lack of tracking methods could let an attacker to transmit improper details such as, by replying with a fake signal about the patient's location [9].

H. Accountability

In the medical field, it is necessary for healthcare providers to safe guard patient health information. If a provider does not secure this information, or worse, abuses his or her responsibility for it then he or she should be made accountable for this to discourage additional abuses [3,6].

I. Flexibility

The patient needs to have the flexibility of designating AP control of medical data within a WBAN. For instance, in the case of an emergency, authorization to interpret patient's data could be given on demand to a different physician who is not necessarily listed as having permission [13].

VI. PROPOSED SYSTEM

For secure cloud-assisted IOT application, three roles participate in this system: the user (U), the cloud-service center (CSC) and the Authenticator (A). Before accessing the system, every participant must register with the CSC and it will issue one specific certificate to access data files in WBAN/IOT.

- Step 1. The user U goes to the Authenticator to take authentication permission to access or upload a file.
- Step 2. The user uploads his/her biometric information in encrypted form to the Authenticator (A) and A will authenticate previously registered user. If not registered then make a registration and store information.
- Step 3. A authenticate user and redirect user U to CSC.
- Step 4. The user U can either upload a new file or access existing files. For accessing other file he has to provide some accessing parameters and accessing license will be provided to the user for a specific time limit.
- Step 5. The authorized user U can access files stored in cloud centre.

VII. CONCLUSION

The Wireless Body Area Network is a rising and future promising innovation that will change individuals' healthcare revolutionarily. Information security and protection in WBANs and WBAN-related e-healthcare frameworks is a huge zone, and there still remain various extensive issues and challenges which is difficult to overcome. This work reviewed the deployment of WBANs in terms of security and privacy. It has also dealt with WBAN communication architecture, the security and privacy in WBAN and the threats to the integration of sensors and actuators as well as attacks to WBANs. This implies that the framework provides for the other substantive safety measures such as trust, audit, digital forensics and IDPS to guarantee compliance within the law and ethical behaviour by healthcare workers and system operators who have the access to patient records and information. These implications require the public and health care personnel to be aware of the challenges that come along with WBAN usage to ensure that the application in delivering patient's healthcare is secured at all levels.

REFERENCES

[1] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen and D. Wu, "Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network," in *IEEE Transactions on Emerging Topics in Computing*.

[2] I. Ivanciu, L. Ivanciu, D. Zinca and V. Dobrota, "Securing Health-Related Data Transmission Using ECG and Named Data Networks," *2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, Paris, France, 2019, pp. 1-6.

[3] M. Kim, J. Lee, S. Yu, K. Park, Y. Park and Y. Park, "A Secure Authentication and Key Establishment Scheme for Wearable Devices," *2019 28th International Conference on Computer Communication and Networks (ICCCN)*, Valencia, Spain, 2019, pp. 1-2.

[4] H. Jiang, J. Starkman, Y. Lee, H. Chen, X. Qian and M. Huang, "Distributed Deep Learning Optimized System over the Cloud and

Smart Phone Devices," in *IEEE Transactions on Mobile Computing*.

[5] I. Pandey, H. S. Dutta and J. Sekhar Banerjee, "WBAN: A Smart Approach to Next Generation e-healthcare System," *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2019, pp. 344-349.

[6] X. Meng, J. Xu, W. Liang and K. Li, "An Anonymous Mutual Authentication and Key Agreement Scheme in WBAN," *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Washington, DC, USA, 2019, pp. 31-36.

[7] M. M. Nezhad and M. Eshghi, "Sensor Single and Multiple Anomaly Detection in Wireless Sensor Networks for Healthcare," *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, Yazd, Iran, 2019, pp. 1751-1755.

[8] K. Shim, "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211-9212, Oct. 2019.

[9] Shanthapriya.R, Vaithianathan.V, “ECG-Based Secure Healthcare Monitoring System in Body Area Networks”, International Conference on Biosignals, Images and Instrumentation (ICBSII), 2018.

[10] Haipeng Peng ; Ye Tian, Jürgen Kurths, Lixiang Li, Yixian Yang, Daoshun Wang, “Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks”, IEEE Transactions on Biomedical Circuits and Systems, Volume: 11 , Issue: 3 , June 2017, pp. 558-573.

[11] Rocker C, Ziefle M. E-health, assistive technologies and applications for assisted living: challenges and solutions. Med Inform Sci Ref 2011;392. ISBN13: 9781609604691.

[12] Rehman OU, Javaid N, Bibi A, Khan ZA. Performance study of localization techniques in wireless body area sensor networks. In: 11th IEEE international conference on trust, security and privacy in computing and communications. p. 1968–75.

[13] Pathania S, Bilandi N. Security issues in wireless body area network. Int J Comput Sci Mobile Comput 2014;3(4):1171–8.

[14] Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wirel Commun 2010;17(1):51–8.

[15] Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 2012;36(1):93–101.