Wireless Body Area Network: An Application of IoT and Its Issues—A Review

Chasiya Krutika[1] Prof. Deepak Upadhyay[2]
[1,2]Department of Cyber Security
[1,2]GTU-School of Engineering and Technology, Ahmedabad, India

Abstract— As a key application of IoT, wireless body area networks (WBANs) provides people good quality of life and high level of medical service. To monitor the functions of physical body and their surroundings Wireless Body Area Network (WBAN) is employed, which are supported low powered and lightweight weight wireless sensors devices. WBAN highly supports numerous applications like remote patient monitoring, E-health care systems. The collected data of WBAN contains important privacy of patients, but these data may be easily obtained by an adversary due to the weakness of the open wireless channels, this imposes the attacks in WBAN networks and devices.

Keywords: IoT (Internet of Things), Wireless Body Area Network (WBAN), security

I. INTRODUCTION

Internet of Things (IoT) is defined as a network with everything which will hook up with the web. IoT technologies are often applied in several fields, like agriculture, healthcare, manufacturing, energy, retailing and transportation. IoT has been changing the planet, the way we live and corporations do business. IoT has no uniform architecture and there are different sorts of attacks on the various layers of IoT. Internet of Things (IoT) defined as "a global infrastructure for the knowledge society, enabling advanced services by interconnecting (physical and virtual) things supported existing and evolving interoperable information and communication technologies" [7] .Some samples of existing IoT systems are self-driving vehicles (SDV) for automated vehicular systems, microgrids for distributed energy resources systems, and Smart City Drones for surveillance systems. The IoT architecture is based on a 3-tier/layer system which consists of a perception/hardware layer, a network/communication layer, and a layer of interfaces/services.

Referring to the IoT security architecture, IoT security issues are pertinent in the least three IoT layers. A very popular vector for gaining access to IoT devices arises due to inadequate authentication and authorization procedures. In the current IoT systems, the protocols that support authentication are MQTT, DDS, Zigbee and Z wave. Even if the developer has provided the authentication tools required for IoT communications, pairing and messaging, there are still opportunities for the communication to be hijacked. Furthermore, insecure network services may cause the bad actor or the threat to explore the network and propagate through it. Currently, authentication is that the hottest security method to realize secure communication within the network layer.

II. WBAN (WIRELESS BODY AREA NETWORK):

Wireless body area networks (WBANs) is a key application of IoT, which provides people good quality of life and high level of medical service. To monitor the functions of physical body and their surroundings Wireless Body Area Network (WBAN) is employed, which are supported low powered and lightweight weight wireless sensors devices. WBAN is a part of IoT technology which is one type of Wireless sensor Network (WSN). WBAN contains one or more Body Sensor Units (BSU), one Body Central Unit (BCU), and long-range wireless devices. BAN also called body sensor network (BSN) established to form health and medical applications more advanced. WBAN isn't only restricted to medical applications but it also can be used as non-medical applications like Consumer Electronics (CE), personal entertainment and other.

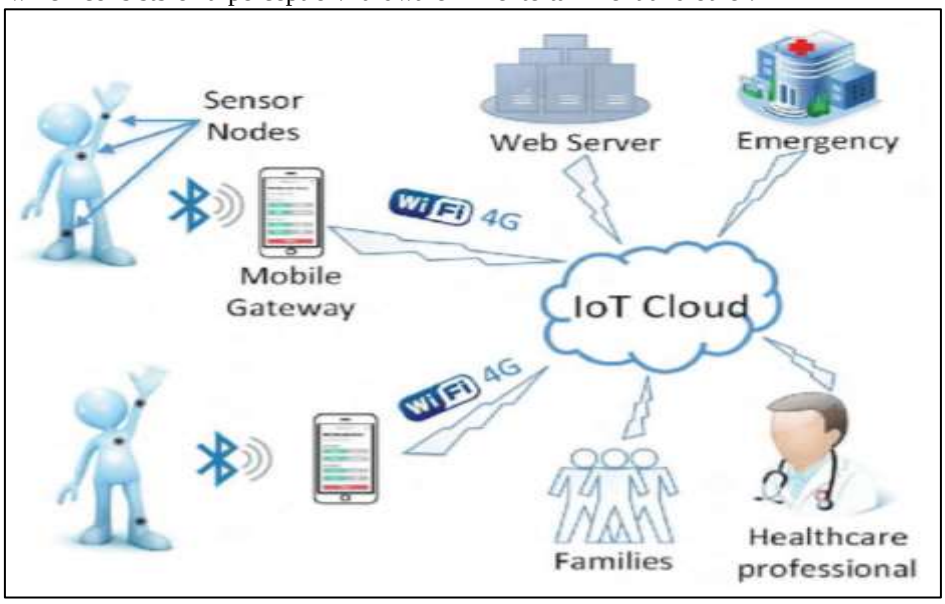

Fig. 1: Application of Wireless Body area network for healthcare

For medical applications it plays a key role to assist medical professionals and patients for the monitoring of medical situation through intelligent body sensor networks (IBAN). The WBAN consists of a group of small autonomous sensor node of different types that are wore by person or may be implanted on the patient's body in order to measure the varied physiological activities (like ECG, EEG, EMG) and record them continuously for medical observation. The sensed data recorded by the sensors is shipped to the hospital community cloud for diagnosis purpose where the clinicians (doctors) monitor the patients remotely. The physiological sensor is electrical equipment that's capable of sensing the varied physiological conditions. The most commonly used physiological sensors are: 1. Electrocardiography (ECG): monitors heart functioning. 2. Electromyography (EMG): monitors muscle functioning. 3. Electroencephalography (EEG): monitors brain functioning. There also are other sorts of sensors like vital sign, tilt, movement, breathing, temperature. There must be only authorized users who can have access to patient related data; otherwise it can be exploited by anyone. The collected data of WBAN contains important privacy of patients, but these data may be easily obtained by an adversary due to the weakness of the open wireless channels, this imposes the security threats in IoT networks and devices.

A. General Architecture of WBAN (Wireless Body Area Network):

WBANs are used by the medical professionals as well as by the patients. Every device in WBAN is independent to each other, and WBAN can be connected to the internet for transmitting data.

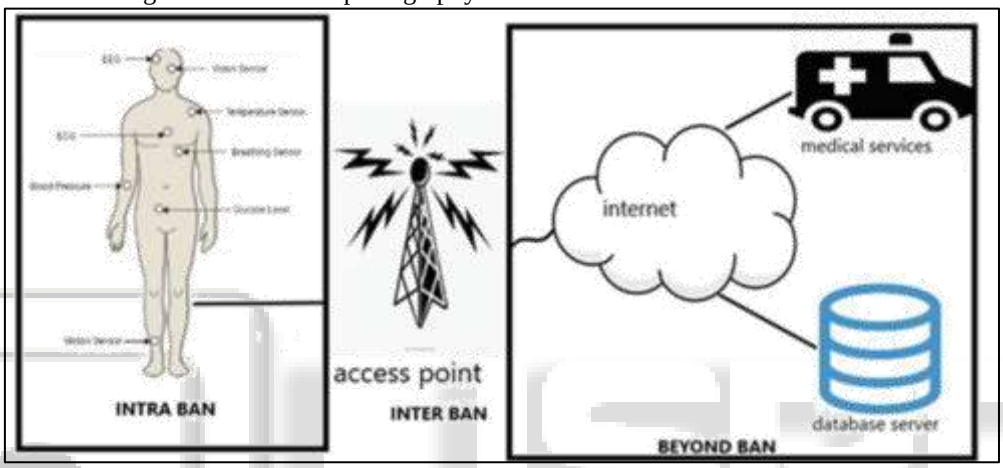

Fig. 2: Three-Tier Architecture of Wireless Body area network

1) Tier-1: Intra-WBAN Communication

TheTier-1consists of different sensors around the body of a patient [3]. For example, an ECG sensor monitors heart activity, an EMG sensor monitors muscle activity, an EEG sensor are often used for brain electrical activity monitoring, while the motion sensors can be used to estimate the patient's movements [4]. Communication in this tier confines within 2m around the body approximately.

2) Tier-2: Inter-WBAN Communication

This works because the gateway between Tier-1 and Tier-3. Personal computer, smart/cell (non-featured) phone, or personal digital assistant (PDA) devices can function as the medium that contains a personal server by which data can be transferred to the Internet [5].

3) Tier-3: Beyond-WBAN Communication

Data at Tier-3 is used for the analysis purpose. After analysis, medical practitioners like doctors or nurse can suggest necessary actions or suggestions. These data can be used for different purposes like short message service (SMS), e-mail, condition monitoring, etc. Responsibility of the medical server is to keep electronic medical records (EMR), authenticate different users, update health record database, and observe health inconsistency for emergency need [6]. This is beneficial for monitoring of elderly patients.

B. Communication Standard of WBAN (Wireless Body Area Network):

Communication standard which are used in WBAN and their features and drawbacks are described in Table 1.

Sr no.	Name	Features	Drawbacks
1.	Bluetooth	Many Devices are allow to get connection	Data rate is 3 Mbps (maximum)
2.	Bluetooth low energy	power consumption is less in duty cycle operation	Interference is 2.4 GHz ISM band
3	ZigBee	Low Data rate, long battery life and secure networking	Batteries need to be replaced
4	IEEE 802.15.4	It used for defining the physical, medium access control layers	Create difficulties in implementation in hospitals or clinics (for multiple patients)
5	IEEE 802.15.6	Frequency bands for data transmission is used	Not possible to meet the constraints of high-quality audio/video transmissions

Table 1: Communication standard of Wireless Body area network

III. Security Issues in WBAN

The WBAN attacks are mainly in two Categories:

- Active attacks
- Passive attacks

A. Active Attack

Active attacks attempt to modify the data stream and re-inject it into the network without changing the nature of communication.

1) Monitoring on Patient

Sometimes, attacker may get the text or messages during transmission. Then attacker can change information containing in the message. This may create some problems both for patient and hospital. Physical harm is also an option of the attacker after obtaining the address.

2) Location Threats

Sensors in case of WBAN support user mobility, and these sensors are generally based on the signal strength and radio frequency so that Patient can change his/her location.

B. Passive Attack

Passive attacks are intended to obtain health-information via techniques such as eavesdropping and/or monitoring the data that are transmitted across WBAN.

1) Threats During Transmission

The interception attack occurs when a 3rd party intercepts the message while it is in transmission. The modification attack is when after obtaining the message, the attacker intentionally changes some information within the message and forwards the altered message to the intended recipient. The recipient, for example, doctor or nurse, might suggest some medications counting on these modified data that may create problems for patients.

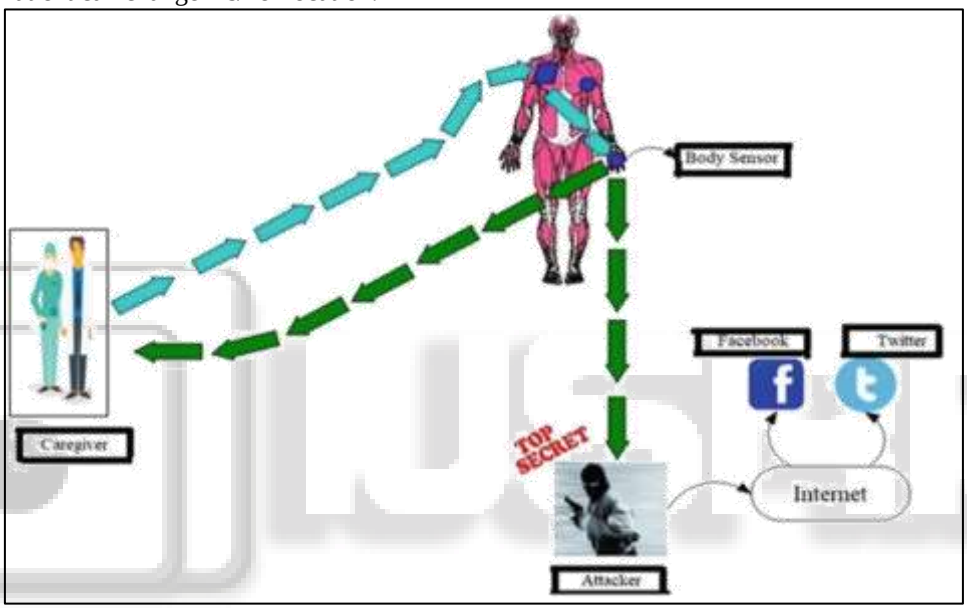

Fig. 3: Attacks during transmission in Wireless Body area network [7]

As shown in Figure.3, while transmission of data from sensors to remote location, an attacker can also track the same data and use these raw data for some wrong purpose like posting or sharing data on to social networking sites.

IV. DRAWBACKS OF WBAN

A. Data privacy and security issues

Generated data in any network shouldn't be interleaved with others collected data there in network and for that reason confidentiality, credibility, affirmation, and integrity should be maintained. Security providence is one among the toughest challenges in any network, and in medical field because it contains persons health-related data, it becomes more important to guard medical information. Leakage within the network may provide attacker some information about patient which when gets disclose, the patient may face humiliation or it'd cause him/her Mediclaim issue.

B. Inconsistency

Generated/collected data must be validated before medical practitioners can give suggestions. In, today's world, a large volume of data is created. Storing and maintaining of these large amounts of data are a very crucial task [8]

C. Storing multiple data at a onetime

System get confused when large amount of data enters at once. Multiple access at a time which causes delay, and bit error rate

D. Network lagging

ZigBee [9], Bluetooth [10] standards generally governs the data transmission. Network should also be expandable. Latency generates from the distance of data centers from their end locations.

V. CONCLUSION

In this paper, a network called as WBAN which is application of the IoT Technology being studied for which remote patient monitoring can be used. The drawbacks of a WBAN structure have also been discussed in this paper. This type of a wireless body area network structure is very useful in medical fields as it may cause some reduction in human errors and reduction of healthcare cost.

REFERENCES

[1] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer Networks 148 (2019): 283-294.
[2] Khan, Fozia Hanif, et al. "A Secure Crypto Base Authentication and Communication Suite in Wireless Body Area Network (WBAN) for IoT Applications." Wireless Personal Communications 103.4 (2018): 2877-2890
[3] Zimmerman, T.G.: Personal area networks: near-field intrabody communication. IBM Syst. J. 35(34), 609–617 (1996)
[4] Jovanov, E., Milenkovic, A., Otto, C., De Groen, P.C.: A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. J. NeuroEng. Rehabil. 2 (2005)
Latré, B., Braem, B., Moerman, I., Blondia, C., Demeester, P.: A survey on wireless body area networks. Wirel. Netw. 17, 1–18 (2011)
[5] Negra,R.,Jemili,I.,Belghith,A.:Wireless body area networks :applications and technologies. Proc. Comput. Sci. 83, 1274–1281 (Elsevier, 2016)
[6] Singh, Ritika, et al. "Wireless Body Area Network: An Application of IoT and Its Issuses—A Survey." Computational Intelligence in Pattern Recognition. Springer, Singapore, 2020. 285-293
[7] Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wirel. Commun. 17, 51–58 (2010)
[8] Z. Specification: ZigBee Document 053474r20, ZigBee Stand. Organ. (2012)
[9] Bluetooth: https://www.bluetooth.com/
[10] https://books.google.co.in/books?id=ouiYDwAAQBAJ&lpg=PP1&ots=vYTzzSj84x&dq=wban%20implementation%20research%20paper&lr&pg=PA8#v=onepage&q=wban%20implementation%20research%20paper&f=false

