Wireless Body Area Network Security and Privacy Issue in E-Healthcare

Muhammad Sheraz Arshad Malik, Muhammad Ahmed, Tahir Abdullah, Naila Kousar, Mehak Nigar Shumaila
Department of Information Technology
Government College University
Faisalabad, Pakistan

Muhammad Awais
Department of Software Engineering
Government College University
Faisalabad, Pakistan

***Abstract*—Wireless Body Area Network (WBAN) is a collection of wireless sensor nodes which can be placed within the body or outside the body of a human or a living person which in result observes or monitors the functionality and adjoining situations of the body. Utilizing a Wireless Body Area Network, the patient encounters a greater physical versatility and is never again constrained to remain in the hospital. As the Wireless Body Area Network sensor devices is being utilized for gathering the sensitive data and possibly will run into antagonistic situations, they require complicated and very secure security medium or structure to avoid the vitriolic communications within the system. These devices represent various security and privacy protection of touchy and private patient medical data. The medical records of patients are a significant and an unsolved situation due to which a changing or exploitation to the system is possible. In this research paper, we first present an overview of WBAN, how they utilized for healthcare monitoring, its architecture then highlight major security and privacy requirements and assaults at different network layer in a WBAN and we finally talk about various cryptographic algorithms and laws for providing solution of security and privacy in WBAN.**

***Keywords*—E-Health; privacy; security; wireless body area networks**

I. Introduction

Recent improvement in wireless technologies and ICT (information and communication technology) frameworks are empowering the health care segment to effectively and efficiently control and provide a variety of solution and health services. Progressed frameworks of ICT will have the capacity to convey medicinal services administrations to patients in healing facilities and therapeutic focuses, as well as in their homes and working environments, along these lines offering cost reserve funds and upgrading the individual fulfillment of patients. E-Health administrations can make use of WBAN, which can go about as an empowering innovation, and gaining its popularity day by day due to its benefits. As by using WBAN patient don't need to visit hospital daily, they stay in home, save its time, and data related to patient is examined by doctor any time at any place.

A WBAN make use of litter sensor and display medical related information on screens by means of WIFI transmission. Sensors are set inside or outside one's body.

Sensors are used to collect sensitive and important medical related information of a patient or it can also be used in sports. WBANs communicate with the net and other technologies such as ZigBee technology, WSNs, WI-FI, Bluetooth, cell systems and Wireless Personal Area Network (WPAN) technology. Sensor collect patient related data, transfer it to cloud using different technology, this data or information is used by doctor, etc.

A wireless body area network has generally two types of nodes i.e. wearable and implantable nodes which work at different frequencies. An implantable node is well on the way to work at 400 MHz utilizing the MICS (Medical Implantable Communication Service) band, while the wearable hub/ node could work in ISM/UWB (Instrumentation Scientific Medical/Ultra Wide Band) or some other specific groups [2], [3].

The paper is sorted out into five Sections. Section I give overview of what is being introduced in the paper. Section II introduces a WBAN architecture. Section III presents the related work done by different researchers which provide solution of security and privacy issues. Section IV presents the WBAN security Requirements and conceivable assaults which occur when utilizing Wireless body area network in E-Health. Section V represents biometric solution for securing Wireless Body Area Network. The last section finishes up our work.

II. General Architecture

A. 3 Tier Architecture

This area gives a general layout of WBAN plan as shown in Fig. 1. WBANs are a vital piece of a multi-level telemedicine framework [4]. Tier 1 incorporates various wireless medical sensor nodes. A WBAN screens physiological signs from these little sensors node with remote transmission capacity set either inside or around a man's body, which are utilized to gather vital wellbeing information of a man amid a specific movement medicinal or game or training related activities. Every sensor node can recognize and test as well as process at least one physiological signs. For instance, heart rate can be checked by an electrocardiogram sensor (ECG), Oxygen saturation sensor (SpO2) used to quantify the level of oxygen, and blood pressure is observed by blood pressure. Tier 2 incorporates the personal server (PS)

application running on a client PDA or iPod or some other convenient gadgets telephone which goes about as a sink for information of the remote devices [1], [2], [4] and at that point exchange those data to an appropriate PC when a correspondence interface is accessible. Tier 3 contains various remote base-stations that keep patient's therapeutic/non-medicinal records and gives huge (indicative) recommendation.

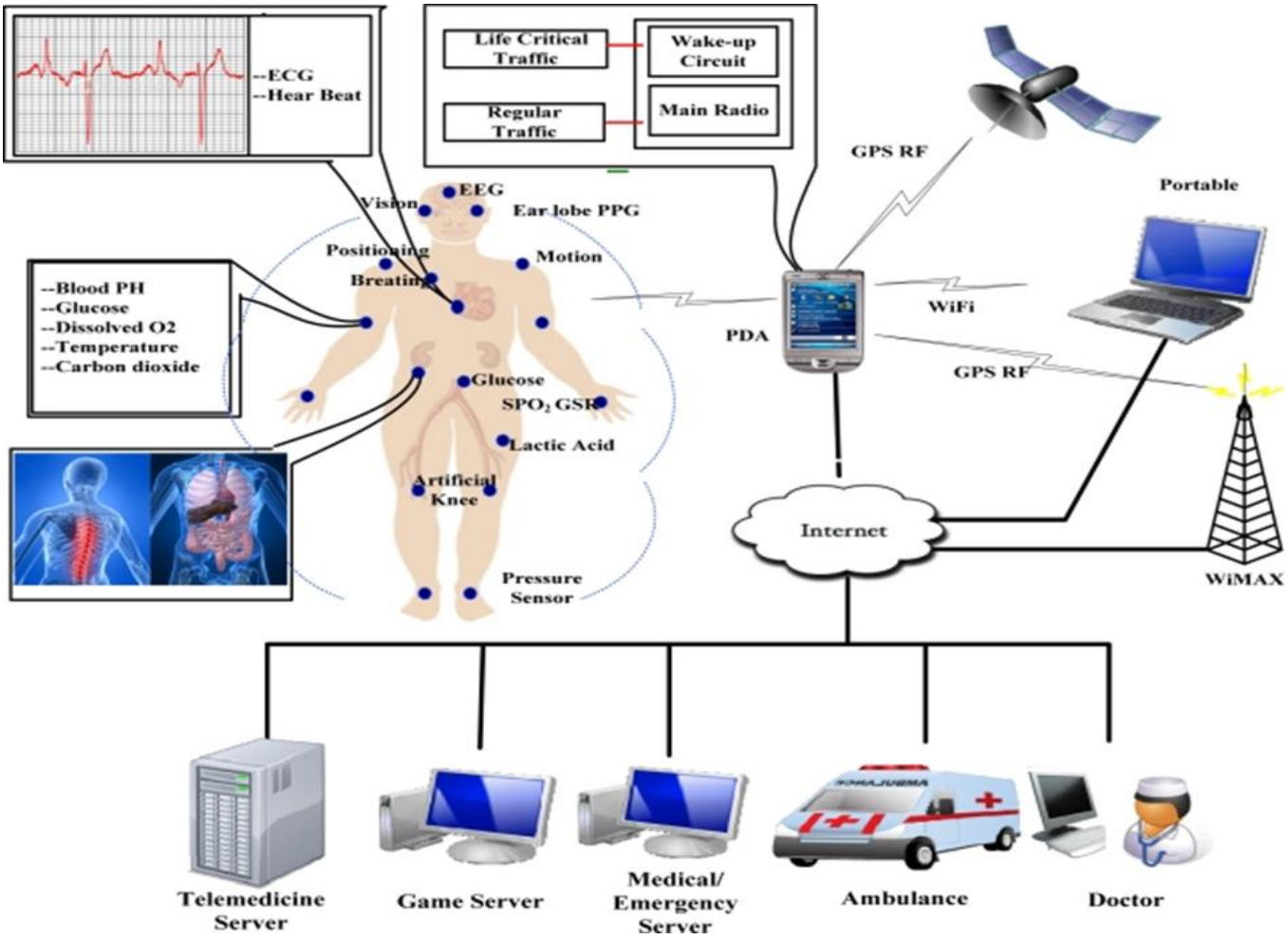

Fig. 1. WBAN architecture [6].

B. *Node Classification in a WBAN*

In WBAN a node is a free gadget which has communication ability. We can classified nodes into three distinct groups based which will perform a role in the network founded on his functionality, implementation.

a) *Node Type based on functionality*

Personal Device (PD): This gadget is responsible of collaboration with other clients by gathering the data given by the sensors and actuators. At that point it is advised the client over an external gateway by the PD, On the Actuator or on the gadget there is a screen/LED. The gadget is called body-gateway, sink, Body Control Unit (BCU) or PDA in few of the applications.

Sensor: In WBANs Sensors measure very certain amount or parameters in patient's body either inside or outside the body. When a physical stimuli happened the nodes automatically assembles and react to the information, process vital information and the information get a reaction from the wireless. The example of this type of sensors is physiological sensors, and the ambient or the biokinectics [5]. Few of the current sorts of these types of sensors could be utilized as a part of one's patients or a person's wrist watch, portable, or headphone and therefore, permit wireless checking of a man anyplace, whenever and with anyone. A rundown of various sorts of monetarily accessible sensors utilized as a part of WBANs are as per the following: DNA Sensor, Blood pressure, EMG, Spirometer, EEG, ECG, Temperature, Humidity, CO2 Gas sensor and so on.

Actuator: After receiving data from sensor the actuator collaborate with the user. The actuator gives feedback in the system by acting on sensor information, such as directing the right dosage of medication into the patient body in omnipresent medicinal services apps.

b) *IEEE classification for Nodes*

Another classification has been purposed by the IEEE 802.15.6 for node in a WBAN in which they are actualized inside the body, [2] [9] that is provided as follows:

Body Surface Node: In this type the node are placed on the surface or the outer side or the node is keep far away from the patient i.e. 2 cm far away from the patient.

External Node: Node in this category is not contacted to the patient's rather it is placed a couple of cm i.e. 5 meters far away from the patient's body.

Implant Node: Implant Nodes are those which are embedded within the human body, under the skin or situated on or in the inside the body tissue.

c) *Node Type base on Role*

These nodes are classified in the WBANs were based on their role as follows:

Coordinator: The working of a coordinator node is resembles to a gateway, or it resembles with another WBAN, or the access coordinator. All other nodes that want to communicate with each other make use of PDA known as WBAN coordinator.

End Nodes: The devices or end nodes used in WBANs are restricted to perform their inserted application. In any case, they don't have ability for transferring messages between nodes.

Relay: The relays node also known as intermediate nodes. They have two nodes one is called parent and the other node is called child node and they transfer the messages. Fundamentally if one of the node reaches at a limit, at that point any of the information is sent is required to be handed off from the alternate nodes before it reaches the PDA. The relays nodes can be used for detecting information.

III. Related Work for Security and Privacy in WBAN

In this section we talk about the recently published literature on E-Health using WBANs. In [17] Muhammed et al. also introduced BARI+ distributed key management protocol based on biometric, for WBANs. The authors assert that this protocol will help numerous security related services like confidentiality, authentication, and will provide security against different routing attacks and also defense against node compromise.

Huang et al. [18] stated secure access to a hierarchical sensor based healthcare monitoring architecture. Its architecture has three tier i.e. sensor, mobile, and back-end network tier and used for three healthcare apps (in-hospital, in-home, and nursing-home).In the sensor network tier, a wearable sensor system (WSS) make use of Bluetooth along with biomedical sensors to monitor the fundamental signs of individuals. Wireless sensor motes (WSMs) i.e., Mica2 are set inside the building to gather the ecological parameters. WSS and WSM safely broadcast physiological info and environmental parameters to the upper layer. WSS use AES authentication (i.e., CBC-MAC) associated with an encryption scheme, on the other hand WSMs utilize polynomial based encryption scheme to set up secure point-to-point communication between two WSM motes.

A protocol based on public-key is utilized to set up the secure keys. In the mobile computing network tier, mobile computing devices (MCD) like PDAs sorted out as in an ad-hoc network, route the data by means of multi-hops to the local station. MCD has the computational capacities needed to dissect the WSS and WSM data. Besides, the authors guarantee that their secure architecture gives security CIA i.e., confidentiality, integrity and authentication.

Muraleedharan Osadciw [19] introduced a secure and safe health monitoring network against DOS attacks utilizing cognitive intelligence. To prevent Sybil and worm whole attacks in health care app they introduced energy efficient cognitive routing protocol.

Le et al. [20] stated a protocol called MAACE in which only an authorized person can gain access to the patient confidential data. Their scheme gives mutual authentication and access control depends on ECC. Besides, the authors guarantee that purposed technique can shield against replay and DOS assaults. Le et al.'s protocol gives security for patient's private and confidential data that could be hazardous for a patient when compromised. Real-time healthcare applications can't compromise or accept, if patient's data disclosed to illegal users.

Malasri et al. [21] actualized a protected wireless mote-base medical sensing network for health care applications. Their set up defend against spoofing and physical layer attack, and gives CIA. Misic et al. [22] purposed 2 key distribution algorithms for implementing patient privacy in healthcare WSNs by utilizing key distribution algorithms.

Haque et al. [23] projected an effective and efficient security mechanism for patient monitoring systems using WSNs. Their scheme make use of public key primarily based infrastructure which gives data confidentiality.

Hu et al. [24] projected a patient healthcare monitoring system called tele-cardiology sensor network (TSN) that is based on software and hardware. TSN is specially intended for the U.S. healthcare community, it performs ongoing healthcare information gathering for aged patients in large nursing homes. In order to secure the patient privacy, TSN encourages confidentiality and integrity. Intra-cluster security, skipjack block cipher cryptography algorithmic program accustomed secure patient physiological (i.e., ECG data), associated an inter-cluster security make use of pre-distributed session keys. For various patients, cluster based routing is employed to diminish the patient-to-doctor routing overhead, and accomplished effectiveness. Security scheme which they used expends twenty six mJ for data processing, 1,002 mJ for radio communication, and 11 mJ for memory accesses.

Dagtas et al. [25] introduced secure architecture for health monitoring by utilizing ZigBee. Session key in WBAN is setup using secure and reliable key management protocol since it gives cryptographic keys that encourage security services, e.g., confidentiality, authentication, and data integrity. An authentication algorithmic program is utilized between the body sensors and also the handheld gadget of the mobile patient. Nonetheless, the authors give security to physiological data, but they didn't discuss which symmetric cryptosystem they utilized, and didn't analyze the energy potency for security services.

Kang et al. [26] for pervasive healthcare introduced a wearable context-aware system. The context-aware system is made out of wearable sensor systems, wearable PCs and communication modules. The wearable sensors are associated with wearable PCs by means of ZigBee. There are two kinds of sensors which can be used to a wearable. For exp, it is a sensor which is like a watch and there is a sensor which can be wearable on chest like a belt. Examples of wearable PCs, Personal digital assistant, are applied to collect the sensors' information. There is a technology which is called ZigBee which is used to communicate between the two first is the wearable sensors and other is Personal digital assistant. A LAN along with 802.11b WiFi is used to communicate among the Personal digital assistant and the services provided by the healthcare over the Internet.

Lin et al. [27] introduced SAGE is the idea which is good to provide solid security and privacy against the eavesdropping on the E-Health applications or systems. The system achieves content which is concerned with security and related privacy beside a solid worldwide foe. The idea behind SAGE is that when a patient information database (PIDB) acquires the Patient health information (PHI) from patient's body sensors for example, the accelerometer, and the blood pressure, or oxygen saturation, and temperature sensors [27]. It transmits the Patient health information to all of the patient doctors but the access is given to only one doctor or doctors which are applicable.. Authors proposed ECC which is based on privacy and security solution and show a proper or written evidence for the suggested solution which is against the eavesdropping worldwide.

Kumar et al. [28] gave another securing health solution which is known as the SHM stand for the secure health Monitoring via a medical WSNs. Secure Health Monitoring offers security facilities including the confidentiality, and the validity, as well as the integrity towards the patient's information at very little cost. In SHM, the privacy is acquired by Ping-Pong 128 stream cipher, validity and the integrity on the other hand are acquired by Ping-Pong-MAC.

Wu et al. [29] introduced AFTCS idea which is based on faultless connection mechanism for the body sensor networks. As the AFTCS give consistent and secure communication of data for precarious sensors by keeping the bandwidth which is regarding to the quantity of human physiological information, and the exterior environs as well as the system itself.

IV. Security and Privacy Requirements in WBANs

A. Security and Privacy Issue to E-health

The data which is created, stored related to patient conveyed by BANs is critical for medical diagnosis and treatment. Importance of securing this data, therefore, cannot be overemphasized. Significance of securing this information, thus, cannot be overemphasized. On the off chance that the information is tainted or appropriated, the impact could extend from ineffectual treatment of patients to abuses debilitating patients' lives.

For across the board acknowledgment by patients, as an essential piece of the healthcare framework, WBANs should likewise address privacy concerns. The conveyed idea of information in WBANs makes implementing security and privacy troublesome. It is imperative to manage these issues notwithstanding when the node is compromised or falls flat. Utilization of encryption and cryptography is picking up cash for upholding access control to secure the privacy of patients. The essential security necessities in WBANs are discussed below

a) *Data Confidentiality*

The confidentiality of data and information can be achieved by protecting data disclosure from illegal and authorized person it also involve data protection from other networks. It is an important issue and proper step should be taken so that we can save patient important information with neighboring or external networks. In a communication channel, we can obtain Data confidentiality of patient and its private or personal data by means of shared secret key and security algorithms.

b) *Scalability*

As in E-Health there are various patient related data, the distributed access control system ought to be versatile with the number of clients. The main important parts of it are low consumption and storage overhead is required. Low management overhead is required to set up and modified easily to obtain better result.

c) *Data Integrity*

The information can be modified or changed when ever data or information is transmitted in an insecure network. To protect information during transmission process where information can be altered, the error control can be guarantee by data integrity amid the transmission time of information. Despite the fact that it is hard to get error free transmission, the process of data integrity are used to confirm that data packets are not exchanged by opponents.

d) *Data Authenticity*

The term Authentication is important for medical as well as non-medical applications. Nodes which take part in communication process proved their identity by authenticity. During transmission process, the coordinator node and the member nodes require affirmation that data is being sent to a guaranteed center and not by intruder for performing some illegal actions.

e) *Data Availability*

Must provide guarantee of data availability in all health care system so that required operation can be carried out any time anywhere during emergency.

It gives an assurance and makes the work easy as they are designed in advance for patient security. Network degradation occurs if there is any problem in the network, switching to other network is important otherwise it leads to loss of life of a patient.

f) *Data Security*

In data security protection of the database from ruinous forces by maintaining secrecy is done. Due to which, an illegal and unauthorized person cannot access as well as cannot alter

data. To ensure data is transmitted securely encryption technique is used.

g) *Encryption*

Data Confidentiality is carried out by algorithm such as AES, DES and Advance Data Encryption Standards (ADES).

h) *Data Privacy*

The data or information can be approved to use only by legal and authorized person in data privacy. When data is disclosed to unauthorized entities (persons) this will lead to several risk factor and medical information of a person is very sensitive issue and can be only accessed by authorized person. Non- cryptographic technique is used for designs and protection of data privacy. The privacy of source location which is essential in WBAN can be improved by a protocol called phantom routing. This protocol will remarkably expands the privacy of source location by initializing a phantom source and flooding and privacy of data is provided. The privacy of medical data must be addressed through proper mechanism by all the system to carry out data privacy in the network.

B. Security and Privacy Related Attacks/Threats

Comparable to any wireless network, WSNs are experiencing a wide range of assaults. In this section, we discuss threats or attacks related to WSNs.

a) *Physical Layer*

Jamming: It is an attack which meddling with the frequencies of the radio that the nodes of a network are utilizing in jamming [11], [12]. These are the typical barriers which are against the jamming incorporate varieties of wide range communication, there are two examples, and one is frequency hopping and the second is code spreading.

Tampering: It is an attack in which a node is given the physical access to intruder, or an intruder can draw delicate data, for example, cryptographic secret keys or any other confidential information on the node. Then node is controlled by the intruder which can alter or supplanted to make it compromised. To make the physical package of the node with proofing with tamper is the defense for this type of attack.

b) *Data Link Layer*

Collision: A collision happens when more than one nodes endeavor to transmit on the same frequency at the exact time. A common safeguard to prevent the collisions is the utilization of correcting codes for the errors [12].

Exhaustion: An attacker can cause collisions that can repetitively be made utilization of to cause asset exhaustion. A solution which is attainable to force rates which limits the confirmation control of MAC and can disregard the excessive requests by the network, so by repeating transmissions it can prevent energy from draining [12].

Unfairness: As opposed to blocking a service access to outright, It can be corrupted by an attacker to gain the advantage and miss their transmission due date by causing the other nodes within a real time of MAC protocol. Utilizing minor frames lessens the effect of these type attacks just with diminishing amount of the time from which attacker grab and hold the communication of the channel.

c) *Network Layer*

Selective Forwarding: Which is mischievous node endeavors in the network to block or stop packets just by dropping or dismissing messages which is going through them. What's more, the malevolent node sends the data or information typically to the wrong or opposite path with the aim to put false routing information [13]. Utilizing various ways to send data or information provide defense against selective forwarding attacks on network layer. While the 2nd resistance is to identify the malevolent node and assume that it has fizzled and searched for an alternate route.

Sinkhole Attack: The main concern of the foe is that to draw all of the traffic from a specific region just with using the method of a traded off node, making a metaphorical sinkhole with the enemy at the middle. The attacks of Sinkhole usually succeed just with making a traded off nodes to appear especially it can be very attractive in terms of algorithm routing with neighboring nodes [14]. These are caused by the attacks of selective forwarding making it very easy and simple because almost all the traffic coming from a massive area within the network moves over the enemy's node.

Sybil Attacks: A single or one node which duplicates or multiplies himself and is introduced in multiple location. These attacks goes for the schemes of fault tolerance, for instance, the storage which is distributed, multipath routing, and topology maintenance. In these attacks, the solitary node shows numerous identities to different nodes in the network. The techniques of Authentication and the encryption methods can obstruct an outcast from beginning a Sybil attack on the sensor network.

Worm hole Attacks: In this attack, the assailant acquires some packets at one of the point within network, and then "tunnel" the packets with other points in the network, and then repeats them within the network from that point [15].

HELLO Flood Attacks: This is substantial many protocols using HELLO packets innocently expect that accepting these packets implies that the sender or transmitter is within the range of the radio also it is subsequently the neighbor. An attacker can utilize powerful transmitter which used to trick the large zone of the nodes to believe that they were neighbors of transmitting node. The Cryptography algorithm is the solution to these kinds of assaults.

d) *Transport Layer*

Flooding: When a new connection is made by an attacker then it requests again & again till the point when the assets compulsory by every connection is shattered or achieved a most extreme cutoff [16]. Answer of these types of issues is to necessitate every connecting user to prove its commitment to the connection by comprehending a puzzle.

Desynchronization: An enemy which repeatedly sends the messages which passes arrangement numbers to either at the endpoints. Requires the authentication of communication between all packets which is within hosts is one of the conceivable answers assault.

C. Regulations and Laws in Security and Privacy

Medical security and privacy is a basic prerequisite in E-Health everywhere throughout in world, so here is various rules and regulations that influence healthcare suppliers. Truth be told the regulations and acts fluctuate enormously from nation to nation. Now talk about the American in which Health Insurance Portability and Accountability Act of 1996 (HIPAA) [7] and the Health Information Technology for Economic and Clinical Health Act (HITECH) [8]. The health Insurance Portability and Accountability Act (HIPAA) orders that, in light of the fact that the sensors in WBAN gather the wearer's health knowledge, should be kept in mind to guard it from illegal access and change of state [9], [10]. As per the Act, human services suppliers are subjected with harsh punishments for exp fine of dollars $250,000 or detainment for Ten years, for the individuals which obtain and uncover the health data of the patient data for making money or malicious damage [8].

V. WBAN Security and Privacy Solutions

As we have realized from the previous sections that all the research aim is to secure the healthcare applications in wireless body area network. Clearly more research is required in E-health application, so that we can solve the security and privacy issues we have talked about in above section.

Wireless medical sensor networks make patients' life more relaxing as patient don't need to visit hospital, WBANs also give reasonable solutions to healthcare applications, for example, key sign observing, hospitals, home care, ambulatory care and as well as in the clinical examine.

To keep up solid security in an ongoing E-Health application, security and privacy should to be each stage like in application design, deployment, and implementation. HIPAA managed stringent principles for healthcare provider. In spite of the fact that it might appear sensible to utilize 128 bit AES. Due to longer secret key encryption/decryption time for this algorithm will be more, its might not be appropriate to use this algorithm.

There is also new block cipher which is more secure and suitable for low power consumption and that is known as HIGHT (high security and light weight) block cipher having 64-bit block size with 128 bit key [7].

Steam cipher, Digital signature, MAC, AES-CTR, AES-CBC-MAC, and AES-CCM based technique is more secure as compare to other but its complex, due to complexity they are difficult to implement.

A solid user verification and validation i.e. authentication protocol has not yet been tended properly at the application layer. User authentication with other possible mechanism should be introduce keeping in mind the end goal to prevent illegal user to gain access to confidential medical data of patient because its disclose can result in patient death.

We also purposed the utilization of Biometric strategy for solving security and privacy issue in WBANs since it is more proficient than other techniques used in WBANs of accomplishing all the security and privacy prerequisites. As in Biometric we make use of physical characteristics like fingerprint retina scanning and palm scanning so no one can take this characteristic so security and privacy is achieved.

Biometric is a procedure or technique which is used for providing distinguishing proof or checking of a person by his or her exceptional physiological or behavioral characteristics. WBAN conveys different security and privacy issues, for example, loss of information, authentication and access control. We recommended that biometric characteristics will be utilized which will not only increase security and privacy but also provide effectiveness in WBAN.

It is more secure, because in biometric provide defense against attack and risk influences, small key utilized, and it's more effective to implement.

A. Heart Rate Variability (HRV)

HRV is a physiological phenomenon where the time interval between heartbeats changes randomly. HRV have unique characteristics and we can use it in secure communications. HRV is measured by calculating the time between the spikes. HRV can be measured by any heart related signal; however Electrocardiogram (ECG) is the most preferred.

We have purposed the use biometric based security technique for the information verification and validation within WBANs. In particular, we use client's ECG feature as a key which is biometric based for information verification in Wireless body area network system. So, the data or the information of a patient can be detected and obtained individually from a patients assigned Wireless body area network scheme and one patient data or record is not mixed with other patients due to different physical and behavior characteristics in biometric system.

The security system implemented in biometric make use of low computational complexity and is more efficient instead of other cryptographic key distribution.

VI. Conclusion

Wireless Body Area Networks supporting healthcare applications are in early development stage yet offer significant commitments at monitoring, diagnostic, or therapeutic levels. As the WBAN sensor devices is being utilized for gathering the sensitive data and possibly will run into antagonistic situations, they require complicated and very secure security medium or structure to avoid the vitriolic communications within the system. These devices represent various security and privacy protection of touchy and private patient medical data.

We have purposed the use of Biometric technique as it's more efficient for acquiring security than other cryptographic procedures and algorithm. It is more secure, because in biometric framework there is no chance of replay eavesdropping and other such attack and threat which compromised the system security when we make use of algorithms having small key.

When we develop a security solution for WBANs we should keep in mind that it conforms to every side of WSN such as data privacy, integrity, data freshness, identity

authentication, and availability which make WBANs secure. As it's necessary to recommend a new policy adaptation in emergency healthcare, a future direction is to develop better, flexible, more secure, cryptographic imposed, and attribute based access control mechanism for wireless body area network because biometric implementation is somehow complex and costly.

REFERENCES

[1] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, "Body area networks: A survey," Mobile Networks and Applications,vol.16,pp. 171–193, 2011.

[2] J. Xing and Y. Zhu, "A survey on body area network," in 5th Int.Conf.on Wireless Communications, Networking and Mobile Computing(WiCom '09), pp. 1 –4, Sept. 2009.

[3] Khan, J.Y., and Yuce, M.R.: 'Wireless body area networks: technology, implementation, and applications' (Pan Stanford Pub., 2012. 2012).

[4] Milenković, A., Otto, C., and Jovanov, E.: 'Wireless sensor networks for personal health monitoring: Issues and an implementation', Computer Communications, 2006, 29, (13), pp. 2521-2533.

[5] Ullah, N., Khan, P., and Kwak, K.S.: 'A Very Low Power MAC (VLPM) Protocol for Wireless Body Area Networks', Sensors, 2011,11,(4).

[6] K. Y. Yazdandoost and K. Sayrafian-Pour, "Channel model for body area network (BAN)," Networks, p. 91, 2009.

[7] Deuko Hong, et al, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," CHES'06, LNCS 4249, 2006.

[8] http://waysandmeans.house.gov/media/pdf/110/hit2.pdf ,accessed on 22 December 2017.

[9] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S.. "PSKA: usable and secure key agreement scheme for body area networks," IEEE transactions on information technology in biomedicine a publication of the IEEE Engineering in Medicine and Biology Society, vol. 14, 2010, pp. 60-68.

[10] Li, M., Lou, W., & Ren, K.. "Data security and privacy in wireless body area networks," IEEE Wireless Communications, IEEE Press, vol. 17, Feb. 2010, pp. 51-58, doi:10.1109/MWC.2010.5416350.

[11] CC2420 DataSheet, "C2420, 2.4GHz IEEEE 802.15. 4/ZigBee-ready RF Transceiver," Chipcon, 2006.

[12] J. Sen, "Security in wireless sensor networks," inWireless Sensor Networks: Current Status and Future Trends,2012.

[13] K. Venkatraman, J. VijayDaniel, and G.Murugaboopathi, "Various attacks in wireless sensor network: survey," International Journal of Sot Computing and Engineering,vol.3,no.1,2013.

[14] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole attack in wireless sensor network," International Journal of Application or Innovation in Engineering & Management,vol.2,no.2,2013.

[15] T. K. Rao, M. Sharma, and M. V. Saradhi, "Wormhole attacks in Ad-Hoc networks," International Journal of Latest Trend in Computing,vol.4,no.2,2013.

[16] H. C. Chaudhari and L. U. Kadam, "Wireless sensor networks: security, attacks and challenges," International Journal of Networking, vol. 1, no. 1, pp. 4–16, 2011.

[17] Muhammad, K.R.R.S.; Lee, H.; Lee, S.; Lee, Y.K. BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors 2010, 10, 3911-3933.

[18] Huang, Y.M.; Hsieh, M.Y.; Hung, H.C.; Park, J.H. Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 2009, 27, 400-411.

[19] Muraleedharan, R.; Osadciw, L.A. Secure Healthcare Monitoring Network Against Denial-of-Service Attacks Using Cognitive Intelligence. In Proceedings of Communication Networks and Services Research Conference, Halifax, NS, Canada, 5–8 May 2008; pp 165-170.

[20] Le, X.H.; Khalid, M.; Sankar, R.; Lee, S. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. J. Networks 2011, 27, 355-364.

[21] Malasri, K.; Wang, L. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 2009, 9, 6273-6297.

[22] Misic, J.; Misic, V. Enforcing Patient Privacy in Healthcare WSNs Through Key Distribution Algorithms. Secur. Commun. Network 2008, 1, 417-429.

[23] Haque, M.M.; Pathan, A.S.K.; Hong, C.S. Securing u-Healthcare Sensor Networks Using Public Key Based Scheme. In Proceedings of 10th International Conference of Advance Communication Technology, Pyeongchang, Korea, 19–22 February 2008; pp. 1108-1111.

[24] Hu, F.; Jiang, M.; Wagner, M.; Dong, D.C. Privacy-Preserving Tele cardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign. IEEE Trans. Inform. Tech. Biomed. 2007, 11,619-627.

[25] Dagtas, S.; Pekhteryev, G.; Sahinoglu, Z.; Cam, H.; Challa, N. Real-Time and Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, doi: 10.1155/2008/135808.

[26] Kang, D.O.; Lee, H.J.; Ko, E.J.; Kang, K.; Lee, J. A Wearable Context Aware System for Ubiquitous Healthcare. In Proceedings of 28th IEEE EMBS Annual International Conference, New York, NY, USA, 30 August–3 September 2006; pp. 5192-5195.

[27] Lin, X.; Lu, R.; Shen, X.; Nemoto, Y.; Kato, N. SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth System. IEEE J. Select. Area Commun. 2009, 27, 365-378.

[28] Kumar, P.; Lee, Y.-D.; Lee, H.-J. Secure Health Monitoring Using Medical Wireless Sensor Networks. In Proceedings of 6th International Conference on Networked Computing and Advanced Information Management, Seoul, Korea, 16–18 August 2010; pp. 491-494.

[29] Wu, G.; Ren, J.; Xia, F.; Xu, Z. An Adaptive Fault-Tolerant Communication Scheme for Body Sensor Networks. Sensors 2010, 10, 9590-9608.