Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1171 – 1178

RESEARCH ARTICLE

SECURITY ISSUES IN WIRELESS BODY AREA NETWORK

Shikha Pathania[1], Naveen Bilandi[2]

[1]M.Tech (CSE) Student, DAV University Jalandhar, Email: shikhapathania02@gmail.com

[2]Assistant Professor in dept. of CSE, DAV University Jalandhar, Email id: naveen.bilandi@davuniversity.org

Abstract: Advances in wireless communication technologies and sensors have empowered development of Wireless Body Area Network (WBAN). The wireless body area network allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern. WBAN faces with various security issues such as loss of data, authentication and access control. In Wireless Body Area Networks (WBAN), security solution is required for data confidentiality, authentication and integrity at low cost. In this paper, we present an overview of body area network and their related issues emphasis in security problem. Finally, we highlight the security attacks in WBAN and the security requirements in WBAN followed by the security risk assessment.

Keywords: Wireless body area network (WBAN); attacks; requirements; risk assessment

I. INTRODUCTION

Wireless Body Area Networks (WBAN) has emerged as a key technology to provide real-time health monitoring of a patient and diagnose many life threatening diseases. WBAN operates in close vicinity to, on, or inside a human body and supports a variety of medical and non-medical applications. IEEE 802 has established a Task Group called IEEE 802.15.6 for the standardization of WBAN. The purpose of the group is to establish a communication standard optimized for low-power in-body/on-body nodes to serve a variety of medical and non-medical applications. [1].

Wireless Body Area Network (WBAN) could be a wireless network used for communication among sensor nodes operational on, in or round the human body so as to watch very important body parameters and movements. These observation signals are gathered by a personal device, e.g. a Personal Digital Assistant (PDA) or smart phone that acts as a sink for information of the sensor nodes and transmits them to care skilled for health observation. Wireless Body Area Network (WBAN) consists of a number of inexpensive, lightweight, miniature sensors which could be

located on the body as tiny intelligent patches, integrated in to clothing or implanted beneath the skin or embedded deeply in to the body tissues. This WBAN technology brings affordable and efficient healthcare solutions to people that will improve their quality of life. A WBAN contains a number of portable, miniaturized, and autonomous sensor nodes that monitor the body function for sporting, health, entertainment, and emergency applications.

In this paper we discussed about the security attacks in WBAN followed by the security requirement in WBAN. We have further discussed the security risk assessment and the existing security mechanisms. In the ultimate section we summarizes the related researches in security issues for Wireless Body Area Network.

1.1 Characteristics of WBAN

Basically, WBAN may be a communication network between the humans and computers through wearable Devices. So as to appreciate communication between these devices, techniques from Wireless Sensor Network and ad hoc networks may be used. A typical device node in WBAN ought to make sure the accurate sensing of the signal from the body, do low-level process of the sensor signal and wirelessly transmit the processed signal to an area process unit [2]. However, attributable to the everyday properties of a WBAN, current protocols designed for these networks don't seem to be forever compatible to support a WBAN. To support this time, TABLE I simplifies the overall variations between a Wireless sensor Network and a Wireless Body Area Network as mentioned elsewhere in [3] and [4]:

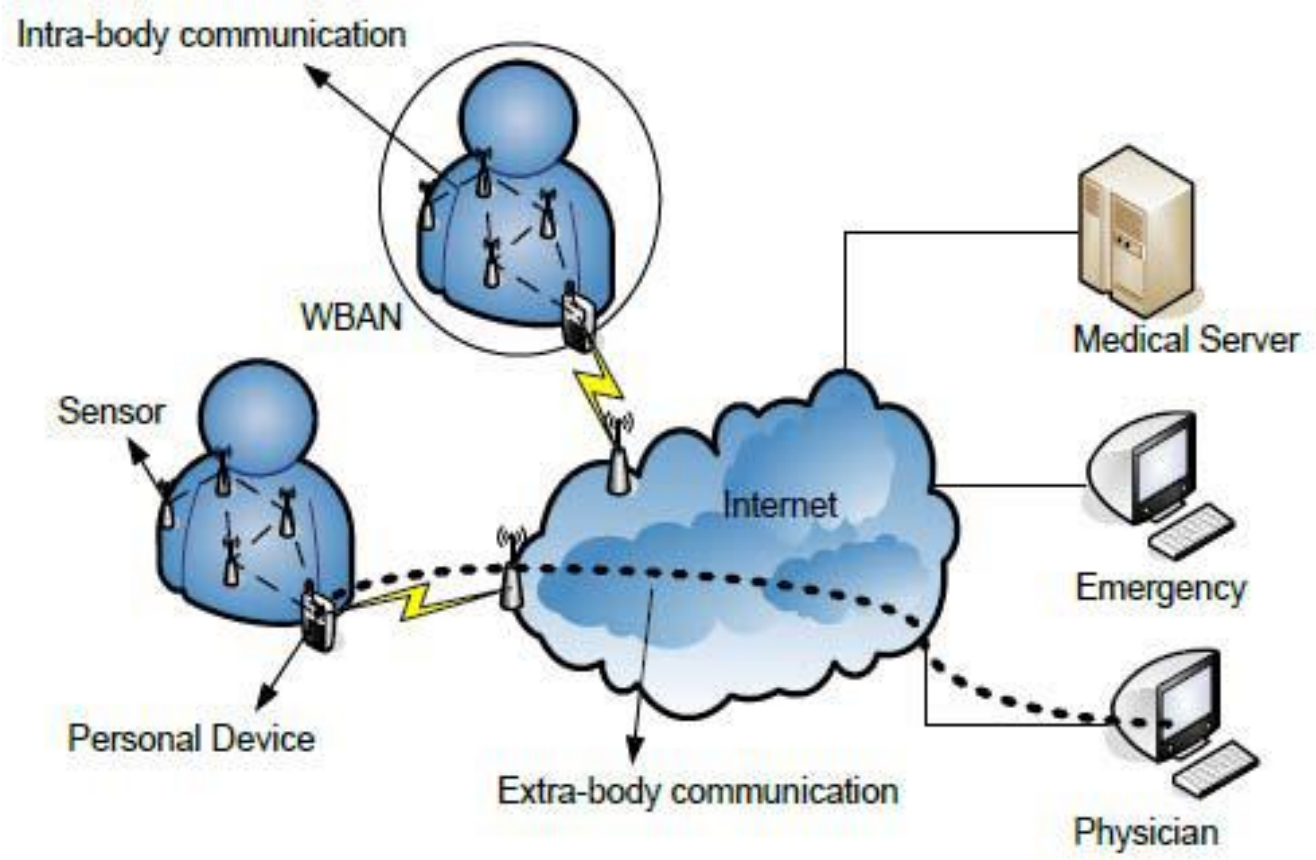
TABLE 1: THE GENERAL DIFFERENCES BETWEEN WBAN AND WSN

	WBAN	**WSN**
Deployment	The number of sensor nodes deployed by the user depends on different factors. (i.e.: on human body or hidden under clothing).Devices are equally important and only added when they are needed for application. WBAN does not employ redundant nodes.	WSN is often deployed in places that may not be easily accessible by operators which require more nodes to be placed to compensate for node failures.
Densiy	WBAN is not node-dense	
Data Rate	WBAN may occur in a more periodic manner and stable data rate.	WSN is employed for event-based monitoring where events can happen at irregular intervals.
Mobility	WSN is employed for Event based monitoring where events can happen at irregular intervals.	WSN nodes are usually considered stationary.
Latency	Replacement of batteries in WBAN nodes is much easier done when energy conservation is definitely beneficial.	Nodes can be physically unreachable after deployment. It may be necessary to maximize battery life-time in WSN at the expense of higher latency.

1.2 General Architecture

This section provides an outline of general design in WBAN. Each form of network has its typical enabling technology, outlined by IEEE. A WPAN uses IEEE 802.15.1 (Bluetooth) or 802.15.4 (Zigbee), a wireless fidelity uses IEEE 802.11 (Wi-Fi) and WMAN IEEE 802.16 (WiMax).The communication during a WAN may be established via satellite links. As mentioned before, though challenges faced by WBAN are in many ways kind of like WSN, there are intrinsic variations between the two requiring special attention. The development associated analysis within the domain of WBANs is simply at an early stage. As a consequence, the word isn't continually clearly denned. In literature, protocols developed for WBANs will span from communication between the sensors on the body to communication from a body node to an information centre connected to the net. So as to own clear understanding, we tend to propose the subsequent dentitions: intrabody communication and extra-body communication. An example is shown on Figure 1.

Figure 1



II. SECURITY ATTACKS IN WBANS

The development of WBANs is hindered by various security threats due to the vulnerable nature of wireless channel. Some of the major attacks in WBANs are as follows:

a. **Eavesdropping:** The features of wireless channels in WBANs are open. Hence the radio communication between the nodes in the WBANs can be intercepted by the attackers freely and easily. This allows the attackers to eavesdrop packets from node to node. It also helps the attackers to obtain sensitive and valuable information. [5]

b. **Data Modification:** The eavesdropped information are partly or fully removed or replaced by the attackers. The modified information is send back to the original receiver to achieve some illegal purpose.

c. **Impersonation Attack:** The attacker eavesdrop the legal BAN Network Controller (BNC's) or the BAN nodes (BN's) private identity information. He uses the legal identity information to cheat BN's or BNC. [6]

d**. Replaying:** A part of the valid information can be eavesdropped by the attacker and is send back to the original receiver after some time to achieve the same purpose in different case.

e. **Denial of Service:** When the traffic is beyond the capacity of the systems, the Denial of Service (DoS) attack occurs. The effect of both intentional act of malicious and compromised nodes and unintentional excessive peak network utilization is associated with it. A DoS attack can be easily initiated by the attackers using the infected BNs, when the authenticated BNs are compromised. [7]

III. SECURITY REQUIREMENTS IN WBANS

In general, the characteristics of an application are needed to build robust security mechanism, which defend the system from possible security threats. The fundamental security requirements in WBAN are described below, [8].

1. Data Confidentiality

To protect the data from a disclosure, the system require data confidentiality. During communication, there is a possibility of overhearing and eavesdropping the sensitive information by the adversary. Encrypting the data with a secret key and sharing the secret key through a secure channel is one of the ways to acquire confidentiality.

2. Data Authentication

Applications including both medical and non-medical application necessitates data authentication. Each BN and BNC has to verify whether the data is transmitted by the trusted sensor or by the adversary. Symmetric technique can be used in a WBAN to achieve data authentication. This technique shares the secret key to compute Message Authentication Code (MAC) for all data.

3. Data Integrity

Data integrity is necessary as an adversary can alter the data that is transmitted over an insecure channel. Absence of data integrity technique paves a way to the adversary to modify the information before it reaches the BNC. Data integrity is attained through data authentication protocols, which ensures that the received data is not changed by the adversary.

4. Data Freshness

The data freshness technique is essential to assure data confidentiality and integrity. The adversary may confound the BNC by taking data during transmission and retransmit them later. Data freshness guarantees the newness of data. In our words, it checks the arrangement of data frames. Strong freshness and weak freshness are the two types of data freshness.

5. Secure Management

As BNC, distribute keys to BNs to achieve encryption and decryption techniques, it demands secure management. The BNC adds and removes the BNs in a secure manner in the case of association and disassociation.

6. Availability

It guarantees that the patient's information is accessible to the doctor. This accessibility can be destroyed by the adversary by disabling an ECG mode. This may lead to critical situation such as loss of life. During the loss of availability, a technique is required to maintain the operation of the BNs and switch the operation to another BN [9]

In addition to the basic security requirements like confidentiality, integrity protection and authentication certain other goals should be met. It includes:

Efficiency: An important aspect of a BSN's design is energy-efficiency due to the limited capabilities of sensors. The continuous monitoring requirements of a BSN can be hindered by the frequent energy depletion even though the sensors are rechargeable. Hence energy-efficient secure communication is needed for BSN.

Usability: The security solutions for BSN have to be useable. The usable security solutions are defined which are activated on employment in plug-n-play manner with minimal initialization procedures [10].

IV. SECURITY RISK ASSESSMENT

Currently, the following two risks were identified. A few more risks will be added later as the system is deployed and services are delivered in a full scale.

A. Qualitative Security Threats Assessment

As the system is in laboratory scale implementation and
testing, we conduct risk assessment with the assumption of user's activities of daily living while the user is using the device for the remote healthcare monitoring service consisting of data collection, processing, transmission, storing and sharing. Two of the major security threats are caused by the user's daily use and data sharing. The

communication links of IEEE 802.15.4, IEEE 802.11g, and Internet protocol are also regarded as vulnerable points of security threats.

When the user has a wireless device in his/her Wireless Body Area Network (WBAN), the vital signals are being sensed by the sensor transmission node, the vital signals can be targeted when intruders synchronize the wireless bandwidth using IEEE 802.15.4 bandwidth as an unauthorized source. It causes a confidentiality issue and an availability issue. When the intruders alter the vital signals in the sensor transmission node, it will cause misinterpretation of the user's vital signals by the automated analysis software tool in the remote web portal system and/or by the health professionals as it causes an integrity issue.

B. Proposed Security Features

The features for security and privacy in transferring data consists of monitoring human body signals needs

Authentication, integrity, access control, non-repudiation and encryption features. For the security features of the system, we need to adopt the concept of scalability and compatibility by adopting the Elliptic Curve Cryptographic algorithm, Mutual Authentication and Group key Agreement protocols. It should include the security features integrated into the cryptographic protocol and the data structure. The verification of security features in the system will also have to assess power consumption and computing resources.

C. Enabling Technology Resolving Security Threats

We reviewed security perspectives for the remote health monitoring system which offers an inexpensive, yet flexible and scalable, wireless platform to deliver, train and monitor data provided by biosensors. For sustaining the high level of security in all the applications in the system, we consider importing cryptographic functions with a plug-and-play (PnP) gadget that can be setup quickly by a non-professional and the pervasive monitoring becomes possible without interruption in patient's daily routines.

For the strong level of security, we need to implement Advanced Encryption Standards (AES) 128 cryptographic algorithm in the hardware accelerator of the user's sensor node module [11]. There is a new block cipher suitable for low resource device in the research community and one of them is HIGHT (aka high security and light weight) block cipher with 64-bit block size and 128 bit key size [12].

For the cryptographic algorithm of TinyOS, elliptic curve cryptographic algorithm, ECIES, and key distribution protocol, ECDH, and digital signature algorithm, ECDSA, have been introduced [13]. With these cryptographic algorithms, we need to investigate and perform feasibility research on real world implementation and field testing of security features in the remote health monitoring system.

V. EXISTING SECURITY MECHANISMS

Security mechanisms are processes that are used to detect, prevent and endure security attacks. This sub-section discusses the problems regarding existing security mechanisms, as follows:

1) Cryptography

As wireless body area sensor networks alter sensitive physiological info, sturdy cryptographic functions are unit preponderating necessities for developing any secure attention application. These cryptographic functions give patient privacy and security against several malicious attacks.. Further, the selection of cryptography system depends on the computation and communication capability of the sensor nodes. Some argue that asymmetric crypto systems are typically too high-priced for medical sensors and interchangeable crypto systems don't seem to be versatile enough [14].

2) Key Management

Key management protocols are measure basic necessities to develop a secure application. These protocols are used to set up and distribute varied forms of cryptographic keys to nodes within the network. Generally, there are three styles of key management protocols, namely, trusty server, key pre-distribution and self imposing [15].

3) Secure Routing

In home care or disaster eventualities sensor devices might require sending their data to alternative devices

Outside their immediate radio vary [16]. Therefore, routing and message forwarding could be a crucial service for end-to-end communication. So far, several of routing protocols are projected for sensor networks; however none of them are designed with strong security as a goal. Karlof-Wagner mentioned the actual fact that routing protocols suffer from several security vulnerabilities, like associate degree offender may launch denial-of-service attacks on the routing protocol. *4) Resilience to Node Capture*

Resilience against node capture is one in all the foremost difficult issues in sensor networks. In real time healthcare applications, the medical sensors are placed on a patient's body, whereas, the environmental sensors are placed on

hospital premises (e.g., ward room, operation area etc.) which can be simply accessible to attackers. Thus, an attacker might be able to capture a sensor node, get its cryptanalytic info and alter the sensor programming consequently. Later, he/she will place the compromised node into the network, which may endanger application success [17].The current cryptographic functions (i.e., node authentication and identification) might discover and defend against node compromised attacks to a point, however these compromised node attacks can't be detected instantly [17] that could be a massive issue for healthcare application..

5) Trust Management

Trust signifies the mutual association of any two trustworthy nodes (i.e., sensor node and information aggregator node), that are sharing their data. In [18] trust is outlined as "the degree to that a node ought to be trustworthy, secure, or reliable throughout any interaction with the node". Boukerche-Ren [18], evaluated the trust for mobile healthcare system.

6) Secure Localization

WBANs facilitate mobility for patient's comfort, thus patient location estimations are required for the success of healthcare applications. Since, medical sensors' sense physiological information of a personal, they additionally ought to report the patient's location to a far off server. As a result, medical sensors need to remember of patient location, i.e., referred to as localization. In [18] the authors mentioned localization systems that were divided into: distance/angle estimation, position computation and localization algorithms, and more, they mentioned attacks on localization systems

VI. RELATED WORK

Ming Li et.al[19] has said that the wireless body area network has emerged as a new technology for e-healthcare. The data of a patient's vital body parameters and movements are collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. They said that it has improved the healthcare quality. The main concern is to secure the data collected from WBAN. They look into two important data security issues namely secure and dependable distributed data storage , and fine grained distributed data access control for sensitive and private patient medical data. Many practical issues has been discussed that need to be taken into account while fulfilling the security and privacy requirements.

Dr. Shinyoung Lim et.al[20] has discussed about the target system that has a scalable platform that requires minimum human interaction during setup and monitoring. The core components of the system include: (i) Biosensor/transceiver pairs, (ii) Hardware modules to automatically setup the wireless body area network, (iii) Data delivery mechanism to an internet server, and (iv) Automatic data collection, profiling and reporting. They assess security risk based on this critical needs of acknowledged risks and threats in the real time remote health monitoring system. They have discussed a simple yet flexible and scalable framework of a scalable wireless biosensor system tuned for real-time remote monitoring as a case study of security threats assessment.

Sofia Najwa Ramli et.al[21], they presented an overview of body area network and their related issues emphasis in security problem. They also study the differences between Wireless Body Area Network and Wireless Sensor Network (WSN). They highlighted the security challenges that still need to be addressed to make WBAN truly ubiquitous for a wide range of applications. WBAN brings out a new set of challenges in terms of scalability, sensor deployment and density, energy efficiency, security and privacy and wireless technology so WBAN requires a strong security system and part of it is authentication. So there is need to discover hybrid authentication protocol in providing a strong security system for WBAN.

Ramesh Kumar et.al[22] have reviewed the present development on Wireless Body Area Network and targeted in security problems faced by this technology. WBAN faces with varied security problems like loss of information, authentication and access control. They tend to give an summary of body area network and their connected problems stress in security downside. Their work presents an outline of the variations between Wireless Body Area Network and Wireless sensor Network. They tend to highlight security challenges that also have to be compelled to be addressed to create WBAN actually present for a wide range of applications. They tend to believe that WBAN needs a robust security system and a part of its authentication.

Ragesh G K et.al[23] presents an overview on the various aspects of WBAN including sensors used, applications, power efficiency, communication protocols, security requirements, existing projects in WBANs and challenges faced in wireless body area networks. They discussed energy requirements, security requirements and issues present in various layers of WBAN. Finally some of the social issues related to WBAN application are mentioned in this paper. There are many challenges that still need to be addressed, especially on high bandwidth and energy efficient communication protocols.

VII. CONCLUSION AND FUTURE SCOPE

WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. It brings out a replacement set of challenges in terms of sensor deployment and density, energy potency, security and privacy and wireless technology. In this paper, we've reviewed the present development on Wireless Body Area Network and that we targeted in security problems faced by this technology. During this paper, we discussed the security attacks and requirements in WBAN. We presented the existing security mechanisms in WBAN. In this paper, we also presented the difference between WBAN and WSN. Thus, we tend to believe that WBAN needs a robust security system and a part of its authentication. A secured authentication system is extraordinarily required in numerous applications WBAN technology notably in medical and military

REFERENCES

[1] Kyung Sup Kwak, Sana Ullah, Niamat Ullah, "An overview of IEEE 802.15.6 Standard", 3rd International Symposium on Applied Sciences in Biomedical & Communication Technologies (ISABEL2010) in Rome, Italy

[2] Selimis, Georgios et al. "A Lightweight Security Scheme for wireless Body Area Networks: Design, Energy Evaluation and Proposed Microprocessor Design," Journal of Medical Systems, 2011, pp. 1-10-10, doi: 10.1007/s10916-011-9669-2.

[3] Latré, Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. "A survey on wireless body area networks," Wireless Networks, vol. 17, 2010, pp. 1-18, doi: 10.1007/s11276-010-0252-4
.
[4] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. "Body Area Networks: A survey," Mobile Networks and Applications, vol. 16, 2011, pp. 171-193, doi: 10.1007/s11036-010- 0260-8.

[5] Jingwei Liu, Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", pp.98-103,2010.

[6] Neha Sharma and Er.Meenakshi Bansal, "Preventing Impersonate Attacks Using Digital Certificates in WBAN", International Journal of Advanced Engineering Sciences and Technologies, Vol-9, pp- 31-35, 2011

[7] T.V.P. Sundararajan and A. Shanmugam, "A Novel Intrusion Detection System for Wireless Body Area Network in Health Care Monitoring", Journal of Computer Science, pp- 1355-1361, 2010

[8] Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, "On the Security Issues in Wireless Body Area Networks", International Journal of Digital Content Technology and its Applications, Vol 3, No 3, Sept 2009.

[9] Shahnaz Saleem , Sana Ullah and Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", Sensors, vol- 11,pp- 1383-1395, 2011

[10] Krishna K. Venkatasubramanian and Sandeep K.S. Gupta, "Physiological Value Based Efficient Usable Security Solutions for Body Sensor Networks", pp.1-77.

[11] CC2420 DataSheet, "C2420, 2.4GHz IEEEE 802.15. 4/ZigBeeready RF Transceiver," Chip-con, 2006.

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

[13] TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks, Ver 1.0, http://discovery.csc.ncsu.edu/software/TinyECC, 2007.

[14] 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.

[15] Ng, H.S.; Sim, M.L.; Tan, C.M. Security Issues of Wireless Sensor Networks in Healthcare Applications. BT Tech. J. 2006, 24, 138-144.

[16] Lorincz, K.; Malan, D.J.; Fulford-Jones, T.R.F.; Nawoj, A.; Clavel, A.; Shayder, V.; Mainland, G.;Welsh, M. Sensor Networks for Emergency Response: Challenges and Opportunities. Pervas.Comput. 2004, 3, 16-23.

[17] Kavitha, T.; Sridharan, D. Security Vulnerabilities in Wireless Sensor Networks: A Survey.J. Inform. Assur. Secur. 2010, 5, 01-044.

[18] Boukerche, A.; Ren, Y. A Secure Mobile Healthcare System Using Trust-Based Multicast Scheme. IEEE J. Select. Area. Commun. 2009, 27, 387-399.

[19] Ming Li et.al "Data security and privacy in wireless body area networks" wireless communication,IEEE(Volume:17, Issue:1), pp 51-58, Feb 2010,doi: 10.1109/MWC.2010.5416350

[20] Dr. Shinyoung Lim et.al "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring" 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pages 327-332, IEEE Computer Society Washington, DC, USA ©2010 doi:10.1109/SUTC.2010.61

[21] Ramli, S.N.; Ahmad, R., "Surveying the Wireless Body Area Network in the realm of wireless communication," Information Assurance and Security (IAS), 2011 7th International Conference on , vol., no., pp.58,61,5-8Dec.2011
doi: 10.1109/ISIAS.2011.6122845

[22] Ramesh Kumar; Rajeswari Mukesh; "State Of The Art : Security In Wireless Body Area Networks" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 4 No. ,05 May 2013 ,pages 622-630, ISSN : 2229-3345

[23] Ragesh G K; Dr.Baskaran K; "An Overview of Applications, Standards and Challenges in Futuristic Wireless Body Area Networks" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, pages180-186,January 2012 ISSN : 1694-0814

