Trustworthiness of Wireless Body Area Networks (WBANs) and Medical Devices in Healthcare Applications

Sunita N. Karande, Govindkumar B. Lohiya

Abstract — **Nowadays, Personal Healthcare Systems (PHS) based on Wearable and Implantable Medical Devices (WIMDs) are commonly used for detecting, diagnosing and correcting medical conditions. Providing us with the greater functionalities, WIMDs are also becoming less trustworthy, less reliable and open up opportunities for malicious attackers. The trustworthiness in WIMDs and WBANs are becoming weakened due to various shortcomings like fault in the hardware, errors in the software, and attacks in wireless communication. Fault in medical devices can cause life critical situation hence trustworthiness of WIMDs must be addressed with highest priority. Conventional fault tolerance and information security solutions, like redundancy and cryptography, which have been employed in general-purpose and embedded systems, are not suitable for many WIMDs due to extreme size and power constraints and unique usage models. This paper discusses trustworthy approach in WIMDs and BANs through a comprehensive study of trustworthiness requirements, reliability issues and solutions for improving trustworthiness of WBANs.**

Index Terms -| **Physical Healthcare System (PHS), privacy, reliability; security, Wireless Body Area Networks (WBANs); Wearable and Implantable Medical Devices (WIMDs)**

I. INTRODUCTION

In the recent years wireless sensor network (WSN) technology has been used for various applications. It is mainly being used in the field of biomedical sensor network (BSN) for measuring physiological parameters. Wireless Body Area Networks (WBAN) is a wireless network which is used for exchanging medical data from the medical sensor which are placed in or around close proximity of the human body. These networks are used to monitor patient's vital body parameters under normal physiological states without disturbing their normal activities. As the system is wireless, patients need not to be admitted in the hospital for hours and no wire is attached to their body. Patient's data is collected from the sensors and monitored using remote health monitoring equipment.

The cardiovascular disease is the main cause of the death in the world. According to the World Health Organizations, worldwide about 17.3 million people died from heart attacks or strokes in 2008, which represents 30% of global deaths. The number of deaths from cardiovascular disease, mainly from heart disease and stroke, will increase to reach 23.3 million by 2030[1].

Manuscript received

***Sunita N. Karande**, Electronics Department, Mumbai University, Datta Meghe College of Engineering, Airoli, Navi Mumbai, India*

***Govindkumar B. Lohiya**, Electronics Department, Mumbai University, Datta Meghe College of Engineering, Airoli, Navi Mumbai, India.*

Research work related to WBAN has been proposed by many universities and researchers. The work can be divided into following categories e.g. by number of vital signal types, single and multiple, by location of medical sensor, implantable or wearable, by wireless transmission type, ZigBee, Bluetooth, and Wi-Fi, by access point, laptop, computers, Personal Digital Assistants and smart phones. Some of them are listed in Table I [2].

Nowadays WIMDs are frequently used in medical applications for performing variety of tasks. For performing these tasks WIMDs should be Intelligent and compatible to work with the smart devices.

Many of the WIMDs are connected to electronic devices and to web or cloud networks, therefore their security becomes the prime concern. WIMDs subjects to many threats like patient data extraction, data tampering, device reprogramming, repeated access attempts, device shut off, therapy update, malicious inputs, data flooding. As these devices can be attacked by the malicious attacker they are becoming less secure, less reliable, or less trustworthy.

WIMDs are coming in the extreme size and shape with the more complex hardware and software. Maintaining reliability of these medical devices becoming a challenging part for the manufactures. As size and power constraints are more important point in designing WIMDs, it creates challenge for embedding any new software or hardware in the device.

In the area of WBAN trustworthiness is referred to the relation among medical devices and the related entities. At the user-system interaction level, this can be normally supported a high transparency and a transparent interaction, complemented with reliable and proper operation. Once used within the system, trust and trustiness consult with relations between entities within the system itself.

Trust is made up of some collective properties, can be determined through monitoring, and is related to the expected service. Trust is defined as the degree to which a trustor has a justifiable belief that the action done by the trustee is reliable. This paper discusses trustworthy approach in WIMDs and BANs through a comprehensive study of trustworthiness requirements, reliability issues and solutions for improving trustworthiness of WBANs.

II. WIRELESS BODY AREA NETWORKS (WBANS)

Wireless Body Area Networks (WBANs) is the sensor network around the body of a person which uses Wearable or Implantable Medical Sensors that can be placed in or around close proximity of the human body. These medical devices can sense biological, physical, and chemical changes of the person. Using WBAN a person who wears it can be warned about the life critical situation. The life critical data can be sent to the medical supervisor or doctor so that the person can get the

ISSN: 2278 – 909X

medication on time in some emergency cases. These medical data can be sent to the close relative, to nearest hospital, or to the medical persons who can then take necessary action.

WBAN contains biodegradable sensors to sense the medical data, trancereceivers to transmit and receive the sensed data, processors for proper functioning of all the components in the WBAN, accelerometers for sensing dynamic changes in the body, and batteries for supplying power to the medical sensors. WBAN is used for detection of chronic diseases in advance. In WBAN communication can pair between sensors on the body and communication from body node to a data center to the Internet, thus communication in WBAN is divided in two categories: Intra body communication, Extra Body communication

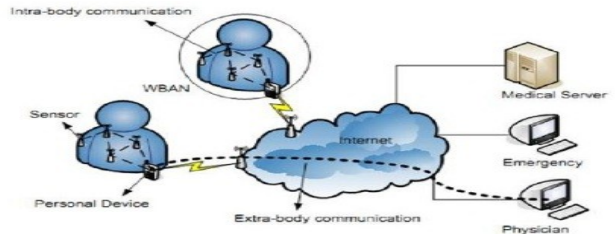


Fig. 1 Intra Body and Extra Body communication in WBAN [3]

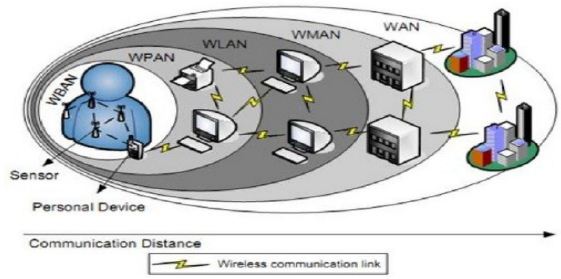


Fig. 2 WBAN is compared with other types of wireless networks [3]

WBAN TRUSTWORTHINESS REQUIREMENTS

Major WBAN Trustworthiness requirements are summarized in Table I [4]

A. WIMDs Reliability

WIMDs are used for medical applications and these applications can be life critical therefore these devices must be reliable. When devices are used only for monitoring and treatment is done based on further assessment then, fault in these devices are not so harmful. But when data provided by these devices are used to take important decisions then fault in these devices concerned.

B. WBAN Confidentiality:

In WBAN medical data is transmitted using wireless medium making BAN compromise on patient data confidentiality. When transmitting life critical data one can gain life critical information by eavesdropping, and can launch attack on BAN integrity.

C. Data Integrity:

Information transmitted or received by the BAN must be authenticate using proper authentication process, and the data must be complete with all respect. If treatment is based on the received data the data should be uncorrupted as it can lead to false treatment, and it should be complete otherwise collecting accurate data may delay the treatment.

D. Network Availability:

BAN should be available in extreme environmental conditions. An attacker can use the denial of service attack, to overflow the requests and restrict BAN to provide services to the patient. All the patient related data must be easily available during the jamming condition also.

E. Privacy:

Patients medical data should be kept confidential during its transmission form patient node to the medical server, patient identity should not be disclose, patient should be provided with maximum privacy.

TABLE I
WBAN TRUSTWORTHINESS REQUIREMENTS

Requirements	Description
Reliability	WIMDs should function correctly even in the extreme environmental conditions
Confidentiality	Information transmitted within the BAN should be secured from unauthorized access. Patient data stored on WIMDs, health hub, or remote server should be kept confidential
Integrity	Information transmitted within the BAN should be authenticate and complete Patient data stored on WIMDs, health hub, or remote server should not be altered
Availability	The BAN should be available even during jamming and denial of service attacks. Patient data stored on WIMDs, health hub, or remote server should be readily retrievable
Privacy	Using a PHS or carrying a device should not disclose patient condition.

III. THREATS, VULNERABILITY, RISKS IN WBAN RELIABILITY ISSUES IN MEDICAL DEVICES AND THEIR SOLUTIONS

In the following subsections we will discuss threats, vulnerability; risks faced by the WIMDs, and then discuss possible countermeasures to treat them.

1. WIMDs Threats, Vulnerabilities and Risks

a. Treats:

Extraction of Data, tampering of Data, Reprogramming, Frequent attempts, Device Breakdown, Medication update, Malicious inputs, Medical data flooding

B. Vulnerabilities:

Communication Channels are unsecured, poor Authentication, Improper Access Controls ,Software Vulnerabilities, imperfect Audit Mechanisms ,Insufficient Storage , deficient Alerts

C. Risks:

Patient Safety, Software Faults, Malicious Therapy Update, Malicious Device Inputs, Loss of Patient Privacy, Data lost from Device , Incorrect Medical Follow-up, Patient Readings Tampering, Unavailability of Device, Battery Power Drainage, Device Data Flooding.

2. Reliability in Medical Devices

Nowadays many of the patients are benefited using Wearable and Implantable Medical Devices (WIMDs). As use of WIMDs is increasing rapidly their reliability also becomes very

ISSN: 2278 – 909X

important. To become reliable WIMDs should prove them secure. In WIMDs security is categorized as hardware security and software security. For analyzing security issues we first go through the hardware and software faults.

a. Hardware Faults

WIMDs that only provides us with the data but final action is taken after processing this data, are less harmful e.g. if the false alarm generated by the fall detector device, the device can be repaired to provide with the correct alarm. In this case there is no harm to the person who is wearing that device only the corrective action should be taken. In other situation where the fault in device can tend to life critical situation e.g. when a driver is driving the vehicle and his vision sensor stops working then the situation can be life threatening. In this situation fault in the devices cannot be tolerated and one should take proper precautions so that these types of situations can be avoided. Extreme working conditions can also make the device faulty e.g. extreme temperature, vibrations, electromagnetic interferences, or power failure. These medical devices are made with complex hardware and software for providing accurate data, their size is extreme as these are also used for monitoring inside body parameters. The software used for these devices is also complex, because many systems are embedded in one device.

b. Software Faults:

As WIMDs uses complex hardware, for controlling this hardware these devices also needs complex software. Sometimes this software can also affected by the fault tending the operation of WIMDs to malfunction. Software failure can be detected by following observations, an alarm failed to sound, patient medicine dosages inconsistent with the data on the display unit, visual outputs and display unit values were inconsistent, system unknowingly stopped, if several conditions occurred simultaneously system acts incorrect, patient data were lost or corrupted. In some of the situations one or software can be faulty which leads to the total system failure. It is very difficult to design perfect software for the given complex medical device. Till date there is no standard verification method is available for the medical device software. It is contended that open source software are becoming more reliable and secure in medical applications.

3) Approaches for Improving WBAN Reliability

In WBAN WIMDs communicates with a programmer or between other WIMDs medical devices and server. The attacker in this situation is an adversary which acts remotely over the air, against the WBAN network. There are two types of adversaries one “Active” which can modify, jam, forge, replay or drop messages within the WBAN network. In second type the adversary cannot directly attack the IMDs as it is implanted in the body. For securing WIMDs key agreement schemes can be used [6]. In this section we discuss some of the solutions for improving WBAN reliability.

A. *Cryptography:*

Cryptography is one of the methods to secure wireless communication channel and to avoid unauthorized access. In WBAN for secure key distribution Public key cryptography is used more frequently. More reliable easily available TLS protocol is used for public key distribution to the server. Public Key Infrastructure (PKI) allows authorities to certify these public keys to the specific domain name so that these public keys make the bond with the respective trusted entity. Allotting these many public keys and maintaining them is the big task and breakdowns in the trustworthiness of certificate issuance also arises the challenges in making PKIs.

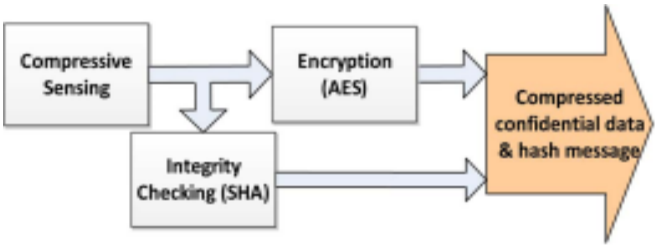


Fig. 3 : Encompression based on compressive sensing

An encompression scheme is shown in Fig. 3 [17]. The advanced encryption standard (AES) is used as the symmetric cipher and for integrity checking the secure hash algorithm (SHA) is used. The hash algorithm must be applied on the plaintext, because without knowing the AES secret key intruders cannot generate encrypted data whose plaintext matches the hash output. If it is applied on the encrypted data, and if intruders have knowledge of the hash function used they can hash and send random spurious data .

The programmer proximity to the WIMD can be checked by many ways one way is to pairing and key agreement. By using one can easily detect the programmers’ proximity to the WIMD. An authorized programmer can be pair with the WIMD using a secret cryptographic key. The key agreement can be done between only the programmer and the authenticate patient only, security can be increased by allotting patient with the security device for trusted authentication.

For making key agreement many methods are used like intra-body key distribution. In this type acoustic and magnetic broadcasting is used. In another type physiological values are used for generating keys. There are several well-known proposed methods for key generation but, none of the cryptographic key generation method is fully secure [6]. Thus, a secure WIMD access control methods remains topic for further research.

B. *Network Coding:*

Implementing network coding in the WBAN can also increase its reliability. In early years network coding, cooperative communication, and cooperative network coding is used for improving WBAN reliability, out of these coding schemes Cooperative Network Coding (CNC) Fig.4 configuration with MIMO system is the more reliable coding technique. As in this technique N number of sensors, R number of relays and S number of sinking nodes are used, hence the packet drop rate is decreased, and throughput as well as reliability of the WBAN network is increased. Packet failure rate is decreased and also the system provides its best performance during node failure situations.[7]

ISSN: 2278 – 909X

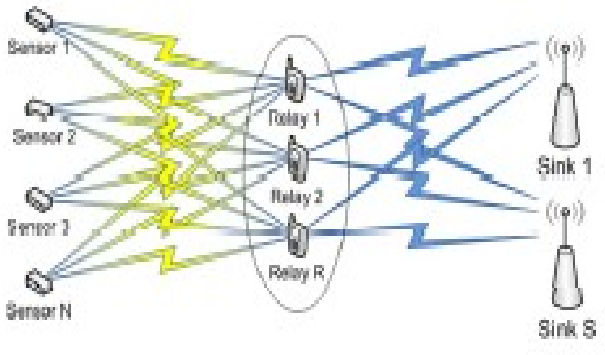


Fig. 4 Cooperative Network Coding Model for WBANs [7]

C. Radio Communication:

For increasing data confidentiality a radio design can be used which can isolate the WIMDs from outside attacks. This design can jam WIMDs messages and decode them itself and blocks unauthorized access to the WIMDs. It also protects WIMDs from unauthorized commands that can make them life critical [5]. Many approaches have been evaluated for WBAN reliability. Various wireless technology and platforms are considered in [8] for investigating performance of WBSN. A ZigBee based WBAN network is made with number of sensors are evaluated their performance in home as well as in the laboratory [8].

a) Wearable Devices

For preserving battery power, trusted external device can be used to verify incoming requests, this device can be easily recharged. A Communication Cloaker is used in [11], which is wearable device. It is used as a communication mediator between the IMD and preauthorized parties. This ignores incoming communications from all unauthorized programmers. In its absence or damage, the IMD accepts and responds to all incoming communications. In emergency situations, in order to access the IMD, the medical staff can remove the Cloaker. This approach can protect the IMD against battery-draining attacks, as computation burden is transferred to the external device

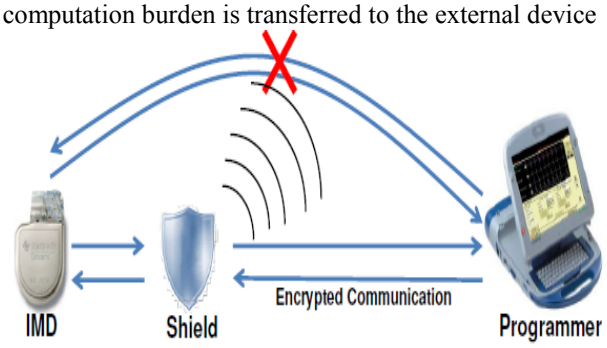


Fig.5 : Protecting an IMD without modifying it [9]

b) External devices

A "shield," is described in [9] is also used as an external device. It is illustrated in Fig. 5 it is used between the IMD and external device. At the same time it receives and jams IMD messages. It encrypts the received messages and sends it to the valid programmer. By avoiding direct communication with external devices shield protects the IMD from unauthorized incoming commands. All commands are encrypted and sent to the shield and then only genuine commands are directed towards IMD. For proper functioning of the shield, all the programmers needs to change their programs but there is no change in IMDs. Shield also provides confidentiality between IMD and the programmer. Fig.6 indicates the jammer cum receiver design for the shield.

A medical security monitor (MedMon), is proposed in [5], it snoops on all wireless communications to and from medical devices. It uses anomaly detection to identify malicious transactions. For detection of anomalies physical characteristics of the transmitted signal are used.

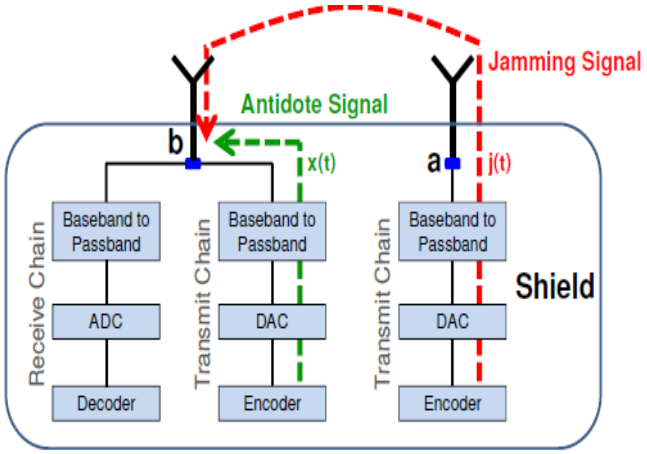
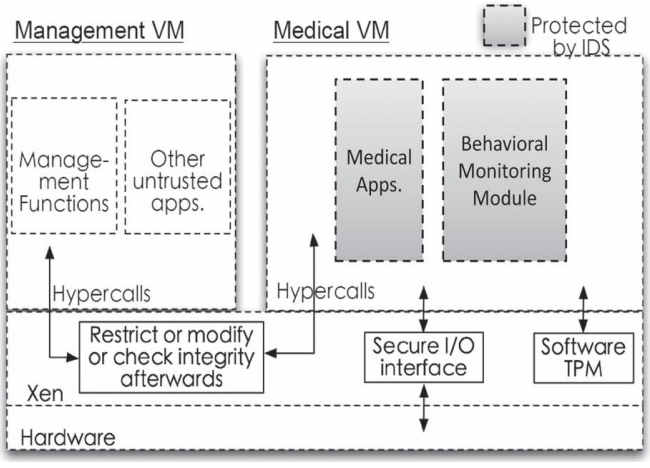


Fig. 6: The jammer cum receiver design [9]

D. Secure Execution Environment :

In WBAN we cannot provide security to all the applications but we can provide secure execution environment to the selected applications as shown in Fig.7 . It is based on two key technologies: secure virtualization and trusted computing. These applications can be protected in a separate virtual machine (VM), which we refer to as the medical VM. It is a restricted environment in which only medical applications with the supporting software libraries can executed by isolating the application from the other applications running on the system [18]. For providing secure execution environment we need to provide logical or physical separation, so that the important application can be isolated and can be provided with high security. The critical codes and less sensitive applications codes can be run on the same processor but isolated by additional software or hardware support.



ISSN: 2278 – 909X

Fig. 7: Secure Medical environment for medical applications

This isolation of medical software does not always provide security against vulnerabilities introduced in the software. For providing security against vulnerabilities Intrusion Detection Techniques (IDT) are used. Using a large set of inputs applications tested in the virtual environment. If the outputs are reliable then its test model is created, which is having a reliable data set. The user inputs are also tested against the developed model and if required changes can be made in the design.

A more powerful approach is to completely separate health-related applications from untrusted applications/ OS by making the hub an independent device. One such wrist-worn device, called Amulet (Fig. 8), is proposed in [12]. Amulet is dedicated to communications with IWMDs. It occasionally communicates with the smartphone in order to connect with health servers.

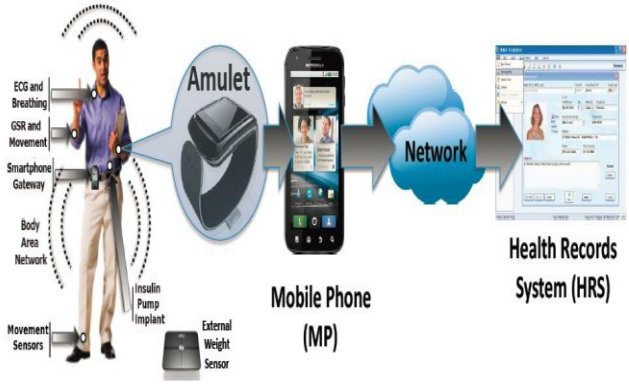


Fig. 8 : Dedicated wrist-worn device as the hub

E. *Runtime Monitoring:*

Software runtime monitor is shown in Fig.9 in which the application is first tested by running against a large data set in a virtualized environment. After passing the test, its behavioral models are generated, which can be seen as a database of good behaviors. Important user-defined policies can also be. At the user end application behavior restricts within the database of good behaviors. Any deviation is detected as an anomaly. As much of the workload is shifted from the user to the testing end, the performance penalty is greatly reduced compared to rigorous runtime checking.

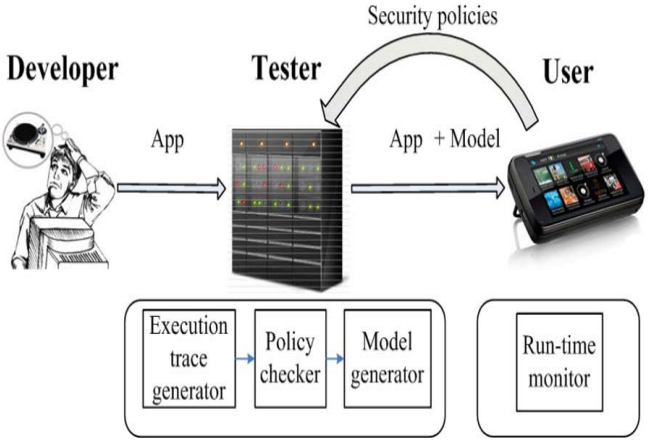


Fig. 9: Software runtime monitor.

IV. CONCLUSION

WBAN provides us with greater functionalities using WIMDs, but these devices are becoming more and more complex. As the WIMDs wireless applications are increasing their security becomes the concern as these devices are attached to the network or cloud. Many years the researchers are working on the security and reliability of the WIMDs but still the trustworthiness of these devices is not reached at the acceptable level. The researchers and the medical device manufactures should come together to find the trustworthy solution on these devices.

Table II shows the comparison of the approaches used for improving security, privacy, and reliability of the medical devices. The parameters that are taken into consideration for comparison of the approaches are vital sign type, Location of body, transmission method, access point for WLAN, security, privacy, and scalability. From the table we can conclude that Life guard and Code blue provides the security, privacy and reliability to the WBAN, but the other approaches lags in fulfilling the required characteristics.

TABLE II

SUMMERY OF THE APPROACHES USED FOR IMPROVING SECURITY, PRIVACY, AND RELIABILITY OF THE MEDICAL DEVICES.

	Life-Guard [19]	Code-Blue [21]	Med-Mon [5]	Wrist-Care [20]	Medisn [22]	Amulet [12]	IMD- Shield [6]
Vital Sign Type	Multiple	Multiple	Multiple	Single	Multiple	Multiple	Multiple
Location for Body	Wearable	Wearable	External	Wearable	Wearable	Wearable	External
Transmission method	Bluetooth	ZigBee	USRP	868 MHz ISM Band	ZigBee	Bluetooth	400 MHz MICS band
Access point for WLAN	Laptop	PDA or laptop	Laptop	Base Station	Base Station	Mobile Phone	PDA or Laptop

ISSN: 2278 – 909X

Security	Yes	Yes		Yes	Yes	Yes	
Privacy	Yes	Yes	Yes			Yes	Yes
Scalability	Yes	Yes		Yes	Yes		

REFERENCES

[1] Meng Zhang, Anand Raghunathan, and Niraj K. Jha,, "Trustworthiness of Medical Devices and Body Area Network", Proceedings of the IEEE Vol. 102, No. 8, August 2014, pp-1174-1188

[2] Chunxiao Li, Anand Raghunathan, and Niraj K. Jha, ''Improving the trustworthiness of medical device software with formal verification methods,'' IEEE Embedded Syst. Lett., vol. 5, no. 3, pp. 50–53, Sep. 2013.

[3] Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks", presented at IEEE conference, Publication Year: 2014 , pp: 524 – 539

[4] D. Kune , ''Ghost talk: Mitigating EMI signal injection attacks against analog sensors,'' in Proc. IEEE Symp. Security Privacy, pp-145-159,May 2013.

[5] Meng Zhang, Anand Raghunathan, and Niraj K. Jha, ''MedMon: Securing medical devices through wireless monitoring and anomaly detection,'' IEEE Trans. Biomed. Circuits Syst., vol. 7, no. 6, pp. 871–881, Dec. 2013.

[6] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, ''IMDGuard: Securing implantable medical devices with the external wearable guardian,'' in Proc. IEEE Int. Conf. Comput. Commun., Apr. 2011, pp. 1862–1870.

[7] Prathamesh Dinkar, Abhishek Gulavani, Sourabh Ketkale, Pratik Kadam, Sheetal Dabhade ,"Remote Health Monitoring using Wireless Body Area Network", (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013, pp-399-402.

[8] Changhong Wang , Qiang Wang ; Shunzhong Shi, "A Distributed Wireless Body Area Network for Medical Supervision", (I2MTC), 2012 IEEE International, 13-16 May 2012 , pp- 2612 - 2616

[9] Shyamnath Gollakota † Haitham Hassanieh† Benjamin Ransford⋆ Dina Katabi† Kevin Fu⋆ ,''They can hear your heartbeats: Non-invasive security for implantable medical devices,'' in Proc. ACM Conf. Special Interest Group Data Commun., Aug. 2011.

[10] Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta,"PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE Transactions On Information Technology In Biomedicine, VOL. 14, NO. 1, JANUARY 2010

[11] T. Denning, Kevin Fu, Tadayoshi Kohno,''Absence makes the heart grow fonder: New directions for implantable medical device security,'' in Proc. Conf. Hot Topics Security, Jul. 2008, pp. 1–7.

[12] Jacob Sorber, Minho Shin† , Ronald Peterson, Cory Cornelius, Shrirang Mare, Aarathi Prasad, Zachary Marois, Emma Smithayer, David Kotz ,''An amulet for trustworthy wearable mHealth,'' in Proc. Workshop Mobile Comput. Syst. Appl., 2012, pp. 7:1–7:6.

[13] Osman Salem, Yaning Liu, Ahmed Mehaoua, and Raouf Boutaba ,"Online Anomaly Detection in Wireless Body Area Networks for Reliable Healthcare Monitoring", *IEEE Journal Of Biomedical And Health Informatics*, VOL. 18, NO. 5, SEPTEMBER 2014

[14] Bhargavi B. Dalal, Ms. Smita Jangale., "Security Requirements and Solution in Wireless Body Area Network (WBAN)" *VESIT , International Technological Conference-2014 (I-TechCON), Jan. 03 – 04, 2014*

[15] M. Patel , Jianfeng Wang, "Applications, Challenges, And Prospective In Emerging Body Area Networking Technologies," *IEEE Wireless Communications, Feb. 2010, pp-80-88*

[16] Gabriel E. Arrobo , Richard D. Gitlin, "Improving The Reliability Of Wireless Body Area Networks", *33rd Annual International Conference of the IEEE EMBS ,pp-2192-2195, Aug- 2011*

[17] M. Zhang, Mehran Mozaffari Kermani, Anand Raghunathan, Niraj K. Jha , ''Energy-efficient and secure sensor data transmission using encompression,'' in Proc. Int. Conf. VLSI Design, Jan. 2013, pp. 31–36.

[18] Trusted Computing Group. [Online]. Available: https://www.trustedcomputinggroup.org

[19] K. Montgomery et al., "Lifeguard- A Personal Physiological Monitor For Extreme Environments", *IEEE International Conference*, pp-2192-2195, 2004

[20] Pervasive Computing Healthcare [Online] Available: https://books.google.co.in/books?id=TWDLBQAAQBAJ&pg….

[21] David Malan , Thaddeus Fulford-Jones , Matt Welsh , and Steve Moulton,"CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004), June, 2004

[22] Jeonggil Ko, Jong Hyun Lim, Yin Chen, Razvan Mus Aloiu-E., Andreas Terzis And Gerald M. Masson, "MEDiSN: Medical Emergency Detection in Sensor Networks", *ACM Transactions on Embedded Computing Systems (TECS) TECS Homepage archive* Volume 10 Issue 1, August 2010

ISSN: 2278 – 909X

Sunita N. Karande received the B.Tech. degree in Electronics Engineering from Yashvantrao Chavan Maharashtra Open University, Nashik, India in 2010. She is currently doing post-graduation in Electronics and Telecomm, Engineering from Mumbai University, Airoli, Navi Mumbai, India. Her current research interests include wireless sensor networks, and ad hoc networks.

Govindkumar B. Lohiya received the M.E. degree in Electronics Engineering from Shri Guru Gobind Singhji Institute of Engineering and Tech., Nanded. He is currently an Assistant Professor in Electronics Engineering Department, at Datta Meghe College of Engineering, Mumbai University, Airoli, Navi Mumbai, India. His current research interests include Embedded Systems, and Networks.

ISSN: 2278 – 909X