ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

A Secure IoT-Based Modern Healthcare System Using Body Sensor Network

Kavitha.Y[1], Lavanya.M[2], Mounika.A[3], Sasirekha.K[4], N.Vigna Vinod Kumar[5]

UG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[1,2,3,4]

Assistant Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India. [5]

ABSTRACT: Advances in information and communication technologies have led to the emergence of Internet of Things (IoT).In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients since they are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management). The body sensor network (BSN) technology is one of the core technologies of IoT developments in healthcare system, where a patient can be monitored using a collection of tiny-powered and lightweight wireless sensor nodes. However, development of this new technology in healthcare applications without considering security makes patient privacy vulnerable. In this article, at first we highlight the major security requirements in BSN based modern healthcare system. Subsequently, we propose a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those requirements.

KEYWORDS: BSN, Data privacy, Data integrity, Authentication

I.INTRODUCTION

The last few decades have witnessed a steady increase in life expectancy in many parts of the world leading to a sharp rise in the number of elderly people. A recent report from United Nations [1] predicted that there will be 2 billion (22% of the world population) older people by 2050. In addition, research indicates that about 89% of the aged people are likely to live independently. Accordingly, providing a decent quality of life for aged people has become a serious social challenge at that moment. The rapid proliferation of information and communication technologies is enabling innovative healthcare solutions and tools that show promise in addressing the aforesaid challenges. Now, Internet of Things (IoT) has become one of the most powerful communication paradigms of the 21th century. In the IoT environment, all objects in our daily life become part of the internet due to their communication and computing capabilities (including micro controllers, transceivers for digital communication). IoT extends the concept of the Internet and makes it more pervasive. IoT allows seamless interactions among different types of devices such as medical sensor, monitoring cameras, home appliances so on. [2], [3]. Because of that reason IoT has become more productive in several areas such as healthcare system. In healthcare system, IoT involves many kinds of cheap sensors (wearable, implanted, and environment) that enable aged people to enjoy modern medical healthcare services anywhere, any time. Besides, it also greatly improves aged peoples quality of life.The body sensor network (BSN) technology [4] is one of the most imperative technologies used in IoT-based modern healthcare system. It is basically a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surrounding environment. Since BSN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, accordingly, they require strict security mechanisms to prevent malicious interaction with the system.

In this article, at first we address the several security requirements in in BSN based modern healthcare system. Then, we propose a secure IoT based healthcare system using BSN, called BSN-Care, which can guarantee to efficiently accomplish those requirements. Therefore, the rest of the article is organized as follows. In Section II, we describe some of the related works in IoT based healthcare system using BSN. In Section III, we present our BSN-Care system and subsequently, in this section, we also so show how to enforce security in our BSN-Care

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

model to achieve all the imperative security properties. In Section IV, we shown the experimental results. Finally, a concluding remark is given in Section V.

II.RELATED WORK

The advancement of BSN in healthcare applications have made patient monitoring more feasible. Recently, several wireless healthcare researches and projects have been proposed, which can aim to provide continuous patient monitoring, in-ambulatory, in-clinic, and open environment monitoring (e.g. athlete health monitoring). This section describes few popular research projects about healthcare system usingbody sensor networks.CodeBlue [5-6] is a popular healthcare research project based on BSN developed at Harvard Sensor Network Lab. In this architecture, several bio-sensors are placed on patient's body. These sensors sense the patient body and transmit it wirelessly to the end-user device (PDAs, laptops, and personal computer) for further analysis. The basic idea of the CodeBlue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a published and subscribed architecture. Besides, CodeBlue's authors acknowledge the need of security in medical applications, but until now security is still pending or they intentionally left the security aspects for future work.Subsequently, a heterogeneous network architecture named Alarm-net was designed at the university of Virginia [7]. The research is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consist of body sensor networks and environmental sensor networks. Besides, the authors have developed a circadian activity rhythms program to aid context aware power management and privacy policies. Furthermore, Alarm-net facilitates network and data security for physiological, environment, behavioral parameters about the residents. However, Wood et al. [7] have pointed out some confidentiality infringement scenarios on Alarm-net, such as the fact it is susceptible to adversarial confidentiality attacks, which can leak resident's location; refer to [8] for details. Meanwhile, Ng et al. another BSN based healthcare system UbiMon [9] was proposed in the department of computing, Imperial College, London. The aim of this project was to address the issues related to usage of wearable and implantable sensors for distributed mobile monitoring. AlthoughNg et al. proposed and demonstrated the ubiquitous healthcare monitoring architecture, it is widely accepted that without considering the security for wireless healthcare monitoring, which is a paramount requirement of healthcare applications, according to government laws [10]. In 2006, Chakravorty designed a mobile healthcare project called MobiCare [11]. MobiCare provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of the patients physiological status.Although, Chakravorty acknowledged the security issues in MobiCare, but only addressing security issues are not sufficient for real-time healthcare applications. Thus, security and privacy is still not implemented in MobiCare healthcare monitoring or may have been left out for future work. Nevertheless, there are many security issues such as secure localization, anonymity, etc, have not even mentioned in MobiCare system. Recently, a new system designed at Johns Hopkins University named Median, especially designed for patient's monitoring in hospital and during disaster events was reported[12]. It comprises multiple physiological monitors (called PMs), which is battery powered motes and equipped with medical sensors for collecting patients' physiological health information's (e.g. blood oxygenation, pulse rate, etc.). In their description of Median its author acknowledged the need for encryption for PMs, however they did not mention which crypto-system has been used for data privacy and how they have checked the integrity of the received data. Thus, although the authors included some of the security properties to Median, their study did not reveal much information about their security implementation. Sometimes an image may contain text embedded on to it. Detecting and recognizing these characters can be very important, and removing these is important in the context of removing indirect advertisements, and for aesthetic reasons.

III. SECURE IOT-BASED HEALTHCARE SYSTEM USING BSN (BSN-CARE)

Body Sensor Network (BSN) allows the integration of intelligent, miniaturized low-power sensor nodes in, on or around human body to monitor body functions and the surrounding environment. It has great potential to revolutionize the future of healthcare technology and attained a number of researchers both from the academia and industry in the past few years. Generally, BSN consists of in-body and on-body sensor networks. An in-body

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

sensor network allows communication between invasive/implanted devices and base station. On the other hand, an on-body sensor network allows communication between non-invasive/wearable devices and a coordinator. Now, our BSN-Care (Fig. 1) is a BSN architecture composed of wearable and implantable sensors. Each sensor node is integrated with biosensors such as Electrocardiogram (ECG), Electromyography (EMG), Electroencephalography (EEG), Blood Pressure (BP), etc. These sensors collect the physiological parameters and forward them to a coordinator called Local Processing Unit (LPU), which can be a portable device such as PDA, smart-phone etc. The LPU works as a router between the BSN nodes and the central server called BSN-Care server, using the wireless communication mediums such as mobile networks 3G/CDMA/GPRS. Besides, when the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors. For example, in general BP less than or equal to 120 is normal, when the BP of the person reaches say 125, the LPU will provide a buzzer sound.When BSN-Care server receives data of a person (who wearing several bio sensors) from LPU, then it feeds the BSN data into its database and analyzes those data.We can continuously monitor the patient when go out of hospital through mobile. We divide the all security requirements (mentioned above) into two parts: network security, and data security. Network security comprises authentication, anonymity, and secure localization. On the other hand, data security includes data privacy, data integrity. Now, to the best of the knowledge there is no two-party authentication protocol which can achieve all the aforesaid properties of the network security. Hence, in order to achieve all the network security requirements here we propose a lightweight anonymous authentication protocol. Subsequently, to accomplish all the data security requirements we adopt OCB authenticated encryption mode.

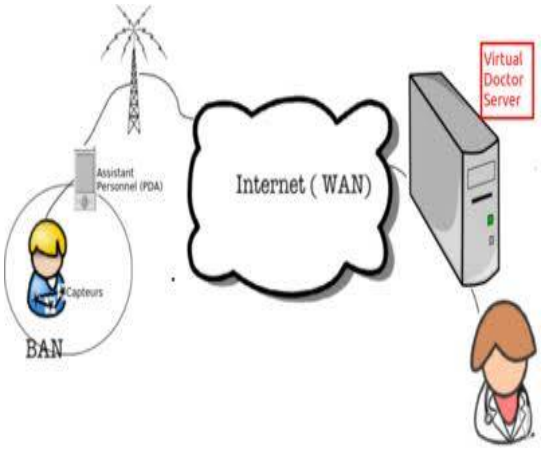

Figure 1.Overall view of BSN Care system using IoT

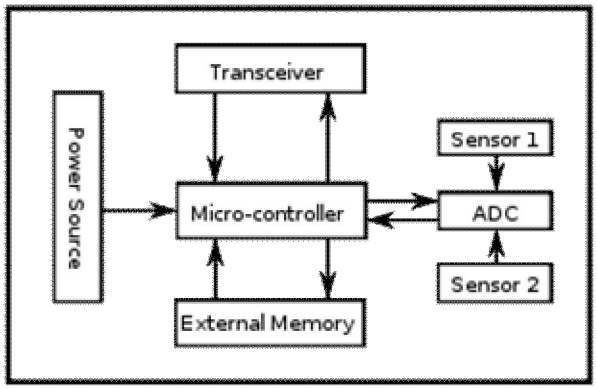

Figure 2.Structure of BSN Network

IV.EXPERIMENTAL RESULTS

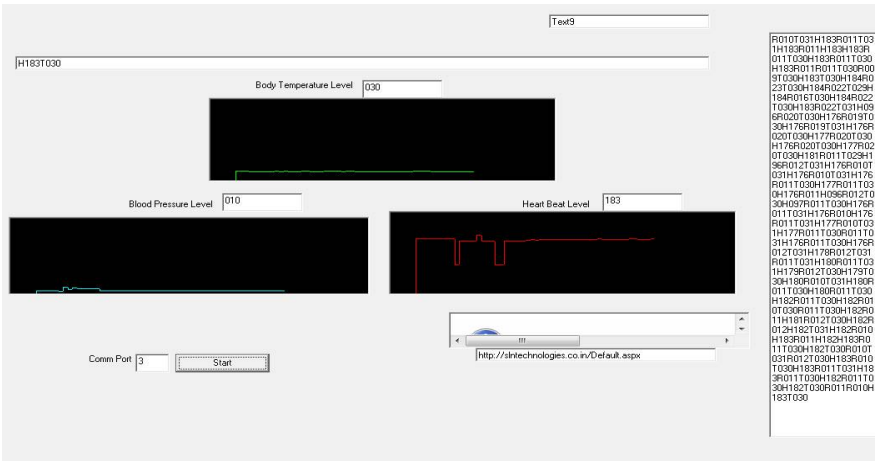

Figure 3.Monitering Patient Health Conditions

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

Figure 4.Mobile monitoring using IoT

V. CONCLUSION

In this article, at first we have described the security and the privacy issues in healthcare applications using body sensor network (BSN). Subsequently, we found that even though most of the popular BSN based research projects acknowledge the issue of the security, but they fail to embed strong security services that could be preserve patient privacy. Finally, we proposed a secure IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish various security requirement of the BSN based healthcare system.

REFERENCES

[1] UN,"World Population Aging 2013," 2013, pp. 8–10.
[2] P. Gope, T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sensors Journal, Vol. 15 (9), pp. 5340 – 5348, 2015.
[3] P.Gope, T.Hwang, "A Realistic Lightweight Authentication Protocol Preserving Strong Anonymity for Securing RFID System," Computers & Security (Elsevier Journal), Vol. 55, pp. 271–280, 2015.
[4] P. Kumar,and H. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey." Sensors (Basel, Switzerland) 12.1 (2012): pp. 55–91.
[5] D. Malan, T. F. Jones, M. Welsh,S. Moulton, "CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care," Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004); Boston, MA, USA. 6–9 June 2004.
[6] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shayder, G. Mainland, M. Welsh, "Sensor Networks for Emergency Response: Challenges and Opportunities", Pervas. Comput. vol.3, pp.16–23, 2004.
[7] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He , S. Lin, J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Department of Computer Science, University of Virginia; Charlottesville, VA, USA: 2006. Technical Report CS-2006-01;
[8] S. Pai, M. Meingast, T. Roosta, S. Bermudez, S. Wicker, D. K. Mulligan , S. Sastry, "Confidentiality in Sensor Networks: Transactional Information," IEEE Security and Privacy Magazine. 2008
[9] J.W.P. Ng, B.P.L Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)," Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp'04); Nottingham, UK. 7–14 September 2004.
[10] Office for Civil Rights, United State Department of Health and Human Services Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. Available online: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/inde x.html (accessed on 15 June 2011).
[11] R. Chakravorty, "A Programmable Service Architecture for Mobile Medical Care," Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06); Pisa, Italy. 13–17 March 2006.
[12] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E, A. Terzis, G. M. Masson, "Median: Medical Emergency Detection in Sensor Networks," ACM Trans. Embed. Comput. Syst. vol. 10, pp. 1–29, 2010.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

[13] P. Rogaway, M. Bellare, and J. Black. OCB: A block–cipher mode of operation for efficient authenticated encryption. ACM Transactions on Information and System Security (TISSEC) 6 (3) pp. 365–403,2003.
[14] T. Hwang, P. Gope, Provably Secure Mutual Authentication and Key Exchange Scheme for Expeditious Mobile Communication Through Synchronously One-Time Secrets. Wireless Personal Communications 77(1), pp. 197-224, 2014.
[15] P. Gope, T. Hwang, "Enhanced secure mutual authentication, and key agreement scheme preserving user anonymity in global mobile networks," Wireless Personal Communications, DOI: 10.1007/s11277- 015-2344-z, 2015.
[16] Oracle Technology Network, "Java Cryptography Architecture", (JCA), http://docs.oracle.com/javase/6/docs/technotes/guides/crypto/CrypoSpec.html.
[17] A. Kumar et al., "Caveat eptor: A comparative study of secure device pairing methods," IEEE International Conference on Pervasive Computing and Communications, 2009. PerCom 2009.
[18] P. Gope, T. Hwang, "Lightweight and Energy Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks," IEEE Systems Journal, DOI: 10.1109/JSYST.2015.2416396, 2015.
[19] T. Hwang, P. Gope, "IAR-CTR and IAR-CFB: Integrity Aware Real-time Based Counter and Cipher Feedback Modes," Security and Communication Networks (Wiley Journal), DOI: 10.1002/sec.1312,
2015.