ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Secured body Sensor healthcare Monitoring System for Elderly Peoples

Jahnavi V [1], P Kokila[2], Shruthi T S [3], SamradhaRao[4], Sujan Kumar [5]

UG Student, Department of ISE, The Oxford College of Engineering, Bommannahalli, Bengaluru, India[1]

Assistant Professor, Department of ISE, The Oxford College of Engineering, Bommannahalli, Bengaluru, India[2]

UG Student, Department of ISE, The Oxford College of Engineering, Bommannahalli, Bengaluru, India[3]

UG Student, Department of ISE, The Oxford College of Engineering, Bommannahalli, Bengaluru, India[4]

UG Student, Department of ISE, The Oxford College of Engineering, Bommannahalli, Bengaluru, India[5]

ABSTRACT: The Internet of Things (IoT) has not been around for very long. Advances in information and communication technologies have led to the emergence of internet of things. The Internet of Things had evolved into a system using multiple technologies, ranging from the Internet to wireless communication. The usage of IoT technologies brings convenience of physicians and patients, since they are applied to various medical areas. The recent advances in wireless sensor networks and embedded computing technologies, miniaturized pervasive health monitoring devices have become practically feasible. 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. In addition to that of monitoring and analysis of physiological parameters, the recently proposed Body Sensor Networks (BSN) incorporates context aware sensing for increased sensitivity and specificity, but development of the body sensor network (BSN) technology in healthcare applications without considering security makes patient privacy vulnerable. At the specification, we mainly concentrate on the major security requirements in BSN-based modern healthcare system. Subsequently, the propose of a secure IoT-based healthcare system using BSN called BSN-Care, in which it can efficiently accomplish the security 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 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. However, medical research surveys found that about 80% of the aged people older than 65 suffers from at least one chronic disease causing many aged people to have difficulty in taking care of themselves. 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.

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. 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 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

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. Propose of a secure IoT based healthcare system using BSN, called BSN-Care, which can guarantee to efficiently accomplish those requirement.

II. LITERATURE SURVEY

David Malan et al [1] propose the completion of an initial design of CodeBlue and prototypes of several of the components described herein. The pulse oximetry method has been completed and development of an ECG mote is currently underway. The use of an adaptive spanning-tree multi-hop routing algorithm, based on the Tiny OS Surge protocol, and the incorporation of a dynamic transmission power scaling to minimize interference. A lightweight public key infrastructure based on elliptic curve cryptography is currently being tested. A sophisticated programming model using abstract regions for routing, data sharing, and aggregation has also been developed. The disadvantages are i) Communication challenges: The first challenge is secure, reliable, ad hoc communication among groups of sensors and mobile, handheld devices. ii) Computational challenges: Sensor nodes have very limited computational power, and traditional security and encryption techniques are not well-suited to this domain.

Jason W.P.Ng et al [2] describes the ubiquitous monitoring system is presented for continuous monitoring of patients under their natural physiological states. The system provides the architecture for collecting, gathering and analyzing data from a number of biosensors. Particularly, the concept of BSN node is implemented which could form the basis for wireless intelligent modules for wearable and implantable sensors. In addition to the physiological parameters, the context awareness aspect is also included in the system to enhance the capturing of any clinical relevant episode. The demerit is the issues in the development of wearable/implantable sensors in BSN

Sideny Katz et al [3] propose the Index was originally derived from observations of old people with fracture of the hip, it was necessary to determine whether it could be applied to others as well. Observations of 1,001 individuals, to date, supported the original finding of an ordered relationship and demonstrated wide applicability. Of the 1,001 people, 96% could be classified by the Index (Table 3). Ninety per cent were 40 years old or older, and more than 60% were 60 or over. Most had more than one chronic disease. The primary clinical diagnoses associated with ADL disability were: fracture of the hip (250 persons), cerebral infarction (239), multiple sclerosis (138), arthritis (60), malignancy (30), cardiovascular dis¬ ease exclusive of cerebral infarction (38), and amputation, paraplegia, or quadriplegia (67). In 38 other patients, the diagnoses were: cerebral palsy, Parkinson's disease, amyotrophic lateral sclerosis, peripheral neuropathy, or other neurological disease. Less commonly, primary diagnoses included such chronic diseases as asthma, emphysema, diabetes, blindness, cirrhosis, alcoholism, malnutrition, and obesity.The problem is they are not able to keep the track of chronic diseases.

Rajiv Chakravorty et al [4] describes the vast opportunity in the ‘point-of-care’ access and the capture and transmission of patient information will continue to drive the healthcare industry towards increased mobility. The importance is in the shifting awareness that mobility in healthcare settings increasingly refers to – the mobility of sensor/actuator devices, the healthcare providers (health ‘outsourcing’) and of the patient (users) themselves. MobiCare leverages the point-of-care patient access to offer important benefits like quality healthcare, a programmable service architecture, flexible service composition and a full-scale medical systems integration. MobiCare is an ongoing project and much work remains to be done. Besides a proof-of-concept prototype, there is a process of investigating other long-term, challenging research problems in MobiCare including the body sensor network security, reliable and secure sensor code updates and upgrades, the potential legal hurdles involved and the privacy issues that arise with dynamic remote code updates. The disadvantage is it is not reliable and secure.

Arun Kumar et al [5] elaborates the presentation of the first experimental evaluation of prominent device pairing methods. Results show that some simple methods (e.g., Visual Number and Image Comparison) are quite attractive overall, being fast and secure as well as acceptable by users. They naturally appeal to settings where devices have appropriate-quality displays. HAPADEP variant seems to be preferable for more constrained devices: it is fast, error-free and requires very little user intervention. LED Button or Vibrate-Button are best-suited for devices lacking screens, speakers and microphones. The demerit is user evaluation for each method is not yet done.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

III. PROPOSED METHODOLOGY AND DISCUSSION

A. METHODOLOGY

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. Generally, BSN consists of in-body and on-body sensor networks. An in-body 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. Each sensor node is integrated with bio-sensors such as blood pressure sensor, motion sensor, ECG etc.

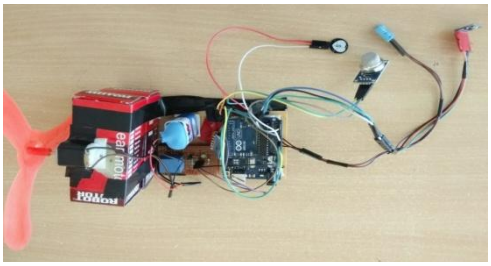

Fig.1: Hardware connections

i. Data Collection

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. When the LPU detects any abnormalities then it provides immediate alert to the person that wearing the bio-sensors. When the 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. Subsequently, based on the degree of abnormalities, it may interact with the family members of the person, local physician, or even emergency unit of a nearby healthcare center.

ii. Lightweight Anonymous Authentication Protocol

The division of 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, and data freshness. 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 a lightweight anonymous authentication protocol is used. Subsequently, to accomplish all the data security requirements we adopt OCB authenticated encryption mode.

In BSN-Care system, when a LPU wants to send the periodical updates to BSN-Care server, then the server needs to confirm the identity of LPU using a lightweight anonymous authentication protocol. In this section we describe our anonymous authentication protocol in details. The proposed authentication protocol consists of two phases: In Phase 1, the BSN-Care server issues security credentials to a LPU through secure channel, this phase is called registration phase. The Phase 2 of the proposed authentication protocol is the anonymous authentication phase, where before data transmission from the LPU to BSN-Care server, both the LPU and the server will authenticate each other. So, the objective of our proposed lightweight authentication scheme is as follows:

- To achieve mutual authentication property.
- To achieve anonymity property.
- To achieve secure localization property.
- To defeat forgery attacks.
- To reduce computation overhead.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

IV. RESULT ANALYSIS

In the proposed work the Sensors are used to monitor elder people's body status and surrounding environment. The Elder people can be in touch with the family, doctor or care taker from remote place. During abnormal condition Automatic alert is sent to the family, doctor or care taker and automatic Control of the home appliances is achieved based on the body condition.

The data are collected using different sensors fig.1. The fig.2 describes the data stored in Android application, where P represent the Pulse, T represent Temperature, AS represent movement of object and CO represent the gas level of the environment. The predefined threshold level is fixed for pulse, temperature and toxic gas of the surrounding, if the values of any one of the mentioned point crosses the threshold value immediately message will be sent to the doctor, family members and to nearby hospital along the patient name, contact number and location as shown in fig.3

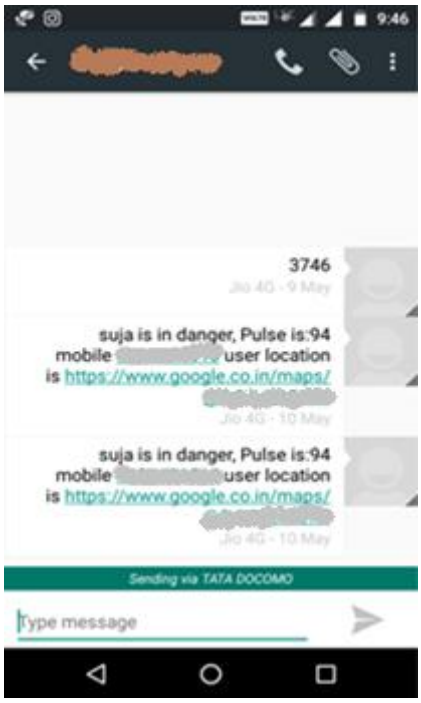

Fig.2: Data Stored In Android App

Fig.3: Message Intimation

.

V. CONCLUSION

The security and the privacy issues in healthcare applications using body sensor network (BSN). Subsequently, 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, the proposed system has a secured IoT based healthcare system using BSN, called BSN-Care, which can efficiently accomplish various security requirements of the BSN based healthcare system.

REFERENCES

[1] David Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue: An ad hoc sensor network infrastructure for emergency medical care," in Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES), Boston, MA, USA, Jun. 2004, pp. 1–8.
[2] Jason W. P. Ng et al., "Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon)," in Proc. 6th Int. Conf. Ubiquitous Comput. (UbiComp), Nottingham, U.K., Sep. 2004, pp. 1–2.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

[3] R. Weinstein, "RFID: A technical overview and its application to the enterprise," IT Prof., vol. 7, no. 3, pp. 27–33, May/Jun. 2005.
[4] R. Chakravorty, "A programmable service architecture for mobile medical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput.Commun. Workshop (PERSOMW), Pisa, Italy, Mar. 2006, pp. 531–536.
[5] A.kumar,N.Saxena,G.Tusdik"Caveateptor:A comparative study of secure device pairing methods",inProc.IEEEInt.Conf Pervasive Comput.commun(Per Com),Mar.20009.pp.1-10
[6] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Sep. 2015.
[7] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Comput.Secur., vol. 55, pp. 271–280, Nov. 2015.
[8] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2012.
[9] K. Lorincz et al., "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Comput., vol. 3, no. 4, pp. 16–23, Oct./Dec. 2004.
[10] A. Wood et al., "ALARM-NET: Wireless sensor networks for assistedliving and residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-01, 2006.
[11] S. Pai et al., "Confidentiality in sensor networks: Transactional information," IEEE Security Privacy Mag., vol. 6, no. 4, pp. 28–35, Jul./Aug. 2008..
[12] Office for Civil Rights. United State Department of Health and Human Services Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. [Online].Available:http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index. html, accessed Jun. 15, 2011.
[13] R. Chakravorty, "A programmable service architecture for mobile medical care," in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput.Commun. Workshop (PERSOMW), Pisa, Italy, Mar. 2006, pp. 531–536.
[14] J. Ko et al., "MEDiSN: Medical emergency detection in sensor networks," ACM Trans. Embed. Comput. Syst., vol. 10, no. 1, pp. 1–29, Aug. 2010.