SECURE M-HEALTHCARE SYSTEM FOR PATIENT MONITORING

***S.P.Gavade , **S.S.Kulkarni**

**Student, ME (Computer), Computer Department*

***Associate Professor, Information Technology Department*

Sinhgad Academy of Engineering

Pune, India

ABSTRACT

Advances in sensors, wireless networks, and portable devices offer unique chances to deliver medical services and information at anytime anywhere. The concept of Wireless Body Sensor Network (WBSN) has been proposed to improve chronic disease management, patient care and support lifelong health and wellbeing for the ageing population. The increasing feasibility and facility of mobile healthcare has already introduced several significant challenges for patients, policy makers, hospitals, and healthcare providers. A major challenge is to provide continuous healthcare services to those patients who require it via wearable wireless medical devices. Also, many patients have privacy concerns when it comes to releasing their personal information over open wireless channels. As a result, the most important and challenging issues are how to secure the personal information of patients and how to eliminate their privacy concerns. In this paper, we present secure m-Healthcare system to impede the attacks faced by wireless communications in healthcare systems and improve the security of mobile healthcare.

Keywords- Wireless Body Sensor Networks, Mobile Healthcare System, Cryptography.

INTRODUCTION

In our aging society, mobile Healthcare (m-Healthcare) system has been developed as an important application of pervasive computing to provide remote health care monitoring to people who have chronic medical conditions such as heart disease, diabetes [1], [2], [3], [4], [5], [6]. Body sensor nodes and smart phones are utilized by m-Healthcare system to monitor people who have chronic medical conditions. On one hand, wireless devices and mobile networks allow medical professionals to operate in hands-free mode, while communicating with other colleagues in a hospital. On the other hand, wearable sensors enable m-healthcare users to have flexibility and mobility, making it possible for patients to be monitored at arbitrary times and places. This can prevent paroxysmal sickness even if patients are not in hospitals or nursing centers, and thereby patients are given maximum freedom while still receiving professional medical supervision. Both patients and paramedics can benefit from mobile healthcare (m-healthcare).

Therefore, the introduction of wireless and mobile technologies makes mobile electronic healthcare systems more realistic and feasible [4].

Security is important requirement for any communication environment. Real-time monitoring and data transmission not only provides necessary information quickly but also can expose a patient's medical data to malicious intruders or eavesdroppers. Medical information of the patients is highly sensitive data which needs data privacy but an m- healthcare system lacks the necessary protection when communicating data. During data transmission, the private data of a patient can easily access by unauthorized parties or persons and medical records may be modified freely by them, and false information can be injected into the data stream by a prohibited node. As a result, when planning mobile healthcare systems, security is indispensable because of the mobility of the patients, the shared nature of wireless devices, and the susceptibility of dynamic and pervasive environments [4].

Patient monitoring can be a vulnerable point due to important function of m-healthcare system through which an attacker may jeopardize the entire functioning of the system and even mislead medical professionals to make improper decisions. In this paper, we study the architecture of mobile healthcare system and show how current secure strategies are applied to achieve the security and privacy requirements.

BODY SENSOR NETWORKS

Body area network (BAN), is also called Body sensor networks (BSN) and wireless body area network (WBAN). Body sensor network (BAN) is an emerging technology in computer world and it plays very vigorous role in health services. It is being very popular in society because patient's data monitoring is a leading issue for disease and health management. BAN helps in monitoring patient's history in routine life activities to provide them accurate treatment. Health center can check the complete details of patients from remote location and can suggest a suitable medication.

Basically, this technology is used to reduce the load at hospitals and provide efficient healthcare facility to patients. To monitor the patients in their natural environments is not practical when devices or sensors are connected through a wire so that we use Wireless body area network (WBAN) to carrying out daily activities through unobtrusive and contented manner. Wireless communication mainly uses a point-to-point connection between sensors and a monitoring object to ensure a BSN's connectivity. Generally, a BSN consists of portable devices such as cellular phones, PDAs, and medical sensors, and uses wireless communication technologies such as General Packet Radio Service (GPRS), and Bluetooth. BAN uses IEEE802.15.4/Zigbee technology to detect and predict the human physiological states of restiveness, fatigue, and

stress. To acquire signals about EEG, ECG, EOG, and EMG different monitoring sensors are integrated and attach to a patient's body.

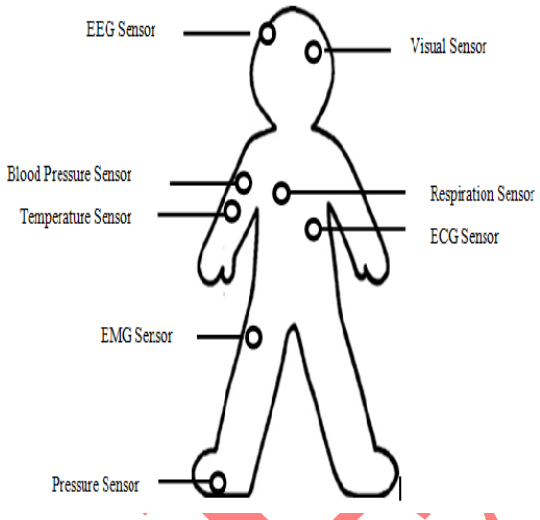

Figure 1.The Example of Body Sensor Networks

PATIENT MONITORING USING M -HEALTHCARE SYSTEM

In m-Healthcare system, each medical users personal health information (PHI) such as temperature, blood pressure, heart beat, and blood sugar level and others can be collected by BSN, and then transmitted to patient healthcare management center via Bluetooth technology or 3G network. Medical professionals at healthcare center can continuously monitor medical users' health condition based on collected PHI report. When medical professionals observe any medical emergency then they quickly react this situation by dispatching ambulance and doctor to an emergency location. Figure 2 illustrates m-healthcare architecture with patient monitoring devices and an emergency response center.

Real-time patient monitoring and data transmission pose the following challenges to mobile healthcare:

- The reliability of patient monitoring.
- The quality of patient monitoring.
- The energy management of patients' devices.
- Security of personal information of patient.

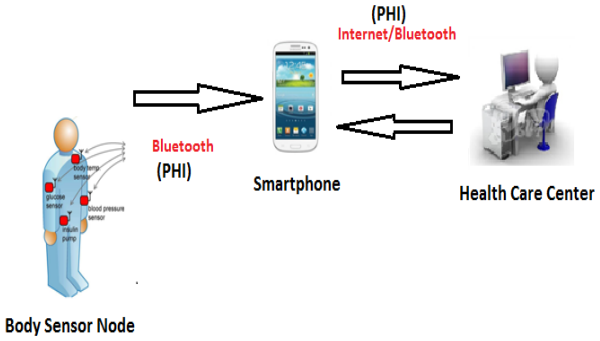

Figure 2. Architecture of m-Healthcare System

Due to these promising characteristics in improving health care quality, m-Healthcare system built on wireless body sensor network. However, the flourish of m-Healthcare system still hinges up the patient concerns, for example, the security issues of patient health condition information. In this paper, we will specifically focus on the security issues in m-Healthcare system. Patient's PHI is always considered being reported directly to the m-Healthcare center in m-Healthcare system, and the primary security issue is to keep the patient's PHI secret, and only the related medical professionals at m-Healthcare center can read them.

SECURITY AND PRIVACY

Undoubtedly, both wireless communication and biosensor technologies have provided a lot of benefits for mobile healthcare, but there are many concerns about security and privacy that need to be solved to protect the user's information. Typical concerns include how to protect the privacy of the patient, how to prevent the disclosure of a patient's data, and who should have the right to access the patient's medical record [4]. In particular, m-healthcare systems have open wireless links, mobile users, and shared resources, and this increases the difficulty of system security. Most current solutions uses cryptography to protect data confidentiality. Either asymmetric or symmetric key cryptography uses encryption and decryption to hide a patient's data. Symmetric keys, such as private key, or session key, secret key, are generally distributed to a user of m- healthcare when he/she registers in the system. Figure 3 shows the process of data encryption and decryption. There are a variety of keys in m- healthcare systems and it is critical to manage these keys so that they are not disclosed to unauthorized third parties or attackers.

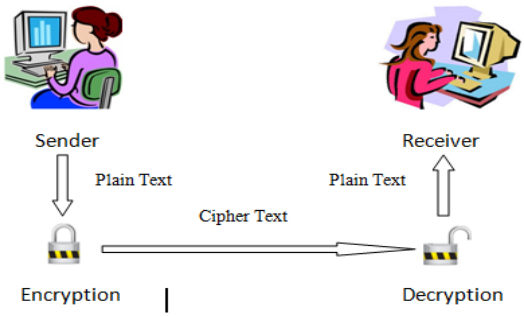

Figure 3.The encryption and decryption process of a patient's information.

A. *Secure M-Healthcare System*

In the system model, we consider a trusted authority (TA) and a group of *l* medical users U = *{*U_1, U_2, ・ ・ , U_l*}*, as shown in Fig .

1) Trusted Authority (TA):

TA is a trustable and powerful entity, and located at the m-Healthcare center. The duty of TA is in charge of the management of the whole m-Healthcare system such as initializing the m-Healthcare system, registering the patients at m-Healthcare center by equipping proper body sensor nodes and key materials to patients.

2) Medical Users U:

U ={U_1,U_2,⋯}are a group of registered patients, each patient $U_i \in U$ is equipped with implantable/wearable body sensor nodes and a smartphone, which can periodically collect PHI and report them to the m-Healthcare center for achieving better healthcare quality, where PHI including blood pressure, heart rate, etc.[3].

In m-Healthcare system, the medical professionals at healthcare center first make medical examination for each medical user $U_i \in U$ and generate U_i's personal health profile $\vec{a}$ = (a_1,a_2,⋯,a_n) where n are medical user's total symptom characters. Later, the following steps will be performed by TA

1. We assume the whole system at healthcare center is monitored by a trusted authority (TA). TA chooses secure cryptographic hash function H, and a secure symmetric encryption algorithm Enc(),that is, AES. In addition, TA choose any random number $a \in Z_q^*$ where q is a prime number, computes b = H(a) as the master key. Finally, TA keeps the master (a, b) secretly.
2. At last, TA uses the master key b to compute the secret key ski = H(U_i||b) for U_i.

To achieve better healthcare monitoring medical user U_i uses following procedure to securely report his PHI to healthcare center.

a. After medical user equipped with the personal BSN and key material sk_i, U_i first chooses the current date cDate to compute the session key $k_i = H(sk_i||cDate)$ for one day and distributes the session key k_i to his personal BSN and smartphone.

b. For every five minutes, BSN collects raw PHI data rPHId and reports the encrypted value $Enc(k_i,rPHId||cDate)$ to the smartphone with bluetooth technology.

c. Upon receiving $Enc(k_i,rPHId||cDate)$, the smartphone uses k_i to recover rPHId from $Enc(k_i,rPHId||cDate)$.

d. 3G technology is utilized by smartphone to report the processed PHI to healthcare center in the form of $(U_i||cDate||Enc(k_i,PHI||cDate))$.

e. When the TA receives $(U_i||cDate||Enc(k_i,PHI||cDate))$ at the healthcare center, first he compute U_i's secret key $sk_i = H(U_i||b)$ by using master key b, and uses sk_i to compute the current session key $k_i = H(sk_i||cDate)$.

f. Then, TA uses k_i to recover PHI||cDate from $Enc(k_i,PHI||cDate)$. TA sends PHI to the medical professionals for monitoring if the recovered cDate is corrected.

PHI data is received by medical professionals at healthcare center to monitor medical users' health conditions and as well quickly react to users' life-threatening situations and dispatching ambulance and medical personnel to an emergency location in a timely fashion to save their lives.

CONCLUSION

In this paper, a secure patient healthcare monitoring and management system has been presented. We show why patient monitoring is so important in m-healthcare, and thus how to construct a monitoring system over reliable and efficient communications.

Smartphone is not only used for healthcare monitoring, but also for phoning with friends so that smartphone's energy could be insufficient when an emergency takes place. Hence, the reliability of m-Healthcare system is still challenging in emergency.

In the future, we will work on m-Healthcare system to enhance the reliability of PHI process and transmission in emergency.

REFERENCES

1. Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, Fellow, "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transactions on Parallel and Distributed systems, 2012.
2. A. Toninelli, R. Montanari, and A. Corradi, "Enabling secure service discovery in mobile healthcare enterprise networks," IEEE Wireless Communications, vol. 16, pp. 24–32, 2009.
3. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network," in Proc. BodyNets'10, Corfu Island, Greece, 2010.
4. Y. Ren, R. W. N. Pazzi, and A. Boukerche, "Monitoring patients via a secure and mobile healthcare system," IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.
5. R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," MONET, vol. 16, no. 6, pp. 683–694, 2011.
6. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed System, to appear.
7. M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, "Wireless body sensor network using medical implant band," Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.
8. W.-B. Lee and C.-D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/ Security Regulations," IEEE Trans. Info. Tech. Biomedicine, vol. 12, 2008, pp. 34–41.
9. A. Boukerche, Handbook of Algorithms for Wireless and Mobile Networks and Computing, Chapman and Hall/CRC, 2005.
10. M. Tentori, J. Favela, and M. D. Rodriguez, "Privacy- Aware Autonomous Agents for Pervasive Healthcare," IEEE Intelligent Sys., vol. 21, 2006, pp. 55–62.
11. D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. of CRYPTO'01, 2001, pp. 213–229.

12. X. Lin, X. Sun, P. Ho, and X. Shen, "Gsis: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, pp. 3442–3456, 2007.

13. R. Lu, X. Lin, H. Zhu, , and X. Shen, "An intelligent secure and privacy- preserving parking scheme through vehicular communications," IEEE Transactions on Vehicular Technology, vol. 59, pp. 2772–2785, 2010.