Homecare Monitoring System

Mrs. M. Seema[1], D. K. Srisubarnaa[2], N. Priyadharshini[3], J. Sheika Zakiya[4]
[1]Assistant Professor, [2, 3, 4] UG Students
Department of Information Technology,
Velammal College of Engineering and Technology, Madurai-625009

Abstract **- WBAN (Wireless Body Area Networks) is a relatively new network paradigm designed to provide users with a remote and periodical healthcare monitor in healthcare system. In WBANs, each patient in the system wears one or more wireless body sensor nodes (BSNs). These sensor nodes monitor and collect personal information (PHI) such as blood pressure, heartbeat, and temperature, regardless of the patient's location and condition (e.g. lying in bed or taking a stroll). Collected PHI will be sent to a smart mobile device, such as a smart phone, via bluetooth, cognitive radio or other communication channel (e.g. WiFi). The mobile smart device will then transmit the PHI to a remote healthcare center via a message or WiFi network. This allows the medical practitioner (e.g.medical doctor and specialist) to monitor and understand the patient's health condition, and respond to any life threatening situation in real-time (e.g. dispatching medical workers to the patient in the event of a potential heart attack or a stroke) thus, providing better quality healthcare for patients.**

Keywords- Mobile healthcare social networks, Cross domain handshake scheme, secure handshake, authentication, elliptic curve, security.

I INTRODUCTION

WBAN is a relatively new network paradigm designed to provide users with a remote and periodical healthcare monitor in healthcare system. In WBANs, each patient in the system wears one or more wireless body sensor nodes (BSNs). These sensor nodes monitor and collect personal information (PHI) such as blood pressure, heartbeat, and temperature, regardless of the patient's location and condition(e.g. lying in bed or taking a stroll). Collected PHI will be sent to a smart mobile device, such as a smart phone, via bluetooth, cognitive radio or other communication channel (e.g. WiFi). The mobile smart device will then transmit the PHI to a remote healthcare center via a 3G/4G or WiFi network. This allows the medical practitioner (e.g.medical doctor and specialist) to monitor and understand the patient's health condition, and respond to any lifethreatening situation in real-time (e.g dispatching medical workers to the patient in the event of a potential heart attack or a stroke); thus, providing better quality healthcare for patients. A typical healthcare-monitoring scenario is shown in Fig.1

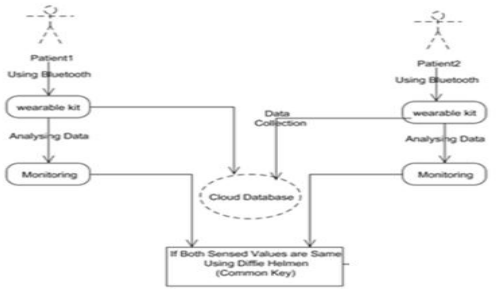


Fig 1: A typical healthcare-monitoring scenario

I.1 MOTIVATIONS

We present a new handshake framework for MHSNs, which comprises two levels. The top level is the trusted authority, who is tasked with generating private keys for participating healthcare centres using the Schnorr signature scheme. The second level is the registered healthcare centres responsible for generating their patients' private keys using the Schnorr signature scheme.

II.EXISTING SYSTEM

The patients could obtain professional health-related advice from medical practitioners, based on the analysis of patients' PHI. Patients having the same symptoms may want to establish a support network, share experiences, and broaden their understanding of illness, in addition to sending new information about their condition to a medical center in real-time using their mobile devices. This can be implemented using a Mobile Social Network (MSN), which is also known as the Mobile. Healthcare Social Network (MHSN). A typical MHSN implementation includes a trusted authority and patients registered with this trusted authority, however, the wireless communication channel can be compromised by an adversary by intercepting, modifying, replaying, inserting, and delaying messages transmitted in the systems. Security of MHSNs is critical, as fatalities and other life-threatening consequences can result from misdiagnosis due to such attacks. The handshake scheme can be used to authenticate a registered patient and preserve the patient's privacy. More specifically, after the successful execution of a handshake scheme, two patients can be assured of each other's identity and generate a session key to ensure the security of their future communication.

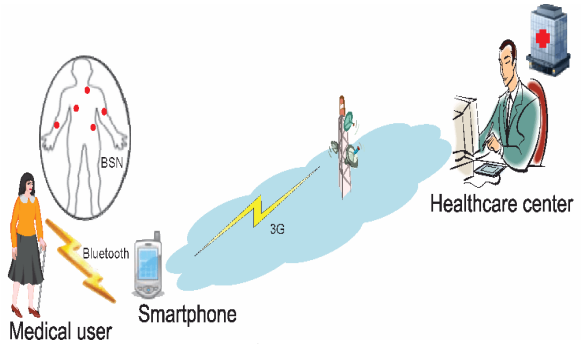


Fig2: Frame Work of pervasive health monitoring

III. PROPOSED SYSTEM

In the proposed system, there is an efficient Cross-Domain Handshake (CDHS) scheme with symptoms matching for MHSNs based on elliptic curve cryptography (ECC). Which is used to protect the patient monitoring information. Patient will receive the suggestion according to sending information. In case attack happens on the patient information doctor may provide wrong suggestion to the patient so we need to protect the monitoring information using ECC. If the sensor sends abnormal value, doctor can receive the values through mobile and then the application will be automatically open on the mobile. Immediately doctor sends the suggestion to the patient also the patient relatives. CDHS act as main role before going to share the information they have to share the keys based on this key Diffie-hellman will produce common key. The data encrypted by using diffie-helman key and decrypted by their won key.

III.1 SECURITY AND FUNCTION REQUIREMENTS

A handshake scheme for MHSNs should satisfy the following requirements.

Mutual authentication: To ensure the eligibility of patients in the healthcare system, the handshake scheme for MHSNs should provide mutual authentication between two patients executing a handshake.

Patient anonymity: To protect a patient's privacy, the handshake scheme for MHSNs should ensure patient anonymity (i.e. an adversary is not able to obtain a user's real identity from the intercepted messages).

Patient traceability: The healthcare center is able to extract the patient's real identity by analyzing relevant messages when necessary. For example, the healthcare center may need to investigate false allegations by a registered patient.

Cross-domain communication: To ensure that patients registered in different healthcare centers can communicate with each other, the handshake scheme for MHSNs needs to provide cross-domain communication.

Resistance of various attacks: To withstand various attacks prevalent in the mobile service system, the handshake scheme for MHSNs needs to provide resistance of various attacks. In other words, the protocol needs to withstand common attacks such as impersonation attack, modification attack, replay attack, and stolen verifier table attack.

IV SOFTWARE AND HARDWARE

IV.1SOFTWARE

a)JAVA

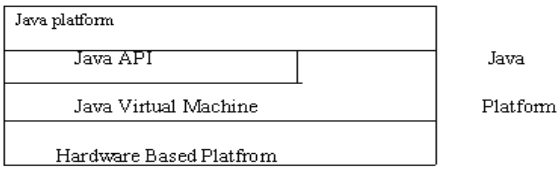
A platform is the hardware or software environment in which a program runs. The Java platform differs from most other platforms in that it's a software-only platform that runs on top of other, hardware-based platforms. Most other platforms are described as a combination of hardware and operating system.

The Java platform has two components :

The Java Virtual Machine (JVM)

The Java Application Programming Interface (Java API)

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries (packages) of related components. The following figure depicts a Java program, such as an application or applet, that's running on the Java platform. As the figure shows, the Java API and Virtual Machine insulates the Java program from hardware dependencies



As a platform-independent environment, Java can be a bit slower than native code. However, smart compliers, weel-tuned interpreters, and just-in-time byte complilers can bring Java's performance close to that of native code without threatening protability

b)APACHE TOMCAT SERVER

Apache Tomcat (formerly under the Apache Jakarta Project; Tomcat is now a top level project) is a web container developed at the Apache Software Foundation. Tomcat implements the servlet and the JavaServer Pages (JSP) specifications from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server. It adds tools for configuration and management but can also be configured by editing configuration files that are normally XML-formatted. Because Tomcat includes its own HTTP server internally, it is also considered a standalone web server.

c)ENVIRONMENT

Tomcat is a web server that supports servlets and JSPs. Tomcat comes with the Jasper compiler that compiles JSPs into servlets. The Tomcat servlet engine is often used in combination with an Apache web server or other web servers. Tomcat can also function as an independent web server. Earlier in its development, the perception existed that standalone Tomcat was only suitable for development environments and other environments with minimal requirements for speed and transaction handling. However, that perception no longer exists; Tomcat is increasingly used as a standalone web server in high-traffic, high-availability environments. Since its developers wrote

Tomcat in Java, it runs on any operating system that has a JVM.

IV.2 HARDWARE

a)HEART RATE SENSOR

Heart rate measurement indicates the soundness of the human cardiovascular system. This project demonstrates a technique to measure the heart rate by sensing the variation of the blood volume inside a finger artery, which is caused by the pumping action of the heart. It consists of an infrared LED that transmits an IR signal through the fingertip of the subject. A part of this infrared light is reflected by the blood cells. The reflected signal is detected by a photo diode sensor. The changing blood volume with heartbeat results in a train of pulses at the output of the photo diode, the magnitude of which is too small to be detected directly by a microcontroller. This Heart rate is the number of heartbeats per unit of time and is usually expressed in beats per minute (bpm). In adults, a normal heart beats about 60 to 100 times a minute during resting condition.

b)BODY TEMPERATURE

The most commonly used type of all the sensors are those which detect Temperature or heat. These types of temperature sensor vary from simple ON/OFF thermostatic devices which control a domestic hot water heating system to highly sensitive semiconductor types that can control complex process control furnace plants. Normal human body temperature, also known as normothermia or euthermia, is the typically temperature range found in humans. The normal human body temperature range is typically stated as 36.5–37.5 °C (97.7–99.5 °F).Individual body temperature depends upon the age, exertion, infection, time of day, and reproductive status of the subject, the place in the body at which the measurement is made, the subject's state of consciousness (waking or sleeping), activity level, and emotional state. It is typically maintained within this range by thermoregulation. Human body temperature is of interest in medical practice, human reproduction, and athletics.

V. RESULT AND DISCUSSION

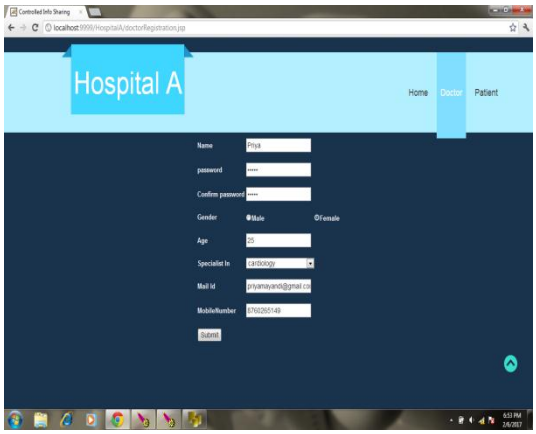


Fig 6.1 Doctor Registration

Fig 6.2 Patient Registration

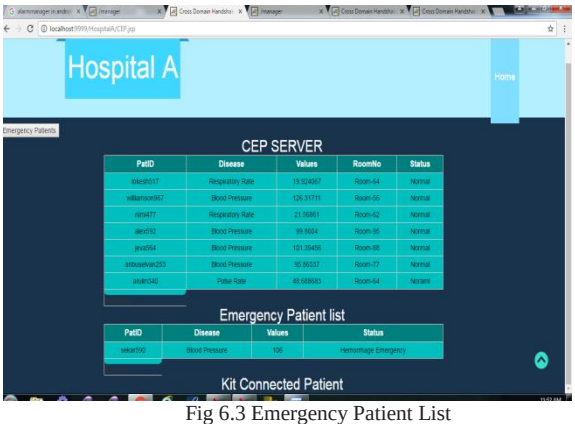


Fig 6.3 Emergency Patient List

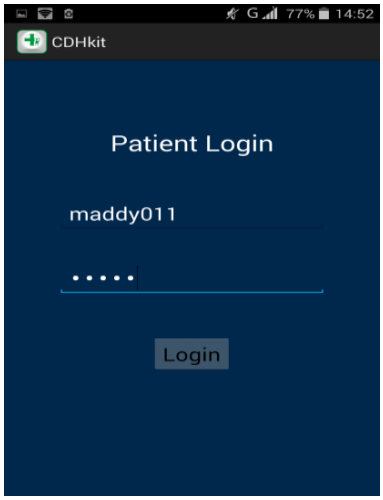


Fig 6.4 Patient Login in Mobile

Fig 6.5 Reading the Patient Body Parameters

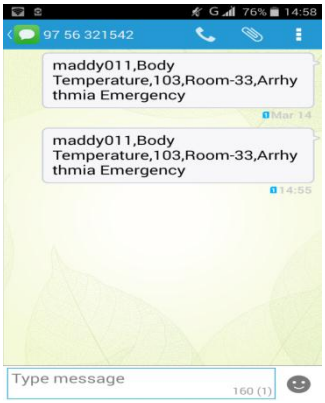


Fig 6.6 Intimation to Doctor

CONCLUSION

The various handshaking schemes proposed in the earlier years suffered from various drawbacks such as lack of support for Cross Domain Handshaking schemes and incompatibility for mobile device deployment and so on. Further, they were found to be either insecure, or suffered from high computation and communication costs. Thus, our technique proves to be an efficient one in terms of mobile device deployment and also provably requires very low computation and communication costs when compared with the previous techniques. Future enhancements could include expanding the horizon with the number of healthcare centers and the wide ranges of diseases covered. This can ensure practical deplorability in real life situations thus serving as a boon to the existing healthcare centers.

REFERENCES

1. A. Petroff, ”World getting ’super-aged’ at scary speed,”, http://money.cnn.com/2014/08/21/news/economy/agingcountries- moodys, 2015.
2. X. Liang, R. Lu, L. Chen, X. Lin and X. Shen, ”PEC: A privacypreserving emergency call scheme for mobile healthcare social networks,” Journal of Communications and Networks, vol. 13, no. 2, pp. 102-112, 2011.
3. S. Jiang, Zhu X, Wang L, ”EPPS: Efficient and privacy-preserving personal health information sharing in mobile healthcare social networks,” Sensors, vol. 15, no. 9, pp. 22419-22438, 2015.
4. D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H. C. Wong, ”Secret handshakes from pairing-based key agreements,” in Proc.IEEE Symposium on Security and Privacy, pp. 180-196, 2003.
5. C. Castelluccia, S. Jarecki, and G. Tsudik, ”Secret handshakes from CAoblivious encryption,” in Proc. Asiacrypt, pp. 293-307, 2004.
6. D. Vergnaud, ”RSA-based secret handshakes,” in Proc. International Workshop on Coding and Cryptography, 2005.
7. S. Jarecki, J. Kim, and G.Tsudik, ”Beyond secret handshakes: affiliationhiding authenticated key exchange,” in Proc. CT-RSA, pp. 352-369, 2008.
8. S. Xu and M. Yung, ”k-anonymous secret handshakes with reusable credentials,” in Proc. CCS04: 11th ACM Conference on Computer and Communications Security, pp. 158-167, 2004.
9. H. Huang and Z. Cao, ”A novel and efficient unlinkable secret handshakes scheme,” IEEE Commun. Lett., pp. 363-365, 2009.
10. R. Su, ”On the security of a novel and efficient unlinkable secret handshakes scheme,” IEEE Commun. Lett., pp. 712-713, 2009.