SECURE HEALTHCARE MONITORING SYSTEM WITH EMERGENCY PREDICTION AND SYMPTOMS-MATCHING FOR MOBILE HEALTHCARE SOCIAL NETWORK

Melvina J.S.M[1], T. Lincy Thangammal[2], S.Mythireyi[3], S. Manisha[4]

[1] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[2] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[3] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*
[4] *Student, Department of Computer science, Panimalar Engineering College, Tamil Nadu, India*

ABSTRACT

With high speed developments of sensor, wireless and mobile communication technologies, Mobile Healthcare Social Networks (MHSNs) have emerged as a popular means of communication in healthcare services. With the help of MHSNs, patients can use their mobile devices to securely share their experiences, broaden their understanding of the illness or symptoms, form a supportive network, and transmit information between users and other stake holders (e.g. medical center). The handshake scheme is a significant cryptographic mechanism, which can provide secure communication in MHSNs (e.g. anonymity and mutual authentication between users, such as patients). The main aim of this project is to detect the possibility of health issues that may occur in a patient by constant monitoring and emergency prediction and to establish a secure framework for handshaking scheme in Mobile Healthcare Social Network (MHSN). Monitoring is done using Wireless Body Area Networking (WBAN) technology which makes use of Body Sensor Nodes (BSN).It is based on hierarchical identity based cryptography. The MHSN is set up using an efficient Cross Domain Handshake Scheme (CDHS) that allows symptoms matching within MHSNs.

Keywords: - *cross domain handshake, body sensor nodes, hierarchical identity based cryptography, mobile healthcare social network, emergency prediction;*

1. INTRODUCTION

Mankind is facing a serious ageing challenge where more than 20% of the world’s population is found to be over 65, partially due to a longer life span but declining birth rate. For instance, it has been predicted that around 13 countries will be “super-aged” by the year 2020 and 34 countries by the year 2034 according to Moody’s Investigation service. An aging demographic will be a trial for our existing healthcare systems and this may place a strain on the healthcare industry, if technologies fail to keep pace with the changing requirements. Hence, Wireless Body Area Networks (WBANs) will help in playing an active role in supporting and complementing existing healthcare systems. WBAN is a relatively new network paradigm designed to provide users with remote and periodical healthcare monitoring in healthcare systems. In this technique, the registered patient is made to wear one or more wireless body sensor nodes (BSNs). These nodes observe and collect personal health 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, via Bluetooth, or other communication channel. The device will then transmit the PHI to a remote healthcare center through a 3G/4G or Wi-Fi network. This allows the doctor to monitor and understand the patient’s health condition, and respond to any life menacing situation in real-time, thus, providing better quality healthcare for patients. In the healthcare system, the patients could obtain professional health-related advice from the doctors, 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. 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, where

PA = PA1; PA2; _ _ _ PAn

denote registered patients. However, the wireless communication channel can be hacked 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 fortify the security of their succeeding communication.

2. RELATED WORK

Ming Li et al[3] proposed a privacy preserving system which made new connections according to personal preferences in mobile social networking, where the initiating user can find matching users within physical proximity of them in the year 2011. Even though it was a secure and efficient technique, it was only applicable for small network sizes in the order of tens. Further, this technique incurred high communication costs. Li et al[7], in the year 2005 designed a system to show that OSBE can be used to break policy cycles in automated trust negotiation (ATN) and to achieve oblivious access control. Lang Zhang and Xiang-Yang Li [4], in the year 2012, proposed a technique to overcome the disadvantages of the previous technique by creating a preference profile for each user which facilitates compatibility matching without revealing personal information regarding the user's profiles. This technique, though incurs lower computation and communication costs, did not ensure forward and backward secrecy. Yamin Wen et al [5] established a full-fledged secret handshaking scheme which worked in such a way that one user will only reveal his/her affiliation to the other user if they were a member of the same organization. Thus, participants only distinguish that they are members of the same organization, without leaking their true identities in this organization. This technique provided efficient backward unlinkability, revocation, traceability and security. But it required better design from multi linear lattices since revocation information is assumed to be at most linear in the number of revoked participators. Dirk Balfanz et al [9], established a secret handshaking technique in 2003 which allowed members of the group to identify each other, but this system was not able to support user authorization and revocation. C. Castelluccia et al [6], in the year 2004, designed a system that allowed members of the same group to authenticate each other secretly, in the sense that someone who is not a group member cannot tell. Yan Michalevsky, Suman Nath and Jie Liu [2], in the year 2016, presented new uses for cryptographic based secret handshakes between mobile devices on top of Bluetooth Low-Energy. It is a mobile application that enables participants to discover and interact with nearby users if and only if they belong to the same secret community. It uses effective handshaking scheme with direct peer-to-peer communication over Bluetooth LE. But the computation peed was observed to be very low in this technique.

Huang and Cao also presented a handshake scheme, which supports both affiliation-hiding and unlinkability. However, Su revealed that an adversary is able to execute the secret handshake with a registered user; thus, breaking the security of the Huang-Cao scheme. Youn and Park also found that Huang and Cao's scheme does not provide affiliation-hiding or authenticated key exchange, as claimed. However, neither Su nor Youn nor Park proposed an improved scheme to address the identified vulnerabilities. In 2011, Gu and Xue proposed an improved handshake scheme but it was subsequently found to be vulnerable to the key-compromise impersonation attack and does not support forward secrecy, as claimed. Wen et al [10] presented a generic approach, designed to transmit an identity-based message recovery signature scheme to a handshake scheme. They also proposed two handshake schemes using their approach. Xiaohui Liang, Rongxing Lu, Le Chen, Xiaodong Lin, and Xuemin (Sherman) Shen [8], in 2011, proposed a method to enable patients in life-threatening emergencies to fast and accurately transmit emergency data to the nearby helpers via MHSNs. But the decentralized nature of this system caused difficulties in data management. Debiao He et al [1], in the year 2016, established a secure Cross Domain Handshake Scheme for

Mobile Healthcare Social Networks. In spite of its efficiency, the system could not handle emergency prediction mechanisms.

Recently, in 2016, Debiao He, Neeraj Kumar, Huaqun Wang, Lina Wang, Kim-Kwang Raymond Choo, Alexey Vinel designed a Cross Domain Handshaking Scheme (CDHS) for Mobile Healthcare Social Networks (MHSN). A wireless BSN is setup in order to constantly monitor the health of the patient. These values, which are stored over the cloud, are matched for establishing MHSN. Even though it facilitated CDHS schemes which were easily suitable for mobile deployment; it lacked emergency prediction mechanisms which were overcome by our work.

3. EXISTING METHODOLOGY

In the existing system, each patient in the system is made to wear one or more of the wireless body sensor nodes (BSNs).These sensor nodes monitor and collect personal health information (PHI) such as blood pressure, heartbeat, and temperature. The collected PHI will be sent to a smart mobile device, via Bluetooth, cognitive radio or other communication channel (e.g. Wi-Fi).The mobile smart device will then transmit the PHI to a remote healthcare center via a message or through a Wi-Fi network. This allows the medical practitioner to monitor and understand the patient's health condition, and respond to any life threatening situation in real-time. For instance, dispatching medical workers to the patient in the event of a potential heart attack or a stroke. These medical symptoms which are stored in a secure database are analyzed for different patients. When a match is found, a session is established upon the consent of the patients using Diffie Hellman Key Exchange in order to facilitate communication between them.

4. PROBLEMS IN THE EXISTING SYSTEM

The existing techniques either did not support Cross Domain Handshaking schemes or failed to assist in mobile device deployment. They also did not support functions important to a real-life user, such as symptoms-matching function, patient anonymity, perfect forward secrecy and backward secrecy and emergency prediction mechanisms which are essential to take precautionary measures.

5. PROPOSED WORK

The proposed method mainly includes five main phases namely Registration and Patient Monitoring, Wireless Sensor Node, CEP Server, Emergency Mobile Application and Cross Domain Handshake scheme.

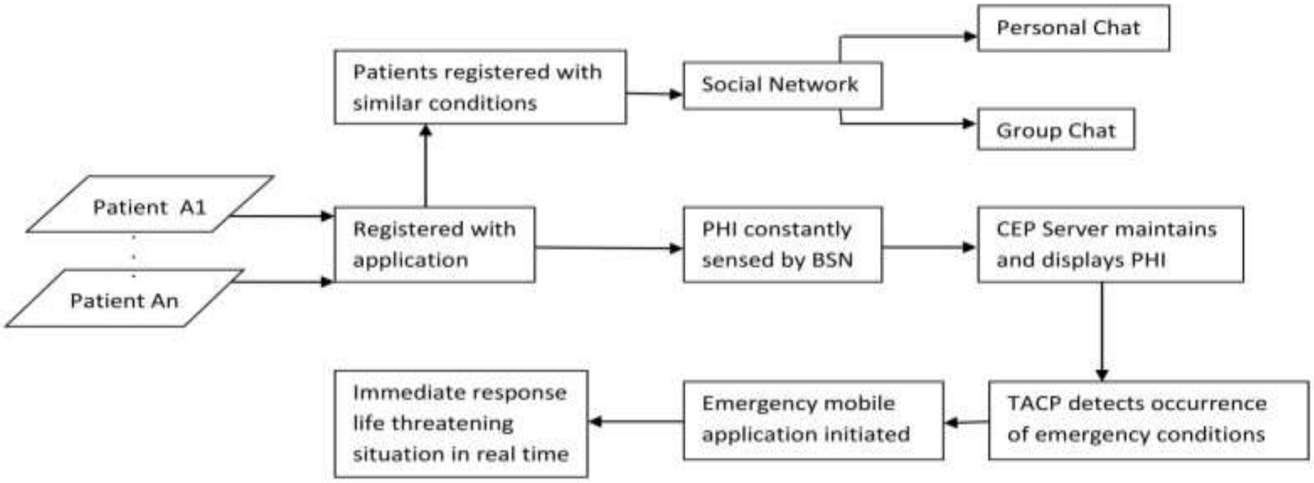
Personal Chat
Patients registered with similar conditions
Social Network
Group Chat
Patient A1
Patient An
Registered with application
PHI constantly sensed by BSN
CEP Server maintains and displays PHI
Immediate response life threatening situation in real time
Emergency mobile application initiated
TACP detects occurrence of emergency conditions

Fig -1 Flow diagram of the proposed method

Figure 1 represents a flowchart that depicts the working of all the phases. In the Registration and patient monitoring phase, the patient and the doctor should be registered with our web application. The CEP server is used to monitor the patient. Once the patient gets registered the patient id will be automatically updated in the CEP server and all the patient health condition are continuously monitored by the complex event processing server.

The next phase describes about the working of the wireless sensor node which will be peripherally attached to the patient. The sensor is made up of a PIC microcontroller (Peripheral Interface Controller), version 16F877A. It is a powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) CMOS FLASH-based 8-bit microcontroller packed into a 40 pin package. It comprises of 14 kB memory size and 7 ADC ports along with a single UART port which enables serial communication. All of these features make it ideal for more advanced level A/D applications in automotive, industrial, appliances and consumer applications. This node, which is attached to the patient's finger, comprises of an IR light which serves as a receiver. The light signal cuts off when the value rises and it is taken as 0 and 1 otherwise (indicated by the glowing light from the sensor). Thus, a series of alternating 0s and 1s are sensed and these values are constantly updated to the mobile device at an interval of 30 seconds. The kit also comprises of an amplifier board which amplifies the LPF values to HPF values. The body temperature of the patient is measured with the help of an LM35 sensor which also converts the Analog to Digital values before sending it to the mobile device.

The next phase describes about the working of the CEP server. Whenever emergency is detected the emergency patient details are separately maintained on the CEP server using a policy called as the Temporary Access Control Policy (TACP) which is in the form of an XML file. Each patient has a unique login and once they are logged in our application and they will see the continuous monitoring values of that patient. Once the emergency has been detected they will able to see the type of emergencies and also policy type. The emergency policy can also be dynamically updated by the hospital admin. The policies are maintained based on this XML file.

The next phase describes about the Emergency Mobile Application that exists in our paper. After the emergency has been detected by the temporary access control policies, that patient's emergency policy and also the abnormal values of the patient are sent to the doctor's mobile by sms and also to the patient's relative's mobile number. After sensing the type of emergency that has arisen, the hospital android application will get automatically opened and the details about the patient and emergency policy are displayed in that application to the doctor, the patient and the same is viewed by the patient's relative too. After viewing the patient's details, the doctor will send the prescription to the patient's relative's mobile number or dispatch the respective staff accordingly based on the type of emergencies.

The final phase depicts about the working of the Cross Domain Handshaking scheme which facilitates communications between patients residing at different healthcare centers. Cross Domain Handshake (CDHS) policy will be checked based on the patient's registered symptoms. CDHS will then detect the type of policy and redirect that patient abnormal values and it will choose the doctor based on the policy type and gives the read or write permission to that specialist doctor in the hospital. The admin has the ability to see all the patient details and also the emergency policy type of the each patient. CDHS, then establishes a secure social networking platform which enables patients exhibiting similar symptoms to communicate with each other either in a private manner or even as a group, thus allows two users registered in different healthcare centers to execute the cross-domain handshake with symptoms-matching.

6. RESULTS AND DISCUSSIONS

Our system was tested for efficiency in terms of computation and communication cost requirements and it was found that our proposed method incurred very less computation and communication costs. Further, the chat application between the patients in the Mobile Healthcare Social Network was encrypted using the Diffie-Hellman key exchange method which required very less cost for setting up and is considered the most efficient for our application since any attempt to hack the system is very expensive and is thus avoided. The cross domain handshaking scheme also permitted patients belonging to various healthcare centers to communicate with each other. Thus our system is found to radiate high performance and efficiency.

7. 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.

8. REFERENCES

[1]. Debiao He, Neeraj Kumar, Huaqun Wang, Lina Wang, Kim-Kwang Raymond Choo, Alexey Vinel, “A Provably-Secure Cross-Domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network” , 2016, IEEE Transactions on Dependable and Secure Computing.

[2]. Yan Michalevsky, SumanNath, Jie Liu, “MASHaBLE: Mobile Applications of Secret Handshakes over Bluetooth LE” 2012, the 22nd Annual Conference on Mobile Computing and Networking.

[3]. Ming Li, Ning Cao, Shucheng Yu and Wenjing Lou, “FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks “2011, IEEE Infocom

[4]. L. Zhang, X. Li, K. Liu, T. Jung, Y. Liu, ”Message in a sealed bottle: privacy preserving friending in mobile social networks,” IEEE Transactions on Mobile Computing, vol. 14, no. 9, pp. 1888-1902, 2015.

[5]. Yamin Wen, Zheng Gong and LinglingXu, “A Backward Unlinkable Secret Handshake Scheme with Revocation Support in the Standard Model “2015, ISSN 2078-2489

[6]. C. Castelluccia, S. Jarecki, and G. Tsudik,”Secret handshakes from CA oblivious encryption,” in Proc. Asiacrypt, pp. 293-307, 2004.

[7]. Ninghui Li, Wenliang Du, Dan Boneh, “Oblivious Signature-Based Envelope “2015, Springer Link

[8]. X. Liang, R. Lu, L. Chen, X. Lin and X. Shen, ”PEC: A privacy preserving emergency call scheme for mobile healthcare social networks,” Journal of Communications and Networks, vol 13, no. 2, pp. 102-112, 2011.

[9]. Dirk Balfanz, Glenn Durfee, Narendar Shankar, Diana Smetters, Jessica Staddon, Hao-Chi Wong, “Secret Handshakes from Pairing-Based Key Agreements” 2003, Security and Privacy.

[10]. Y. Wen, F. Zhang, L. Xu,”Secret handshakes from ID-based message recovery signatures: A new generic approach,” Computers & Electrical Engineering, vol. 38, no. 1, pp. 96-104, 2012.