Research Paper

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Framework For a Secure and Privacy Preserving Opportunistic Computing (Spoc) in Mobile-Healthcare Emergency

Engineering

KEYWORDS : Mobile-Healthcare emergency, opportunistic computing, user-centric privacy access control, Keys, PHI, smart phone

Shivani Arora	Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India
Waje Archana Tryambak	Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India
Pawar Bhagyashri Sanjay	Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India
Amrin Siddiqui	Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India
Poonam Sonawane	Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India

ABSTRACT

With the advancement of smart phones and wireless Body Sensor Networks (BSNs),mobile Healthcare (m-Healthcare) System, which provides the facility of Healthcare to the patients being present anywhere and anytime has resulted in better health monitoring, and has therefore attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. Through this system we propose a secure and privacy-preserving opportunistic computing framework called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. Specifically, in a m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smart phone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere and as well quickly react to user's life-threatening situations and save their lives by dispatching ambulance and medical personnel to an emergency location in a timely fashion. We can't implement the Body Sensor, so we are implementing the Desktop application

INTRODUCTION

The aim of the project is to build a secure and privacy-preserving opportunistic computing framework which is known as SPOC and it is used for mobile Healthcare emergency. With SPOC, smart phone resources which consist of computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure.

The Health care system provides medical aid to the patients at any time and not considering their location as it can be traced with help of GPS facility of the android mobile. Security is also provided to the patient's information by restricting the other patients to access the information of the current patient. The goal of Mobile Healthcare System is to provide patients a more dynamic role in the m-healthcare system. There is a need to ensure the end-to-end security of data during transmission. In this project, Attribute Based Encryption (ABE) and access policies are based on the attributes of users that enable a patient to give access to her/his PHI among a set of users by encrypting the file under a set of attributes, without knowing about the list of the users.

The basic attention is paid on the architecture, design and implementation of a mobile health service platform.

RELATED WORK DONE:

Mobile Patient Monitoring:

The Mobile Health patient is facilitated with various sensors that continuously examine medical signs. They are connected together through a healthcare body area network (BAN) which consists of sensors, communication, actuators, processing services and all facilities which are linked together by using wireless network.

Opportunistic Computing For Wireless Sensor Network

The WSN is a distributed network which does not require any external infrastructure which is used to monitor a physical phenomenon.

SAGE (Scheme against Global Eavesdropping)

It does not only achieve the content oriented privacy but also the contextual privacy against strong global adversary.

Scalable and Secure Sharing Of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

This paper proposes ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, with the settings for multiple owners. The security and performance requirements are important in this paper.

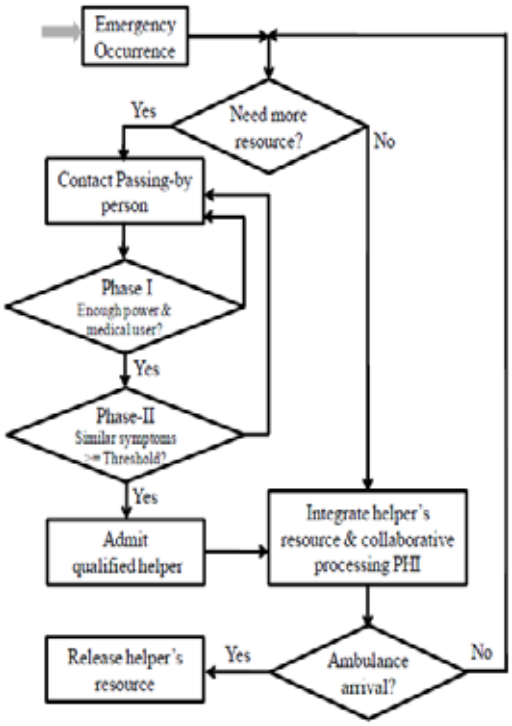
PROPOSED FRAMEWORK

In our project we are implementing the two-phase privacy access policy to provide high reliability of PHI process and transmission while minimizing PHI privacy disclosure in m-Healthcare emergency. In this, the access to the information of the patients is allowed only to the trust worthy authority. The patients can also view the prescriptions and suggestions given by the doctors to the other patients having similar symptoms. In this we implement two phase security model that is required to maintain the PHI of a patient in m-Healthcare system.

Phase-1: When there is enough power in the mobile phone of the patient and is a medical user.

Phase-2: When enough power is not there in the mobile phone of the patient and if the symptoms of the patient are similar to any other authorized medical user in the surrounding then the emergency healthcare details of the patient are transmitted to the server through the authorized medical user.

Figure 1: Flowchart showing two phase computing in m-Healthcare System



Sources: IEEE transactions on parallel and distributed systems, vol. xx, no. xx, xx 2012

Generation of Master Key

According to the security parameter κ, firstly trusted authority (TA) generates the bilinear parameters (q, g, G, G', e) by running $Gen(\kappa)$ and chooses a secure symmetric encryption algorithm $Enc()$, i.e., AES, and two secure cryptographic hash functions H and H'. Then TA chooses two random numbers $(a, x) \in Z$, as the master key, two random elements (h_1, h_2) in G, and computes $b = H(a)$, $A = g^a$, and $e(g, g)^x$. At the end, TA keeps the master (a, b, x) secretly, and publishes the system parameter $params$ = (q, g, G, G',e, H,H', h_1, h_2,A, $e(g, g)^x$, $Enc()$).

Generation of Access Control Key and Secret Key:

Suppose there are total n symptom characters considered in m-Healthcare system. A binary vector $\mathbf{a} = (a_1, a_2, ..., a_n)$ in the n-dimensional symptom character space, where $a_i \in \mathbf{a}$ indicates a symptom character, i.e., $a_i = 1$ if the medical user has the corresponding symptom character, and $a_i = 0$ otherwise.

- Then TA chooses two random numbers and computes the access control key $aki = (g^{x+at}{}_{i1}, g^{t}{}_{i1}, g^{t}{}_{i2}, h_1{}^{t}{}_{i1}, h_{2,i2}{}^{t})$ for U_i
- Finally, TA uses the master key b to compute the secret key $ski = H(U_i//b)$ for U_i.

Generation of Session Key

Ui first chooses the current date CDate, computes the session key $k_i = H(s\ k_i\ //\text{CDate})$ for one day, and distributes the session key *ki* to the desktop and smartphone.

- Upon receiving $Enc(k_i$, rPHI//CDate), the smartphone uses *ki* to recover rPHI from $Enc(k_i$, rPHI//CDate).

After processing rPHI, through 3G technology smartphone reports the processed PHI to healthcare center in the form of U_i//CDate//$Enc(k_i$,PHI//CDate).

- TA uses the master key b to compute U_i's secret key $sk_i = H(U_i //b)$, and uses sk_i to compute the current session key $ki = H(sk_i//\text{CDate})$. After that, TA uses k_i to recover PHI//CDate from $Enc(k_i$,PHI//CDate). If the recovered CDate is corrected, TA sends PHI to the medical professionals for monitoring.

ADVANTAGES

- Monitor the patients anytime and anywhere
- Reminder system: send notification to the patients
- Bluetooth, GPS and Internet connection are continuously observed by the system
- Track the current location of the patients.
- Maintains the security

FUTURE SCOPE

- To bring an alternative for the android mobile, if in case it turns off due to battery low or any other reason.
- This system can be implemented in the enterprise industries by the trusted authority to monitor the healthcare of the workers.

CONCLUSION

The concept of Mobile Computing or SPOC comes in which the patient will be provided with several different services even if the patient is far from the hospital. The patient's security issues will also be considered. The security issues regarding the secrecy of the information of the patients as well as the trusted authority will be resolved with the help of security algorithms. Location of the patients (far from hospital) will be traced with the help of GPS (Global Positioning System). For storing the patient record, the database will be maintained, with the help of MySQL and SQLite for android applications.

ACKNOWLEDGEMENT

We express true sense of gratitude towards our project guide Prof. Ms. A. V. Kanade for her invaluable co-operation and guidance that he gave us throughout out project. We would also like to specially thank our, head of department Prof. Mrs. D. A. Godse for inspiring us and providing us all the lab facilities with the Internet, which made this project work very convenient. We are also thankful to all the staff members of the Department of Information Technology of Bharati Vidyapeeth's College Of Engineering For Women, Pune for their valuable time, support, comments, suggestions and persuasion. We would also like to express our appreciation and thanks to all our friends who knowingly or unknowingly have assisted and encourage us throughout our hard work. Finally, how can we forget the almighty the supreme power of the GOD and our loving parents without which this work task was a distant dream.

REFERENCE

[1] A. Toninelli, R. Montanari, and A. Corradi, Enabling secure service discovery in mobile healthcare enterprise networks, IEEE Wireless Communications, vol. 16, pp.2432, 2009. | [2] Y. Ren, R. W. N. Pazzi, and A. Boukerche, Monitoring patients via a secure and mobile healthcare system, IEEE Wireless Communications, vol. 17, pp. 5965, 2010. | [3] 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. | [4] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, Opportunistic computing for wireless sensor networks, in IEEE Proc. of MASS07, pp. 16. | [5] W. Du and M. Atallah, Privacy-preserving cooperative statistical analysis, in Proc. Of ACSAC 01, 2001, pp. 102111. | [6] Aart Van Halteren, Richard Bults, Katarzyna Wac, Dimitri Konstantas, Ing Widya, Nicoslay Dokovsky,George Koprinkov, Val Jones, "Mobile Patient Monitoring: The MobiHealth System" ,The Journal on Information Technology in Healthcare 2004. |