International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Protected and Seclusion Preserving Computing Framework for Mobile Healthcare Services

Nivedha R V[1], Bimal Kalsa A R[2]

[1] PG Student, DMI College of Engineering, Chennai – 600123, India
[2] PG Student, DMI College of Engineering, Chennai – 600123, India
[1]nivedha.jayavel@gmail.com
[2]kalsaalex@gmail.com

***Abstract* — With the extensiveness of smart phones, and Mobile Healthcare (m-Healthcare) facilities, the Healthcare operations such as health care monitoring, has engrossed considerable interest recently. The nurturing of m-Healthcare still faces many challenges including information security and privacy preservation of the users. Thus, in this work, a Protected and Seclusion preserving Opportunistic Computing Framework (PSCF) for m-Healthcare Services has been proposed. This PSCF Framework aims at the security and privacy issues and it also provides an advantage of shifting from a hospital-oriented, centralized healthcare system to a patient oriented, Distributed healthcare system. With the proposed PSCF framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. It also reduces healthcare expenses through more efficient and protected use of this framework. To clout the PHI privacy disclosure, high reliability of PHI process and transmission in m-Healthcare, an efficient Signature Exchange Protocol is introduced in this framework.**

***Keywords* - Smartphones, Mobile Healthcare, opportunistic computing, Privacy, Security.**

I. INTRODUCTION

Mobile Healthcare is a term used for the practice of medicine and public health, supported by mobile devices. This term is also written as m-health, mobile health or m-healthcare.

The term is most commonly used in reference to using mobile communication devices, such as mobile phones, tablet computers and PDAs, for health services and information, but also to affect emotional states. The Mobile Healthcare field has emerged as a sub-segment of eHealth, the use of information and communication technology (ICT), such as computers, mobile phones, communications satellite, patient monitors, etc., for health services and information. Mobile Healthcare applications include the use of mobile devices in collecting community and clinical health data, delivery of healthcare information to practitioners, researchers, and patients, real-time monitoring of patient vital signs, and direct provision of care (via mobile telemedicine). Mobile eHealth or mHealth broadly encompasses the use of mobile telecommunication and multimedia technologies as they are integrated within increasingly mobile and wireless health care delivery systems. The nurturing of m-Healthcare still faces many challenges including information security and privacy preservation of the users.

In this paper, a new protected and seclusion preserving computing framework (PSCF) for mobile healthcare services has been proposed to address the challenging issue. Actually, the main contributions of this paper are threefold. 1) First, we define, a protected and seclusion preserving opportunistic computing system for mobile healthcare. With this framework, the different resources which are available on other opportunistically communicated patient's Smartphone can be collected together to handle with the computing-intensive PHI process in emergency cases.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

To minimize the privacy disclosure in opportunistic computing, PHI will be disclosed and this introduces a user-centric two-phase privacy access control for allowing only those patients who have same symptoms to participate in opportunistic computing. 2) Second, we guarantee the user-centric privacy access control for that, an efficient attribute based control and Signature Exchange algorithm. 3) Finally, we develop a custom simulator which is built in java to develop its substantial improvement in terms of PHI delivery ratio. In this, we discuss the promising application and extensive simulation results that shows proposed framework can effectively balance the high reliability of PHI process and minimizing the privacy disclosure compared with ordinary PHI reporting without social collaboration.

II. Models And Design Goal

In our system model, we consider a trusted authority (TA) and a group of medical users = {U_1, U_2, ・ ・ ・ , U_l}, TA, the manages the whole m-Healthcare system. Each medical user $U_i \in U$ is armed with personal BSN and smartphone, which can intermittently collect health information and report them to the healthcare center for achieving better health care quality. Unlike in-bed patients at home or hospital, medical user in our model are considered as mobile ones, i.e., walking outside.

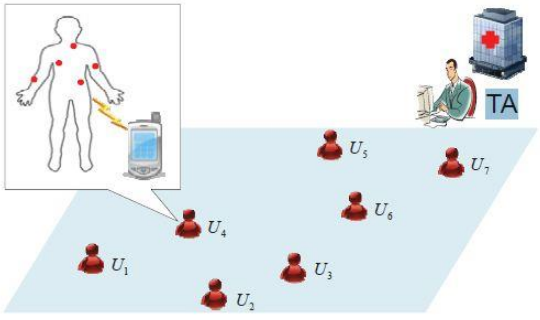

Fig 1 System Model under consideration

Design Goal

Our design goal is to develop a protected and seclusion preserving computing framework to provide high reliability of PHI process and transmission while diminishing PHI privacy confession in m-Healthcare emergency.

III. Proposed System

In this work, a Protected and Seclusion preserving Opportunistic Computing Framework (PSCF) for m-Healthcare Services has been proposed. This PSCF Framework aims at the security and privacy issues and it also provides an advantage of shifting from a clinic-oriented, centralized healthcare system to a patient oriented, Distributed healthcare system. With the proposed PSCF framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. It also reduces healthcare expenses through more efficient and protected use of this framework. To clout the PHI privacy disclosure, high reliability of PHI process and transmission in m-Healthcare, an efficient Signature Exchange Protocol is introduced in this framework.

Phase-I access control shows that suppose a passing-by person, is a non-medical user and he/she holds a Smartphone with enough battery power but he couldn't participate in opportunistic computing. And this pattern requires Smartphone with necessary software to cooperatively process the PHI. If he doesn't have the required medical software then it does not make him an ideal helper. Hence the phase-I privacy access control is necessary for auxiliary proceedings.

In phase-II access control, only the patients with similar symptoms would participate in opportunistic computing. Because of this, that system would process the same kind PHI due to similar symptoms.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Here we use threshold control parameter which is user self-control parameter so that when emergency takes place in high traffic at location, threshold will set high to minimize the privacy disclosure and if there's low traffic at location then threshold must be low so that high reliable process and transmission should be promised.

.

IV. MODULE DESCRIPTION

Medical User Module

In this module an application for Android smart phone is developed, to register the medical user, send and view their heal reports.

User Registration

The user is prompt to register with trusted authority to send the report and view diagnosis, on the time of registration user need to give their personal information such as name, age, address, contact number, email id, and username, password to login and send the reports, User need to give the emergency contact number to call immediately in emergency situations

Emergency Call

The user can call the emergency number by pressing a simple button, no need to open their dialer and enter the number or search the contacts and call the number, the user is prompt to give the emergency number to call at the time of registration, that number is called when the user is in emergency situation by pressing a simple button.

Send Report

User periodically sends their Personal Health Information (PHI) such as Pulse rate, Blood sugar, Blood pressure and Body temperature to the Trusted Authority. 14

View Report

User can view the report sent to the Trusted Authority and the diagnosis received from the trusted authority, then they can do the need, based on the diagnosis.

Settings

User has the options to update their Personal information, Username, Password and Emergency number when they needed.

Trusted Authority Module

This module is developed as PHP project; Trusted Authority can login in to the web application running in the server and can review all medical user PHI reports, time of the report and also the status of the report. The option to filter by the medical user name to view the particular medical user report is available. After reviewing the report, the trusted authority would send the diagnosis to the medical user based on their PHI status to their Smartphone application. The user can now receive the diagnosis as the email in the address given at the time of registration, and can receive the report in SMS in the number given.

FLOW DIAGRAM

The User should register to the Medical center with User name and Password. With the registered user name and password, the user can login to the application. If the User exists, he could proceed further; if not user should be registered to the medical center. The Flow Diagram of PSCF Framework is shown in the Fig 2.

During Emergency situations, a call will be connected to emergency number provided by user during registration. The report of user's health condition will be sent to the TA. Trusted Authority will view the report and send diagnosis to the medical user. The medical user will receive the report to his/ her Smartphone. Profile can be updated both by Medical User and the TA. In an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smartphone and wireless body sensor network formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

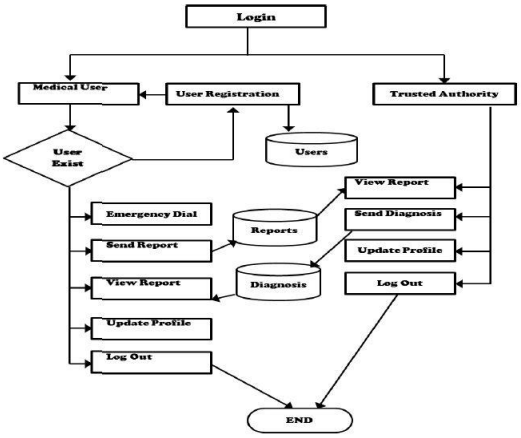

Fig 2 Flow Diagram

V. CONCLUSION

In this work a Protected and Seclusion preserving Opportunistic Computing Framework (PSCF) for m-Healthcare Services has been proposed. This PSCF Framework aims at the security and privacy issues and it also provides an advantage of shifting from a clinic-oriented, centralized healthcare system to a patient oriented, Distributed healthcare system. With the proposed PSCF framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. An algorithm named Signature Exchange algorithm can be used to impose Security during PHI transfer in Emergency Situations in this PSCF Framework.

V. REFERENCES

[1] Rongxing Luy, Xiaodong Linz, Haojin Zhux, and Xuemin (Sherman) Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme Using Vehicular Communications", published in IEEE INFOCOM.

[2] Arindam Dasgupta1 and Kothari Namita N, "An Opportunistic Computing System For Mobile-Healthcare Emergency", IEEE Transactions On IJAET, May 2013.

[3] [3] Kwang-Cheng Chen, "Machine-to-Machine Communications for Healthcare", in IEEE Journal of Computing Science and Engineering, Vol. 6, No. 2, June 2012, pp. 119-126

[4] [4] Ming Li, Wenjing Lou and Kui Ren, "Data Security And Privacy In Wireless Body Area Networks" in IEEE Wireless Communications, February 2010.

[5] [5] Michele Garetto, Paolo Giaccone and Emilio Leonardi, "Secure Friend Discovery in Mobile Social Networks" in IEEE/ACM Transactions on Networking, Vol. 17, No. 5, October 2009

[6] [6] Ming Li, Ning Cao, Shucheng Yuy and Wenjing Lou, "FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks", in IEEE Conference on INFOCOM, 2011

[7] [7] Jane Y. Yu And Peter H. J. Chong , "A Survey Of Clustering Schemes For Mobile Ad Hoc Networks", IEEE Communication Survey 2005, VOLUME 7

[8] [8] Xiaodong Lin, Xiaoting Sun and Xuemin Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications" in IEEE Transactions on Vehicular Technology, Vol. 56, No. 6, November 2007

[9] [9] M. Geetha, R. Revathi, "M-Healthcare Emergency Monitoring In Framework using Smart Phones" International Journal of P2P Network Trends and Technology (IJPTT) - Volume3 Issue 6- July 2013

[10] [10] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp. 1–6.

[11] [11] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in Proc. of ACM MSWIM '10, 2010, pp. 291–298.

[12] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010.