Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Opportunistic Computing Framework for M-Healthcare

Mr. Ajinkya S. Shewale
ME (appearing) Computer Science
Sangli, India

Abstract: Mobile Phones is mainly used for communications purpose, (i.e., phoning with friends, relatives, etc.). Mobile Phones is not only used for phoning and also used for other applications like healthcare monitoring with the help of wireless body sensor network. With the pervasiveness of smart phones, the advance of wireless body sensor networks (BSNs) and mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. In the SPOC (Security and Privacy Preserving opportunistic computing) framework aims at the security and privacy issues, and develops a user centric privacy access control of opportunistic computing in Mobile-Healthcare emergency. Whenever, critical battery achieved in the patient's mobile then he/she can connect with other's mobile. The SPOC software installed in the mobile will detect the other mobiles that have SPOC software. While the data is transferred to the database by using others mobile then the data will be sending in the encrypted format by using AES (Advanced Encryption Standard) technique so, that the information is more security for privacy preserving opportunistic computing system.

Keywords—opportunistic computing, user-centric privacy access control, PPSPC, wireless body sensor network

I. INTRODUCTION

In our aging society, mobile Healthcare {m-Healthcare} system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. Specifically, in an m-Healthcare system, Medical users are no longer needed to be monitored within home or hospital environment. Instead, after being equipped with Smartphone and wireless body sensor network (BSN) formed by body sensors nodes medical users can walk outside and receive the high quality healthcare monitoring from medical professionals anytime and anywhere.

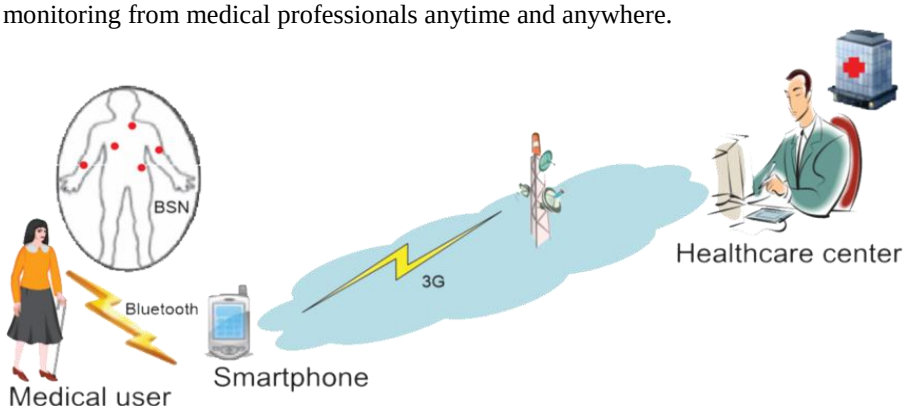

Fig. Pervasive health monitoring in m-Healthcare system

For e.g. as shown in fig each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure, temperature and others, can be first collected by body sensor network (BSN), and then aggregated by Smartphone via Bluetooth. Finally, they are further transmitted to the remote healthcare center via 3G networks. Based on these collected PHI data, medical professionals at healthcare center can continuously monitor medical user's health conditions 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.

Although m-healthcare system can benefit medical users by providing high quality pervasive healthcare monitoring, the flourish of m-Healthcare emergency, we consider the following scenario. In general, a medical user's PHI should be reported to the healthcare center every 5 minutes for normal remote monitoring. However, when he has an emergency medical condition, for example, heart attack, his BSN becomes busy reading a variety of medical measures, such as heart rate, blood pressure, and as a result, a large amount of PHI data will be generated in a very short period of time, and they further should be reported every 10 seconds for high-intensive monitoring before ambulance and medical personal's arrival. However, since Smartphone is not only used for healthcare monitoring, but also for other applications,

i.e., phoning with friends, the Smartphone's energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, i.e. 0.005, for a medical emergency, when we take into 10,000 emergency cases into consideration, the average event number will reach 50, which is not negligible and explicitly indicates the reliability of m-Healthcare system is still challenging in emergency.

II. BACKGROUND AND RELATED WORK

Opportunistic computing: The study of opportunistic computing has gained the great interest from the research community recently, and we briefly review some of them related to our work [7], [8], [9], [10].

In [7], Avvenuti et al. introduce the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node. Especially, their solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules, and each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes.

In [8], Passarella et al. evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services, that are opportunistically contributed by providers and invoked by seekers. Then, they present a complete analytical model to depict the service invocation process between seekers and providers, and derive the optimal number of replicas to be spawned on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used.

III. MODELS AND DESIGN GOAL

A. System Model:

In our system model, we consider a trusted authority (TA) and a group of *l* medical users U = *{U*1, *U*2,.... , *Ul},*as shown in Fig. 2. TA is a trustable and powerful entity located at healthcare center, which is mainly responsible for the management of the whole m-Healthcare system, e.g. initializing the system, equipping proper body sensor nodes and key materials to medical users. Each medical user *Ui* ∈ U is equipped with personal BSN and Smartphone, which can periodically collect PHI and report them to the healthcare center for achieving better health care quality using session key and send to Smartphone through which it is transferred to TA.

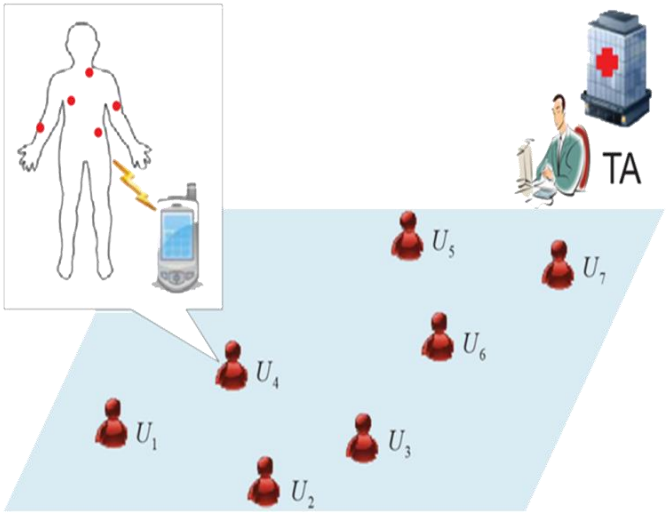

Fig. System Model

B. Security Model:

Opportunistic computing can enhance the reliability for highintensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure. Specifically, in our security model, we essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency, as shown in Fig.

Phase-I access control: Phase-I access control indicates that although a passing-by person has a smartphone with enough power, as a non-medical user, he is not welcomed to participate in opportunistic computing1. Since the opportunistic computing requires smartphones that are installed with the same medical softwares to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary softwares does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite.

Phase-II access control: Phase-II access control only allows those medical users who have some similar symptoms to participate in the opportunistic computing. The reason is that those medical users, due to with the similar symptoms, are kind of skilled to process the same type PHI. Note that, the threshold *th* is a user self-control parameter. When the mergency takes place at a location with high traffic, the threshold *th* will be set high to minimize the privacy disclosure.

However, if the location has low traffic, the threshold *th* should be low so that the high-reliable PHI process and transmission can be first guaranteed.

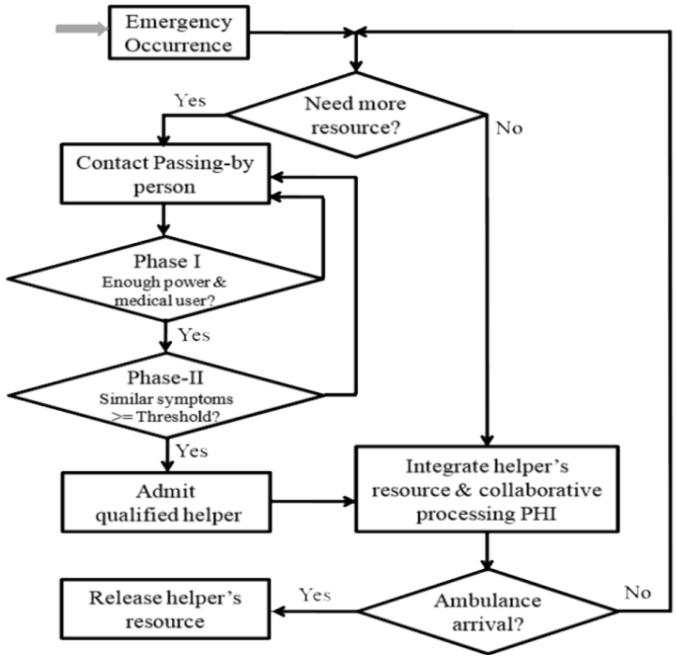

Fig. Security Model

C. Design goal:

Our design goal is to develop a secure and privacy-preserving opportunistic computing framework to provide high reliability of PHI process and transmission while minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, we i) apply opportunistic computing in m-Healthcare emergency to achieve high-reliability of PHI process and transmission ii) develop user-centric privacy access control to minimize the PHI privacy disclosure.

IV. OPPORTUNISTIC COMPUTING FRAMEWORK

A. System initialization:

Trusted Authority TA has full access control over whole healthcare system. Each medical user's symptoms are represented through his PHP i.e. a binary vector a={a1,a2,….,an} The medical professionals make medical examination for user and generate PHP i.e. binary vector a. TA chooses body sensor nodes to establish personal BSN and installs specific medical software in users smartphone.TA computed access control keys and master keys for a particular users. User prepares session key for current date and for every 5 min BSN collects raw PHI data Raw PHI data is encrypted using session key and send to Smartphone through which it is transferred to TA.

B. User-centric privacy access control for m-Healthcare emergency:

Phase-I: In this phase checking of available resources enough power and checking whether the user is a medical user or not.

Phase-II: In this phase checking of similar symptoms in the medical user happense.The standard threshold value is settled.

C. Analysis of opportunistic computing in m-Healthcare emergency:

Consider the ambulance will arrive at the emergency location in the time period t. To gauge the benefits brought by opportunistic computing in m-Healthcare emergency, we analyze how many qualified helpers can participate in opportunistic computing within the time period t, and how many resources can the opportunities computing provide.

If ambulance at emergency location will come in time t. In this time t how many users can join opportunistic computing and the resources available is measured.

V. CONCLUSIONS

A Secure Privacy-preserving Opportunistic Computing framework, to address this challenge. With the proposed SPOC 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.

REFERENCES

[1] Rongxing Lu Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuem in {Sherman} Shen, Fellow, IEEE.

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

[9] 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.

[10] 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.

