International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

SPOC: A Secure And Privacy Preserving Oppurtunistic Computing Framework Using PPSPC Technique

N.PADMASHRI
PG Student,Bharathiyar Institute of Engineering for Women, Deviyakurichi,Attur,Tamilnadu.
shrivijay1011@gmail.com

Abstract—With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, 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. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m- Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high-reliable-PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

***Index Terms*—Mobile-healthcare emergency, opportunistic computing, user-centric privacy access control, PPSPC**

I. INTRODUCTION

In 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 Smartphone 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 environments. Instead, after being equipped with Smartphone 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. For example, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by 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 system still hinges upon how we fully understand and manage the challenges facing in m-Healthcare system, especially during a medical emergency.

To clearly illustrate the challenges in 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

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

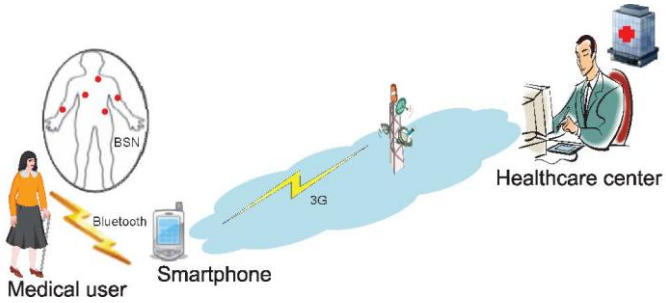


Fig. 1. Pervasive health monitoring in m-Healthcare system

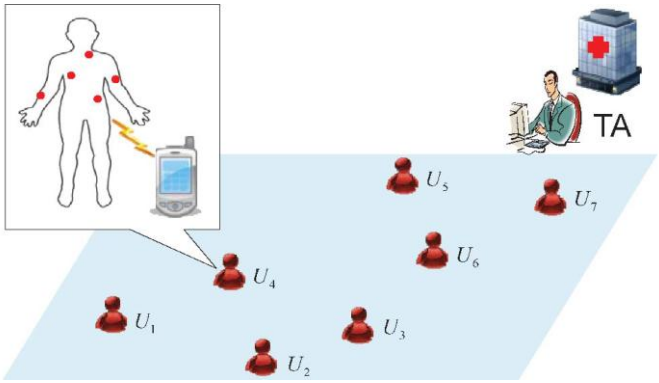


Fig. 2. System model under consideration.

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 person's arrival. However, since smart phone is not only used for healthcare monitoring, but also for other applications, ith 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.

Recently, opportunistic computing, as a new pervasive computing paradigm, has received much attention [7], [8], [9], [10]. Essentially, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for the distributed execution of a computing-intensive task [10]. For example, once the execution of a task exceeds the energy and computing power available on a single node, other opportunistically contacted nodes can contribute to the execution of the original task by running a subset of task, so that the original task can be reliably performed [7]. Obviously, opportunistic computing paradigm can be applied in m-Healthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI is personal information and very sensitive to medical users, once the raw PHI data are processed in opportunistic computing, the privacy of PHI would be disclosed. Therefore, how to balance the high reliability of PHI process while minimizing the PHI privacy disclosure during the opportunistic computing becomes a challenging issue in m-Healthcare emergency.

In this paper, we propose a new secure and privacy preserving opportunistic computing framework, called SPOC, 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. specifically, the main contributions of this paper are threefold.

First, we propose SPOC, a secure and privacy preserving opportunistic computing framework for m-healthcare emergency. With SPOC, the resources available on other opportunistically contacted medical users' smart phones can be gathered together to deal with the computing-intensive PHI process in emergency situation. Since the PHI will be is closed during the process in opportunistic computing, to minimize the PHI privacy disclosure, SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing. . Second, to achieve user-centric privacy access control in opportunistic computing, we present an efficient attribute-based access control and a novel non homomorphism encryption-based privacy preserving scalar product computation (PPSPC) protocol, where the attributed-based access control can help a medical user in emergency to identify other medical users, and PPSPC protocol can further control only those medical users who have similar symptoms to participate in the opportunistic computing while without directly revealing users' symptoms. Note that, although PPSPC protocols have been well studied in privacy-preserving data mining [11], [12], [13], yet most of them are relying on time-consuming homomorphic encryption technique [14], [15]. To the best of our knowledge, our novel non homomorphic encryption-based PPSPC protocol is the

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

most efficient one in terms of computational and communication overheads. . Third, to validate the effectiveness of the proposed SPOC framework in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed SPOC framework can help medical users to balance the high reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency.

II. System Model

In our system model, we consider a trusted authority (TA) and a group of l medical users UU ¼ fU1; U2; . . . ; Ulg, 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 2 UU 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. Unlike in-bed patients at home or hospital medical users UU in our model are considered as mobile ones, i.e., walking outside. BSN and Smartphone are two key components for the success of m-Healthcare system. In order to guarantee the high reliability of BSN and Smartphone, the batteries of BSN and Smartphone should be charged up every day so that the battery energy can support daily remote monitoring task in m-Healthcare system. In general, since the BSN is dedicated for remote monitoring, after being charged every day, BSN can deal with not only the normal situations but also the emergency cases in m-Healthcare. However, since the Smartphone could be used for other purposes, e.g., phoning friends, surfing WebPages, when an emergency suddenly takes place, the residual power of Smartphone may be insufficient for high-intensive PHI process and transmission. To deal with this embarrassing situation, opportunistic computing provides a promising solution in m-Healthcare system, i.e., when other medical users find out one medical user Ui 2 UU is in emergency, they will contribute their Smartphone resources to help Ui with processing and transmitting PHI.

III. Security Model

Opportunistic computing can enhance the reliability for high-intensive 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. 3.

Phase-I access control. Phase-I access control indicates that although a passing-by person has a Smartphone with enough power, as a nonmedical user, he is not welcomed to participate in opportunistic computing.1 Since the opportunistic computing requires smart phones 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 software does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite.

A. 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 emergency 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.

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

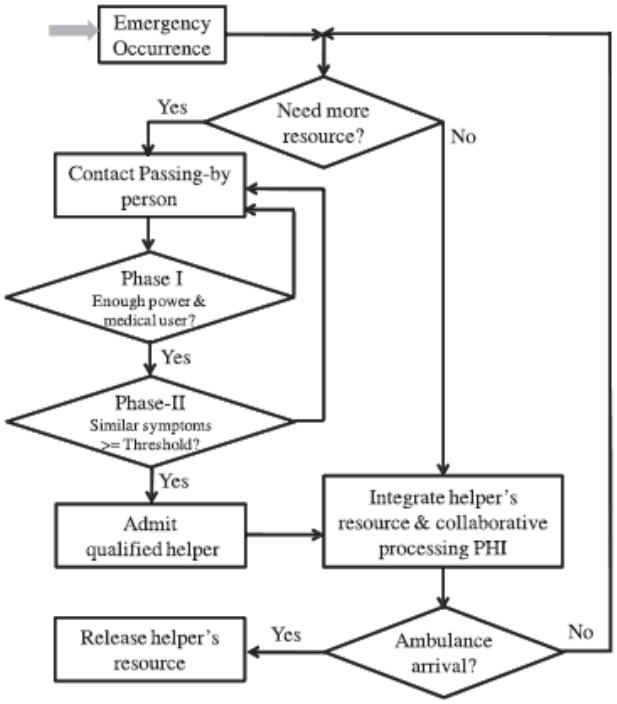


Fig. 3. Opportunistic computing with two-phase privacy access control for m-Healthcare emergency.

IV. Security Model

Opportunistic computing can enhance the reliability for high-intensive 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. 3. Phase-I access control. Phase-I access control indicates that although a passing-by person has a smartphone with enough power, as a nonmedical user, he is not welcomed to participate in opportunistic computing.1 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 emergency 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.

V. Proposed SPOC Framework

In this section, we propose our SPOC framework, which Consists of three parts: system initialization, user-centric Privacy access control for m-Healthcare emergency, and Analysis of opportunistic computing in m-Healthcare Emergency. Before describing them, we first review the Bilinear pairing technique, which serves as the basis of the proposed SPOC framework.

VI. Bilinear Pairings

Definition 1. A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter as input, and outputs a 5-tuple ðq; g;GG;GGT ; eÞ, where q is a bit prime number, GG and GGT are two groups with order q, g 2 GG is a generator, and e : GG _ GG ! GGT is a non degenerated and efficiently computable bilinear map.

VII. Description of SPOC

A. *System Initialization*

For a single-authority m-Healthcare system under consideration, We assume a trusted authority located at the healthcare center will bootstrap the whole system. Specifically, given the security parameter , TA first generates the bilinear parameters Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, a binary vector in the n-dimensional symptom character space, where indicates a symptom.

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

VIII. User-Centric Privacy Access Control for m-Healthcare Emergency

When an emergency takes place in m-Healthcare, e.g., user U0 suddenly falls down outside, the healthcare center will monitor the emergency, and immediately dispatch an ambulance and medical personnel to the emergency location. Generally, the ambulance will arrive at the scene around 20 minutes [25]. During the 20 minutes, the medical personnel needs high-intensive PHI to real time monitor U0. However, the power of U0's Smartphone may be not sufficient to support the high-intensive PHI process and transmission. In this case, the opportunistic computing, as shown in Fig. 3, is launched, and the following user-centric privacy access control is performed to minimize the PHI privacy disclosure in opportunistic computing.

Phase-I access control. The goal of phase-I access control is to identify other medical users in emergency. To achieve the phase-I access control, U0's smartphone first chooses a random number where timestamp is the current timestamp, and send back Authktimestamp to U0. When user U0 receives Authktimestamp at time timestamp0, he first checks the validity of the time interval between timestamp0 and timestamp in order to resist the replaying attack. If jtimestamp0 _ timestamp j _ _T, where _T denotes the expected valid time interval for transmission delay, U0 accepts and processes If it does hold, Uj is authenticated as a medical user, and passes the phase-I access control. Correctness.

Phase-II access control. Once Uj passes the phase-I access control, U0 and Uj continue to perform the phase-II access control to check whether they have some similar symptoms. Suppose the personal health profiles of medical users U0, Uj are respectively. U0 first defines an expected threshold th for the number of Common symptom characters. Then, in order to compute in a privacy-preserving way, U0 and Uj invoke our newly assigned PPSPC protocol in Algorithm 1. Since the PPSPC protocol ensures neither U0 nor Uj will disclose their personal Healthcare profiles to each other during the computation of , it can efficiently achieve privacy preserving access control. For example, if the returned value th, Uj passes the phase-II access control and becomes a qualified helper. Then, U0 assigns the current session key k0 ¼ Hðsk0kCDateÞ to Uj. With the session key k0, Uj can decrypt and process the raw PHI sent from U0's personal BSN, and also transmit the processed PHI to healthcare center to reduce the burden of U0's smartphone. However, if the returned value < th, Uj is not a qualified helper to participate in opportunistic computing. Note that the threshold th is not fixed, if the residual power of U0's smartphone can last a little long time, th can be set relatively high to minimize the PHI privacy disclosure. However, if the residual power is little, th can be set low so as to first guarantee the reliability of high-intensive PHI process and transmission.

IX. 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. Assume that the arrival of users at the emergency location follows a Poisson process denoted as the number of qualified helpers (NQHs) and the number of nonqualified helpers within time. For arriving user at time , the probability that the user is a qualified helper

X. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed SPOC framework. In specific, following the security requirements discussed earlier, our analyses will focus on how the proposed SPOC framework can achieve the user-centric privacy access control for opportunistic computing in m-Healthcare emergency. . The proposed SPOC framework can achieve the phase-I access control. In the phase-I access control, the single attribute encryption technique is employed. the proposed SPOC framework can achieve the phase-II access control. In the phase-II access control, our novel PPSPC protocol is employed.

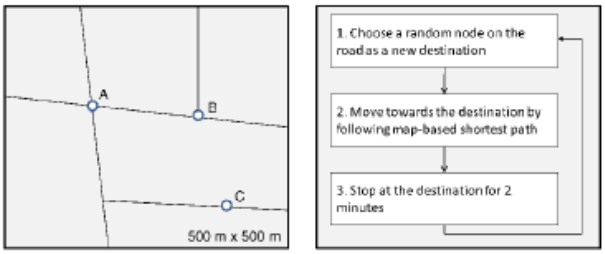
XI. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed SPOC framework using a custom simulator built in Java. The simulator implements the application layer under the assumptions that the communications between smartphones and the communications between BSNs and smart phones are always workable when they are within each other's transmission ranges. The performance metrics used in the evaluation are 1) the average number of qualified helpers, which indicates how

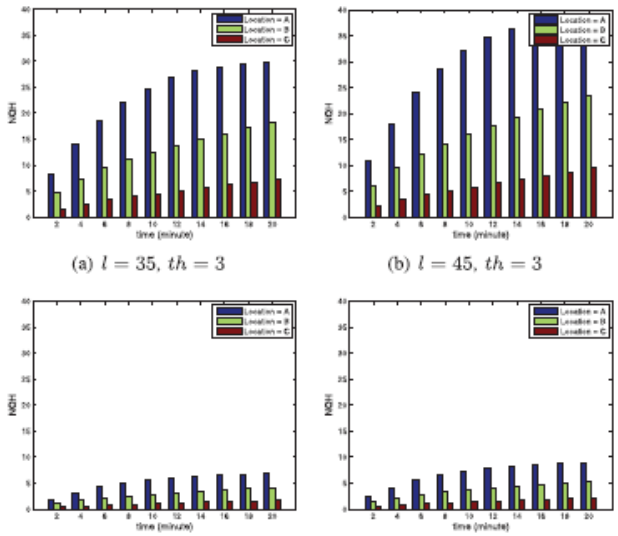
Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

many qualified helpers can participate in the opportunistic computing within a given time period, and 2) the average resource consumption ratio (RCR), which is defined as the fraction of the resources Consumed by the medical user in emergency to the total Resources consumed in opportunistic computing for PHI process within a given time period. Both NGH and RCR can be used to examine the effectiveness of the proposed SPOC framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.



(a) Simulation area (b) Mobility model



(a) $l = 35,\ th = 3$ (b) $l = 45,\ th = 3$

(c) $l = 35,\ th = 5$ (d) $l = 45,\ th = 5$

Fig. 6. NQH varying with time under different l and th.

XII. Simulation Setup:

In the simulations, total l users UU ¼ fU0; U1; . . . ; Ul_1g are first uniformly deployed in an interest area of 500 m _ 00 m, as shown in Fig. 5a. Each user Ui 2 UU is equipped with his personal BSN and a smartphone with a transmission radius of 20 m, and independently moves along the road with the velocity v 2 ½0:5; 1:2 m=s in the area by following the mobility model described in Fig. 5b. Assume that the symptom character space n ¼ 16, each user is randomly assigned 6-8 symptom characters. Let the emergency of user U0 take place at time t ¼ 0, he sets the
threshold th as f3; 5g, and waits the qualified helpers participating in the opportunistic computing before the ambulance arrives in 20 minutes. Note that, in the simulations, we consider all users will stop when they meet U0's emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, we consider U0's emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations. The detailed parameter settings are summarized in Table 1. In the following, we run the simulations with different parameter settings. For each setting, the simulation lasts for 20 minutes (excluding the warm-up time), and the average performance results over 10,000 runs are reported.

XIII. Simulation Results

In Fig. 6, we compare the average NQHs at locations A, B and C varying with time from 2 to 20 minutes under different user number l and threshold th. From the figure, we can see, with the increase of time, the average NQH will also increase, especially for the location A. The reason is that, when all users move in the simulation area by following the same mobility model, location A will have higher traffic than locations B and C. In addition, when the

TABLE 1
Simulation Settings

Parameter	Setting
Simulation area	500 m × 500 m
Simulation warm-up, duration	10 minutes, 20 minutes
Number, velocity of users	$l = \{40, 60\}$, $v = 0.5 - 1.2$ m/s
Similarity threshold	$th = \{3, 5\}$
Transmission of smartphone, BSN	20 m, 20 m
Raw PHI data generation interval	every 10 seconds
Emergency location	A, B, and C

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

user number l in the simulation area increases, the user arrival rate at locations A, B, and C also increase. Then, the average NQH increases as well. By further observing the differences of the average NQH under thresholds th ¼ 3 and th ¼ 5, we can see the average NQH under th ¼ 5 is much lower than that under th ¼ 3, which indicates that, in order to minimize the privacy disclosure in opportunistic computing, the larger threshold should be chosen. However, since the high reliability of PHI process is expected in m-Healthcare emergency, minimizing the privacy disclosure in opportunistic computing is not always the first priority. In Fig. 7, we plot the corresponding RCR varying with the time under different user number l and threshold th. From the figure, we can observe both high-traffic location, i.e., location A, and large number of users, i.e., l ¼ 45, can reduce the U0's RCR. However, the RCR under th ¼ 5 is higher than that under th ¼ Fig. 6. NQH varying with time under different l and th.Fig. 7.

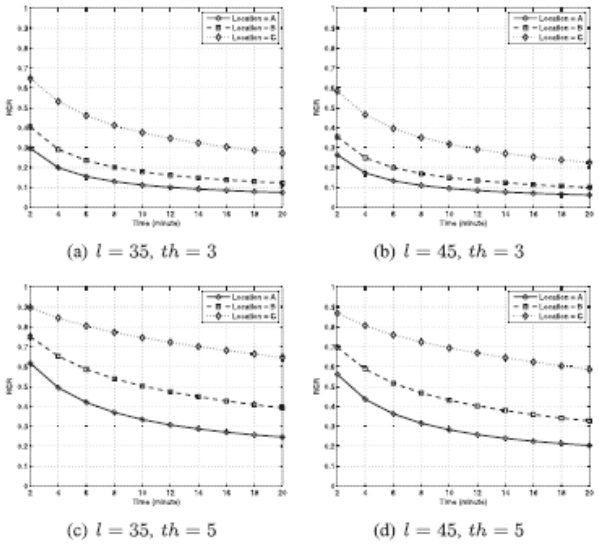


Fig. 7. RCR varying with time under different l and th.

Therefore, once U0 sets the threshold th ¼ 5 while the residual energy in his smartphone is not enough, his smartphone cannot support high reliability of PHI process and transmission before the ambulance arrives. This indicates U0 should carefully choose the threshold th to balance the high reliability of PHI process and privacy disclosure. For example, if the emergency takes place at a high traffic location and the residual energy in U0's smartphone is not too low, U0 can choose a relative high threshold to minimize the privacy disclosure. However, if the emergency location has low traffic and the Smartphone's energy is also insufficient, th should be as low to first fit the high-reliability of PHI process and transmission in m-Healthcare emergency.

XIV. CONCLUSIONS

In this paper, we have proposed a secure and privacy preserving opportunistic computing framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed SPOC framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency. In our future work, we intend to carry on smartphone-based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

XV. REFERENCES

[1] A. Toninelli, R. Montanari, and A. Corradi, "Enabling Secure Service Discovery in Mobile Healthcare Enterprise Networks,"
IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 2009.
[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Handshake with Symptoms-Matching: The Essential to the Success of Mhealthcare Social Network," Proc. Fifth Int'l Conf. Body Area (BodyNets '10), 2010.
[3] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., vol. 16, no. 6, pp. 683-694, 2011.
[5] 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 Trans. Parallel and Distributed System, to be published.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 2, Issue 1, No 4, 2014. ISSN: 2348-6600.
Reference ID: IJCS-047. PAGE NO: 265-272.

[6] M.R. Yuce, S.W.P. Ng, N.L. Myo, J.Y. Khan, and W. Liu, "Wireless Body Sensor Network Using Medical Implant Band," J. Medical Systems, vol. 31, no. 6, pp. 467-474, 2007.
[7] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic Computing for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), pp. 1-6, 2007.
[8] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance Evaluation of Service Execution in Opportunistic Computing," Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.
[9] M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.
[10] M. Conti and M. Kumar, "Opportunities in Opportunistic Computing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.

Published by SK Research Group of Companies (SKRGC).