IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Merging Patient And Doctor Through Spoc In Android

S.C.Balaji[1], J.Govindarajan[2], B.Saravanakumar[3] and Dr.R.Sugumar[4]

[1, 2, 3] Computer Science and Engineering,
Vel Tech Multi TechDr.RR Dr.SR engineering college,
Chennai,TamilNadu, India

[4]Associate Professor, Computer Science and Engineering,
Vel Tech Multi TechDr.RR Dr.SR engineering college,
Chennai,TamilNadu, India

ABSTRACT

In, which uses smart phone resources includes computing power and energy can be opportunistically gathered to process the personal health information (PHI) 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.

Keywords*:Personal health information(PHI);secure and privacy-preserving opportunistic computing framework(SPOC);PPSC.*

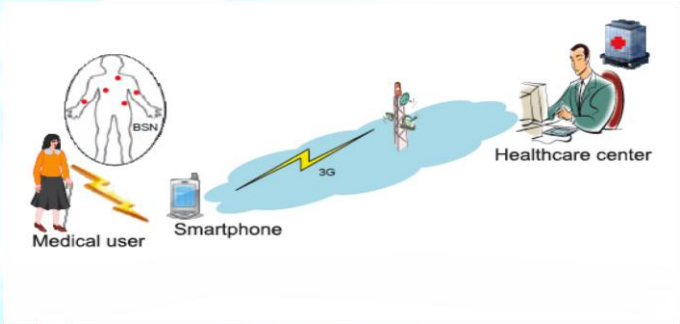

Fig.1 Personal Health Information

I. INTRODUCTION

In our 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. 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 medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. For example, as shown in Fig. 1, 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. 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 users' health conditions and as well quickly reactto users' 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 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 personnel's arrival. However, since smart phone 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.

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. 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. Obviously, opportunistic computing paradigm can be applied in m-Healthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI are 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.

Secure and privacy- In this paper,

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' smartphones can be gathered together to deal with the computing- intensive PHI process in emergency situation. Since the PHI will be disclosed 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-homomorphic 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, yet most of them are relying on time-consuming homomorphic encryption technique. To the best of our knowledge, our novel non-homomorphic encryption based PPSPC protocol is the 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.

The remainder of this paper is organized as follows. In Section 2, we formalize the system model and security model, and identify our design goal. Then, we present the SPOC framework in Section 3, followed by the security analysis and performance evaluation in Section 4 and Section 5, respectively. We also review some related works in Section 6. Finally, we draw our conclusions in Section 7.

II. MODELS AND DESIGN GOAL

In this section, we formalize the system model and security model, and identify our design goal as well.

a.System Model

In our system model, we consider a trusted authority (TA) and a group of l medical users U = {U1,U2,⋯,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. Unlike in-bed patients at home or hospital medical users U 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 everyday 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 everyday, 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∈ U is in emergency, they will contribute their smartphones' resources to help Ui with

processing and transmitting PHI.

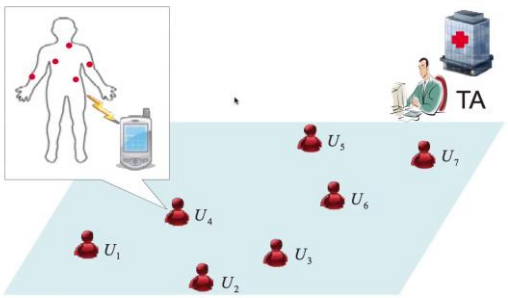

Fig. 2. System model under consideration

b. 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.

*1) 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 par- ticipate in opportunistic computing1. Since the opportunistic computingrequiressmartphonesthat are installed with the same medical software's to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary software's does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite.

*2) 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 dis- closure. 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.

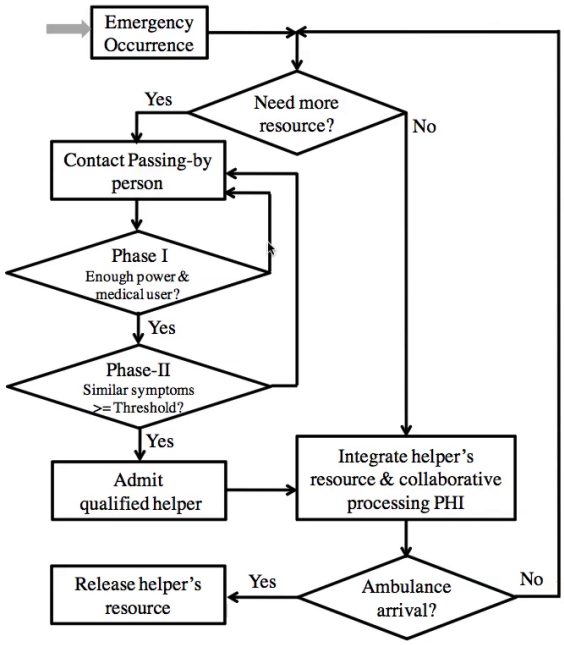

Fig.3 Emergency Flow Chart

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; and ii) develop user-centric privacy access control to minimize the PHI privacy disclosure.

III CONCLUSION

In this paper, we have proposed a secure and privacy- preserving opportunistic computing (SPOC) 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 SPOC with internal attackers, where the internal attackers will not honestly follow the protocol.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure shar- ing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed System*, to appear.

[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," *Journal of 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," in *IEEE Proc. of MASS'07,* pp. 1–6.

[8] 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.

[9] 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.

[10] M. Conti and M. Kumar, "Opportunities in opportunistic computing," *IEEE Computer*, vol. 43, no. 1, pp. 42–50, 2010.

[11] W. Du and M. Atallah, "Privacy-preserving cooperative statistical anal- ysis," in *Proc. of ACSAC '01,* 2001, pp. 102–111.

[12] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *Proc. of ACM KDD'02,* pp. 639–644.

[13] A. Amirbekyan and V. Estivill-Castro, "A new efficient privacy-preserving scalar product protocol," in *Proc. of AusDM '07,* pp. 209–214.

[14] P. Paillier, "Public-key cryptosystems based on composite degree resid- uosity classes," in *Proc. of EUROCRYPT'99,* 1999, pp. 223–238.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel Distributed and Systems*, to appear.

[16] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy- preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[17] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 51–58, 2010.

[18] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," *IEEE Transactions on Parallel Distributed and Systems*, vol. 21, no. 6, pp. 754–764, 2010.

[19] "Exercise and walking is great for the alzheimer's and demen- tia patient's physical and emotional health," http://free-alzheimers-support.com/wordpress/2010/06/exercise-and-walking/, June 2010.

[20] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "Grs: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28–35, 2011.

[21] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. of CRYPTO'01,* 2001, pp. 213–229.

[22] X. Lin, X. Sun, P. Ho, and X. Shen, "Gsis: A secure and privacy preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, 2007.

[23] R. Lu, X. Lin, H. Zhu, , and X. Shen, "An intelligent secure and privacy- preserving parking scheme through vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2772–2785, 2010.

[24] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Transactions on Vehicular Technology*, vol. 61, pp. 86–96,

2012.

[25] http://www.uaproperty.com/articles/In-Ukraine-ambulance-come-patient-10-minutes.html.

[26] S. Ross, *Introduction to Probability Models, Ninth Edition,* 2007.

[27] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets," in *Proc. of INFOCOM'11,* 2011, pp. 2147–2155.

[28] W. Du and Z. Zhan, "Building decision tree classifier on private data," in *Proc. of CRPIT '14,* ser. CRPIT '14, 2002, pp. 1–8.

[29] I. Ioannidis, A. Grama, and M. Atallah, "A secure protocol for comput- ing dot-products in clustered and distributed environments," in *Proc. of ICPP '02,* 2002, pp. 379 – 384.

[30] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Prof. of INFOCOM'11,* 2011, pp. 1647– 1655.

[31] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in *Prof. of INFO- COM'12,* 2012, pp. 1–9.

[32] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *INFOCOM,* 2011, pp. 2435–2443.