Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160

Research Paper | Engineering

Privacy-Preserving Emergency In M-Healthcare Emergency Monitoring Framework Using Smart Phones

E.P.Narayanan Final Year M-tech, SRM University, Chennai

T.Iyyapaswamy Annapoorana Engineering College

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. Health Care is very important factor in life, may be due to unexpected changes in health May causes some health problem in our daily life like sudden hardtack or occurrence of accidents, due to sudden occurrence of problem in health it may leads to serious conditions. To reduce this problem our paper is going to present a mobile itself a plenty of applications as repository, on adding the new health care application in mobile, it provides the user knowledge of disaster management of health problems. The system further integrates with GPS, Google Search and Google Map functionalities to facilitate the user to find all hospitals near to his/her current location including address, phone number, directions to the selected hospital and street view of the selected hospital.

KEYWORDS : Health care in mobile, mobile health care application, Mobile-Healthcare emergency, opportunistic computing, user-centric privacy access control.

Introduction

There is no doubt that healthcare is a social-scale problem. Especially with the elderly populations increasing, the burden of healthcare is steadily increasing. Also, health care providers are faced with a shrinking professional care giving force, which means there is a need for the patients' family members, friends and communities to involve in the care activities. Thus, there is an urgent need for building collaborative care environment to maximize caregivers' efficacy, to improve the safety and quality of care by providing timely health information to professional health care providers, patients and patients' family

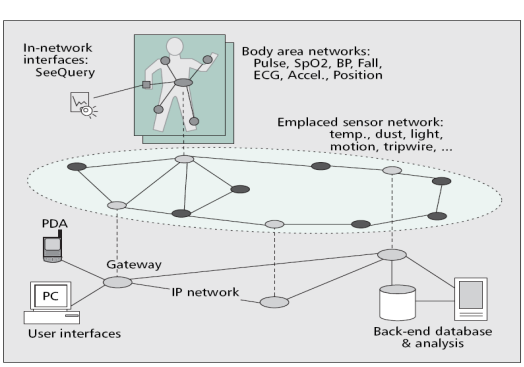
Literature Review

We summarize the healthcare system as two categories: 1) health mentoring system which is designed for monitoring physical vital signs of patients like blood glucose level, ECG and blood pressure; 2) health support system which is designed to facilitate the people's daily activities like taking medicine timely and completely, exercise and taking healthy food.

2.1 Health monitoring system

2.1.1 Common architectures for health monitoring system

Wireless sensor networks (WSNs) and smart phone technology have opened up new opportunities in health monitoring system. The integration of the existing specialized medical technologies with cell phone and wireless sensor networks is a very promising application in home monitoring, medical care, emergency care and disaster response. In the emergency situations, the most important thing is to determine the rapid and accuracy triage of the patients with limited resource. And the real-time and continuous triage information must be distributed to health care providers. Light weight and no-intrusive biomedical sensors like pluse oximeter and electrocardiogram are easy to be deployed for continuously monitoring the vital signs of a patient and deliver the data to the first responders[5][6][7].



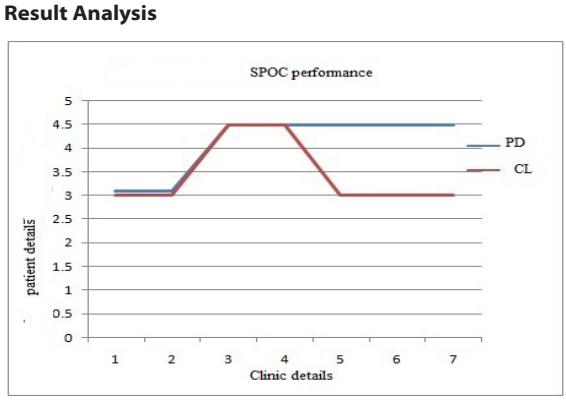
Methods

User-Centric Privacy Access Control for m-Healthcare Emergency

When an emergency takes place in m-Healthcare, e.g., user U_0 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 highintensive PHI to realtime monitor U_0. However, the power of U_0'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.

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 smartphones 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 (NQH), which indicates how 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.

Result Analysis



we compare the average NQHs at locations A, B and C varying with time from 2 minutes to 20 minutes under different user number *I* and threshold *th*. From the figure, we can see, with the increase of time, the

average QH 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 user number *I* in the simulation area increases, the user arrival rate at locations A, B, and C also increase.

Conclusion

we propose a privacy-preserving emergency call scheme, called PEC, enabling patients in life-threatening emergencies to fast and accurately transmit emergency data to the nearby helpers via mobile healthcare social networks (MHSNs). Once an emergency happens, the personal digital assistant (PDA) of the patient runs the PEC to collect the emergency data including emergency location, patient health record, as well as patient physiological condition. The PEC then generates an emergency call with the emergency data inside and epidemically disseminates it to every user in the patient's neighborhood. If a physician happens to be nearby, the PEC ensures the time used to notify the physician of the emergency is the shortest. We show via theoretical analysis that the PEC is able to provide fine-grained access control on the emergency data, where the access policy is set by patients themselves. More- over, the PEC can withstand multiple types of attacks, such as identity theft attack, forgery attack, and collusion attack. We also de- vise an effective revocation mechanism to make the revocable PEC (rPEC) resistant to inside attacks. In addition, we demonstrate via simulation that the PEC can significantly reduce the response time of emergency care in MHSNs.

we have proposed a secure and privacypreserving 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 PPSPC 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. 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. | [6] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp. 1–6. | [7] 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. | [8] 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. | [9] M. Conti and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, 2010. | [10] W. Du and M. Atallah, "Privacy-preserving cooperative statistical analysis," in Proc. of ACSAC '01, 2001, pp. 102–111. | [11] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. of ACM KDD'02, pp. 639–644. | [12] A. Amirbekyan and V. Estivill-Castro, "A new efficient privacypreserving scalar product protocol," in Proc. of AusDM '07, pp. 209–214. | [13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. of EUROCRYPT'99, 1999, pp. 223–238. | [14] 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. | [15] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacypreserving scheme against global eavesdropping for ehealth systems," IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365–378, 2009. | [16]. Wan-Young Chung, Chiew-Lian Yau, Kwang-Sig Shin, and ksto Myllyla, A Cell Phone Based Health Monitoring System with Self Analysis Processor using Wireless Sensor Network Technology, Proceedings of the 29th Annual International Conference of the IEEE EMBS Cite Internationale, pp 3705-3708, Lyon, France August 23-26, 2007. | [17]. Benny P.L.Lo,Surapa Thiemjarus,Rachel King,Guang-zhong Yang, Body Sensor Network - A Wireless Sensor Platform for Pervasive Healthcare Monitoring, Adjunct Proceedings of the 3rd International conference on Pervasive Computing (PERVASIVE'05), pp 77-88, May 2005. | [18]. José M. Reyes Álamo, Johnny Wong, Ryan Babbitt, Carl Chang. MISS: Medicine Information Support System in Smart Home Environments. pp 185-199, ICOST 2008. | [19]. José M. Reyes Álamo, Hen-I Yang, Ryan Babbitt, Johnny Wong and Carl Chang, Support for Medication Safety and Compliance in Smart Home Environments. International journal of advanced pervasive and ubiquitous computing, Volume 1, Issue 3, IGI Global, 2009. | [20]. Fuchao Zhou, Hen-I Yang, José M. Reyes Álamo, Johnny S. Wong, Carl K. Chang, Mobile Personal Health Care, System for Patients with Diabetes, Volume 6159/2010, pp 94-101, ICOST 2010. |