A PROTECTED AND PRIVATE OPPORTUNISTIC COMPUTING SYSTEM FOR MOBILE-HEALTHCARE EMERGENCY

Arindam Dasgupta[1] and Kothari Namita N.[2]
[1]Dept of IT, University of Pune, Sangamner, Maharashtra, India
[2]M.E I.T, Dept of IT, University of Pune, Sangamner, Maharashtra, India

ABSTRACT

With widespread of smart phones and the progress of wireless Body Sensor Networks(BSNs),mobile healthcare (m-Healthcare) is used for better health monitoring and is seeking a lot of attention towards it. But m-Healthcare still faces some problems like information security and preservation of private data. With the help of this we propose a protected and private opportunistic computing system. Therefore with the help of this, different smart phone resources such as energy and computing power can be opportunistically collected for the processing of intensive Personal Health Information (PHI) during m-Healthcare emergency with least possible privacy access control and a technique called Privacy-Preserving Scalar Product Computation (PPSPC) which allows a medical user to think who can participate in opportunistic computing to help in the processing of very large PHI data. The proposed framework in m-Healthcare emergency can effectively and easily gain user-centric privacy control with the help of detailed security analysis. Through extensive simulations, performance evaluation demonstrate the system's effectiveness by providing highly trusted PHI process and transmission during-Healthcare emergency while minimizing the privacy disclosure.

KEYWORDS: *Opportunistic Computing, m-Healthcare, BSN, PHI, PPSPC*

I. INTRODUCTION

Mobile healthcare system has been envisioned for future events and an important application of pervasive computing by improving quality of health care and save lives. For this Smartphone and implantable body sensor nodes are used by providing remote healthcare super visioning to people who have long term disease such as blood pressure and diabetes [2], [3], [4], [5], [6]. It is not necessary that, medical users are needed to be continuously monitored within home and hospital environments. Instead of this, in m-Healthcare they are being supplied with Smartphone and wireless body sensor networks (BSN) which are produced by body sensor nodes. Medical users receive the high-quality healthcare monitoring from medical professionals anytime and anywhere outside. Suppose for example as shown in following fig 1, personal health information(PHI) of mobile medical user can be taken by BSN like heartbeat, weight, blood sugar level, blood pressure, temperature etc. and sent by Smartphone through Bluetooth. Then they get transmitted to the remote healthcare center via 3G networks [1]. On the basis of these whole PHI data, medical professionals who are available at healthcare center can constantly monitor medical users health conditions and quickly response to users life-threatening or any dangerous situations and save their lives by sending off an ambulance and medical professional to an that location. Although m-Healthcare provides high-quality healthcare monitoring, but it still facing and managing the challenges in m-Healthcare system, especially in case of medical emergency. Therefore to understand the challenges clearly, we assume the following scenario that a medical user's PHI should be updated to the healthcare center for every 5 minutes for monitoring [7]. So whenever any emergency condition occurs like heart attack, his body sensor nodes will be taking different medical measures like blood pressure, heart rate, temperature and within a short period of time, few amount of data will be formed and they should be reported every 10 seconds with highly monitoring before any medical personnel or ambulance arrival. In m-Healthcare system, patient's PHI is one of the primary issues that have to keep in secret and can be readable only by

medical professionals at m-Healthcare center. Two patients can have same symptom, so that they can share their experience, health condition, support and encourage each other to remove unwanted loneliness. These security issues should be considered and which is very serious issue and indicates the reliability of m-Healthcare is still facing problems in emergency cases. In recent years, opportunistic computing which is a proposed mobile computing paradigm, extending the application areas of pervasive computing and networking [8], [9], [10], [11]. Essentially, in opportunistic networks, nodes exploits all available computing resources and contribute and avail of each other's resources in an opportunistic environment to provide a platform for the execution of computing-intensive task in distributed environment[11]. And this paradigm can be applied in m-Healthcare emergency to solve the reliability issue in PHI process.

We propose a new protected and private opportunistic computing system for mobile healthcare emergency. Using this framework system, each patient in emergency can achieve the user-centric privacy access control to permit only those ideal helpers to participate in the opportunistic computing to minimize the privacy disclosure and highly reliable PHI process. Actually, the main contributions of this paper are threefold. 1) Firstly, we define, a protected and private opportunistic computing system for mobile healthcare emergency. With this framework, the different resources which are available on other opportunistically contacted patient's Smartphone can be collected together to handle with the computing-intensive PHI process in emergency cases. 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) Secondly, we guarantee the user-centric privacy access control. For that, an efficient attribute based control and a non-homomorphic encryption based privacy preserving scalar product computation (PPSPC) protocol is presented. Attribute based access control can support patient in emergency to identify other medical users. Then PPSPC protocol can controlled by those patients who have same symptoms to participate while without directly exposing user's symptoms. These PPSPC protocols are related to time-consuming homomorphic encryption technique [12], [13] but our novel non-homomorphic encryption based PPSPC protocol is the most efficient and best regarding to computational and communication overheads.3)Thirdly, 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 balanced the high reliability of PHI process and minimizing the privacy disclosure compared with ordinary PHI reporting without social collaboration.

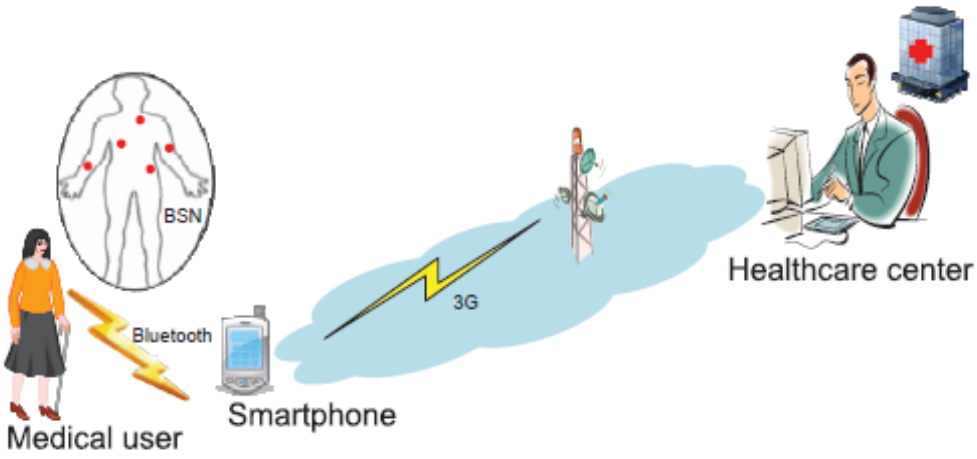

Fig. 1. Health monitoring in m-Healthcare system

The rest of this paper is organized as follows. In section II, we introduce background and some related concepts of the paper. In section III, we present existing systems and related works. We propose our protected and private opportunistic computing system for mobile-healthcare emergency and its architecture in section 4. Finally we draw our conclusions and future work in section V and section VI respectively.

II. BACKGROUND

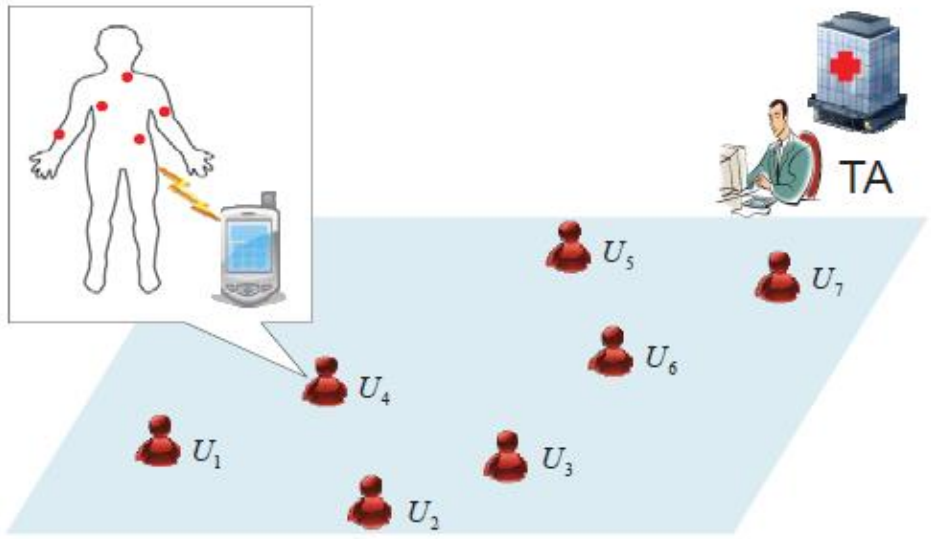

Fig.2. System model under consideration

Trusted Authority(TA) is mainly responsible for the management of total m-Healthcare system such as initializing the system, equipping proper body network nodes and key materials to patients. Therefore it acts as a trustable and powerful entity. In this process, each patient is equipped with Smartphone and BSN, which collects PHI periodically and report them to healthcare center to achieve good healthcare quality [1].

In m-Healthcare, PHI is very sensitive, a patient, even in emergency. So, opportunistic computing can be used to enhance the reliability and transmission in m-Healthcare emergency. Opportunistic computing with two-phase privacy access control for m-Healthcare emergency defines a security model which is required for achieving high reliable PHI process and transmission in m-Healthcare emergency, as shown in fig 3. Phase 1 access control indicates that although a passing-by person has a Smartphone and who is non-medical user, he can't participate in opportunistic computing. If passing by person having Smartphone and is not medical user and if he is not having necessary software's, it doesn't make him an ideal helper. In phase 2 access control, it only allows those patients who have same symptoms to participate in opportunistic computing. Due to this, similar symptoms processes same type of PHI. Here, threshold *th* is a user self-control parameter and threshold will be high when energy takes place with a high traffic at a location otherwise it will be low [1].

III. EXISTING SYSTEM

In existing system, according to the sensex over the age of 65, is expected to hit 70 million by 2030, is doubled since 2000 healthcare expenditures projected to increase to 15.9% by 2010. The cost of health care for nation's aging population has become a national concern are important for understanding how the opportunistic computing paradigm work when different resources available on different nodes can be opportunistically collected together to provide greater functionality, they have not considered the privacy and security related issues that are existing in opportunistic computing paradigm. The emerging technologies for assisting physicians to order medicines, provide care, and manage nursing efforts are included in existing system. Information technologies are often applied to different medical units like surgery, inventory to enhance processes and extend the reliability of diagnosis, to reduce human error, and to search for and provide appropriate medical information. Mobile technology has also been produced and used in hospitals to enhance real-time monitoring and nursing care using mobile and wireless communication networks. The speed and security of data transfers for mobile information technology are key factors considered by the users of these systems. In order for mobile information technology to integrate tracking, monitoring, and detection

technologies, the nursing processes and records must be well defined and streamlined. Hospitals are beginning to adopt information technologies in an attempt to lower equipment costs, improve processing times, and also allow for focused patient care. Hence, existing healthcare systems re-engineering consists of identifying the information technologies that will improve processes and also reducing operation complexity, eliminating redundancy with lowering costs.

IV. PROPOSED SYSTEM

In our proposed framework, which aims at the security and privacy issues and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency to provide high reliability of PHI process and transmission by minimizing PHI privacy disclosure [1]. We have two approaches-1) Use opportunistic computing in m-Healthcare emergency by providing high reliability of PHI process.2) Produce the user-centric privacy access control for minimizing the PHI privacy disclosure.

In following figure, phase-I access control shows that suppose a passing-by person, which is non-medical user and he has Smartphone with enough power but he can't participate in opportunistic computing. And this paradigm requires Smartphone with necessary software to cooperatively process the PHI. If he doesn't have that software then it does not make him an ideal helper. Hence the phase-I privacy access control is necessary for further proceedings.

In phase-II access control there are only those patients who have similar symptoms to participate in opportunistic computing. Due to this, a system processes same type PHI due to similar symptoms. 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.

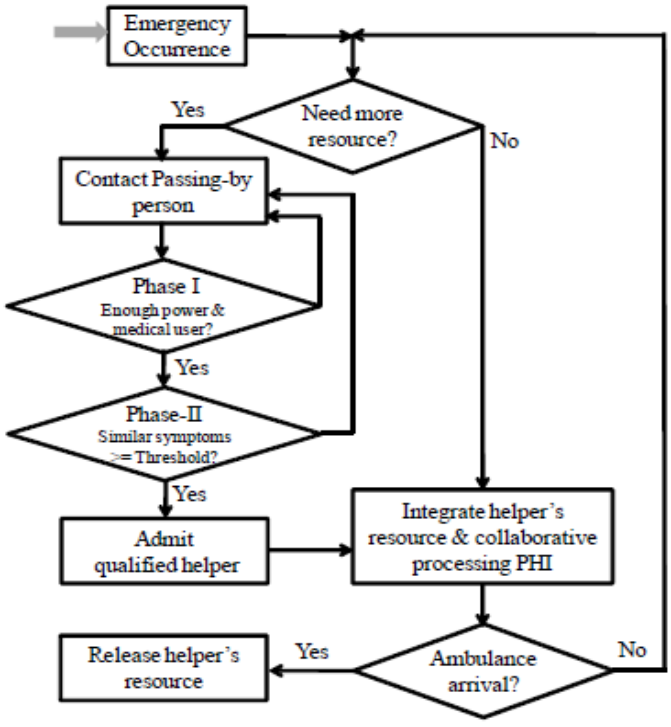

Fig. 3. Opportunistic Computing with two-phase privacy access control for m-Healthcare emergency

V. CONCLUSIONS

A protected and private opportunistic computing system for mobile-healthcare emergency, has been paid great attention, which mainly focuses how to use opportunistic computing to achieve highly reliable PHI process and transmission in emergency while minimizing the privacy disclosure with the provable security technique, the proposed system has been demonstrated to be secure in the m-

Healthcare scenarios. Since the proposed system will not disclose each other's symptom information if two patients don't have same symptom, this system can be widely accepted by patients, so that they can enjoy the benefits such as eliminating the loneliness in our aging society. In addition we have also demonstrated the proposed framework that can balance high-intensive PHI process and transmission by extensive performance evaluation in m-Healthcare emergency.

VI. FUTURE WORK

In our future work, we expect to carry on Smartphone based experiments to verify the effectiveness and efficiency of the proposed framework. We will also exploit various security issues of PPSPC with internal attacks, where they will not honestly follow the protocol. Once technology is invented, high medical costs will be reduced for correcting chronic medical conditions and our society will benefit from their increased productivity and societal contributions.

REFERENCES

[1]. Rongxing Lu,Xiadong Lin and Xuemin(Sherman), "SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Transactions on Parallel and Distributed Systems, vol.XX,no.XX,XX 2012.
[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]. A. Toninelli, R. Montanari, and A. Corradi, "Enabling secure service discovery in mobile healthcare enterprise networks," *IEEE Wireless Communications*, vol: 16, 24-32, 2009.
[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]. 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.
[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.
[11]. M. Conti and M. Kumar, "Opportunities in opportunistic computing," *IEEE Computer*, vol. 43, no. 1, pp. 42–50, 2010.
[12]. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT'99*, 1999, pp. 223–238.
[13]. 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.

AUTHORS

Arindam Dasgupta received his B. Tech and M.Tech Degree in Information Technology. His currently working as a Professor in Pune University. His research interests include Artificial Intelligence.

Namita Kothari her B.E in information Technology from Pune University, in 2012.She is currently doing her M.E in Information Technology from University of Pune