IJRRECS/August 2013/Volume-1/Issue-4/338-343 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# A SAFE AND CONFIDENTIALITY SAFEGUARDING OPPORTUNISTIC COMPUTING FRAMEWORK

**M.Sree Ram Kiran Nag[1], Y.Madhusekhar[2]**

[1]M.Tech Student, Dept of CSE, RRS College of Engineering and Technology, Patancheru, Medak, A.P, India

[2]Associate Professor, Dept of CSE, RRS College of Engineering and Technology, Patancheru, Medak, A.P, India

**ABSTRACT:**

With the popularity of smart phones and the progress of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which expands the process of Healthcare provider into a persistent environment for enhanced health monitoring, has fascinated substantial interest recently. However, the increase of m-Healthcare still faces many challenges including information safety and confidentiality safeguarding. In this paper, we propose a safe and privacy preserving opportunistic computing framework, called SPOC, for m-Healthcare crisis. With SPOC, smart phone assets including computing control and energy can be opportunistically accumulated to direct the computing concentrated personal health information (PHI) during m-Healthcare emergency with negligible confidentiality discovery. In specific, to influence the PHI privacy disclosure and the high consistency of PHI process and broadcast in m-Healthcare emergency, we launch a resourceful user-centric confidentiality access control in SPOC structure, which is based on an attribute-based access power and a new privacy preserving scalar product computation (PPSPC) technique, and permits a medical user to choose who can take part in the opportunistic computing to help in processing his irresistible PHI data. Detailed safety analysis shows that the proposed SPOC framework can proficiently accomplish user-centric confidentiality access control in m-Healthcare emergency.

***Keywords: Wireless Body Sensor Networks, Mobile Healthcare, SPOC, Personal Health Information, Attribute Based Access, PPSPC, User Centric.***

## 1. INTRODUCTION:

In a Mobile Healthcare system, medical users are no longer essential to be monitored inside home or hospital atmosphere [1]. Mobile Healthcare system has been envisioned as an essential application of pervasive computing to progress health care excellence and save lives, where body sensor nodes and smart phones are making use to contribute inaccessible healthcare observing to persons who have chronic medical situations such as diabetes and heart disease [2]. Medical users can walk outside and be given the high-quality healthcare monitoring from medical expert anytime and anywhere after being equipped with smart phone and wireless body sensor network formed by body sensor nodes. Every mobile medical user's personal fitness information such as blood pressure, heart beat and temperature can be initially collected by body sensor nodes, and then combined by smart phone by means of blue tooth [3] [5].

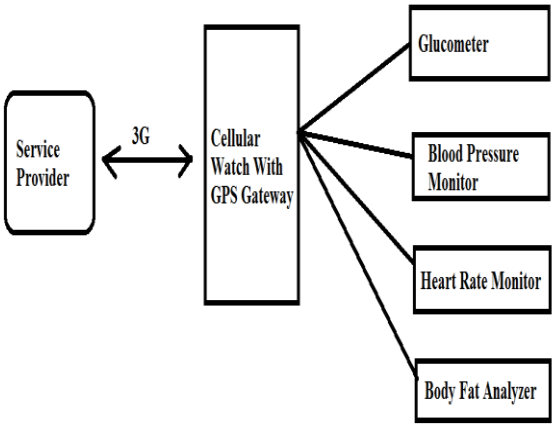


**Fig 1: Mobile Healthcare System**

Based on these collected personal health information medical proficient at healthcare centre can constantly supervise medical users' health conditions and as well rapidly act in response to user serious situations and put aside their lives by send off ambulance and medical people to an urgent situation location in a timely manner. Even though mobile healthcare system shown in fig1 can benefit medical users by providing premium persistent healthcare observing, the flourish of mobile healthcare system still pivot upon how we fully comprehend and supervise the challenges facing in mobile Healthcare system, particularly throughout a medical urgent situation [4] [7]. In wide-ranging, a medical user's personal health information should be reported to the healthcare centre each five minutes for standard isolated monitoring. Though, when he has an

urgent situation medical condition, for instance heart attack, his body sensor network turn out to be full of activity reading a variety of medical process, such as heart rate, blood pressure, and as a consequence, a large amount of personal health information data will be produced in a very short period of time, and they additional should be reported every ten seconds for high-intensive monitoring earlier than ambulance and medicinal personnel's entrance [6] [8]. On the other hand, in view of the fact that smart phone is not only used for healthcare monitoring, but also for other functions, the smart phone's force could be inadequate when an urgent situation takes place.

## 2. STABILIZING HIGH-RELIABILITY OF PERSONAL HEALTH INFORMATION:

A novel secure and privacy- preserving opportunistic computing framework is proposed. Every medical user in urgent situation can get the user-centric confidentiality admission control to permit only those qualified helpers to contribute in the opportunistic computing to steadiness the high-reliability of personal health information process and reducing personal health information confidentiality revelation in mobile healthcare emergency in secure and privacy- preserving opportunistic computing [9] [11] [12]. A secure and privacy-preserving opportunistic computing framework for mobile Healthcare emergency is proposed. With secure and privacy-preserving opportunistic computing, the resources obtainable on other opportunistically contacted health check users' smart phones can be getting together to contract with the computing-intensive personal health information procedure in emergency circumstances. In view of the fact that the personal health information will be revealed throughout the process in opportunistic computing, to reduce the personal health information privacy disclosure, secure and privacy- preserving opportunistic computing introduces a user-centric two-phase confidentiality access control to only permit those medical users who have similar indications to contribute in opportunistic computing [10] [13]. To attain user-centric privacy admission control in opportunistic computing, a competent attribute- based access control and a new non-homomorphic encryption based privacy-preserving scalar product computation protocol is proposed, where the attributed-based admission control can help a medicinal user in urgent situation to recognize other medical users, and can further manage only those medical users

who have comparable indications to contribute in the opportunistic computing while with no directly revealing users' symptoms [14]. Even though privacy-preserving scalar product computation have been well considered in privacy-preserving data mining so far for the most part of them are relying on prolonged homomorphic encryption practice. Non-homomorphic encryption based privacy-preserving scalar product computation protocol is the most efficient in terms of computational and contact outlay. To authenticate the efficiency of the projected secure and privacy-preserving opportunistic computing structure in mobile Healthcare emergency, we also expand a custom simulator built in Java. Widespread simulation results show that the proposed secure and privacy-preserving opportunistic computing framework can help medical users to steadiness the high-reliability of personal health information process and minimizing the personal health information confidentiality disclosure in mobile healthcare emergency.

## 3. ACCOMPLISHING OF CONSISTENT PERSONAL HEALTH INFORMATION PROGRESSION:

Body sensor network and smart phone are two key constituents for the success of mobile healthcare system. In order to assurance the high consistency of body sensor network and smart phone, the batteries of body sensor network and smart phone should be stimulating up every day so that the battery power can hold up every day distant monitoring task in m-Healthcare system [16]. In general, given that the body sensor network is committed for remote monitoring, after being stimulating every day, body sensor network can deal with not only the standard situations but also the urgent situation in mobile healthcare. In view of the fact that personal health information is very susceptible, a medical user, even in emergency, will not be expecting to reveal his personal health information to all passing-by medical users [15]. As a substitute, he may only reveal to those medical users who have some comparable symptoms with him. The urgent situation can be hold by opportunistic computing with negligible privacy revelation. A two-phase privacy access control in opportunistic computing, which are necessary for accomplishing high-reliable personal health information process and broadcast in mobile Healthcare emergency is defined.

## 4. CONCLUSION:

In this paper, a safe and privacy preserving opportunistic computing (SPOC)

framework for m-Healthcare emergency is proposed, which primarily uses how to use opportunistic computing to accomplish high consistency of PHI process and broadcast in crisis while reducing the confidentiality discovery during the opportunistic computing. Detailed safety analysis shows that the proposed SPOC framework can accomplish a resourceful user-centric privacy access control. In addition, through widespread performance assessment, we have also established the proposed SPOC framework can balance the high concentrated PHI process and broadcast and minimizing the PHI confidentiality discovery in m-Healthcare crisis. In our future work, we propose to transmit on smart phone based experiments to further confirm the efficiency of the proposed SPOC framework.

## 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.