ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2, Issue 2, Ver. 1 (April - June 2014)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

A Secure Health Care Management System

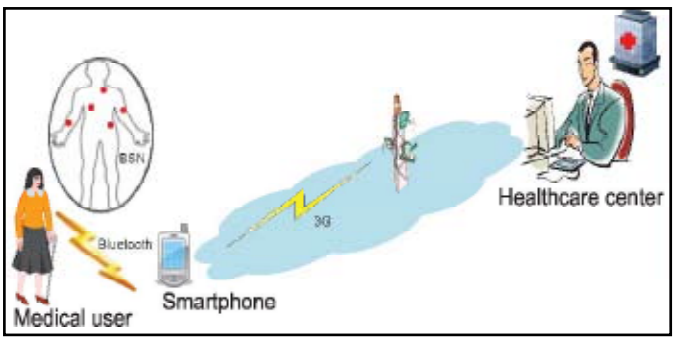
[I]Amisha.N, [II]Mr.Sathish Kumar
[I,II]M.E,CS Dep, Anna University, Chennai, Tamil Nadu, India

Abstract
The m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the growing of m-Healthcare system still strangest on how we fully understand and manage the challenges facing in this m-Healthcare system, especially on during a medical emergency. In this paper, we propose a new secure and privacy-preserving opportunistic computing framework, called SPOC, to address this challenge.
With the help of our proposed SPOC framework, each medical user who is 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-Health care 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 great PHI data.

Keywords
Mobile-healthcare emergency, opportunistic computing, user-centric privacy access control, PPSPC.

I. Introduction

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.



Although m-Healthcare system can benefit medical user by providing high-quality pervasive healthcare monitoring ,the flourish of m-Healthcare system still hinges upon how they 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, they consider the following scenario. In general, a medical user's PHI should be reported to the health care 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 smart phone'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.

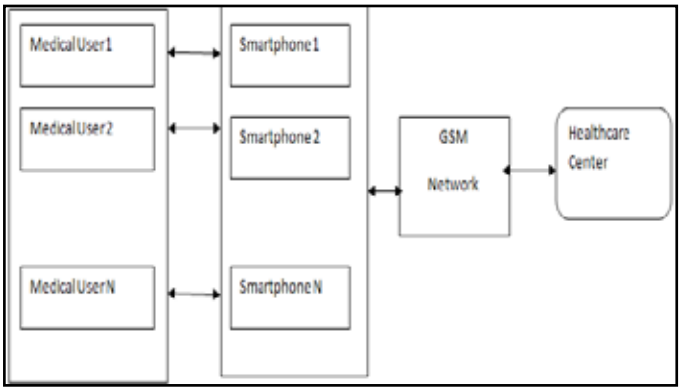
II. Proposed System

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-Health care 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.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

SPOC framework allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. 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. The attributed-based access control can help a medical user in emergency to identify other medical users

III. System Details

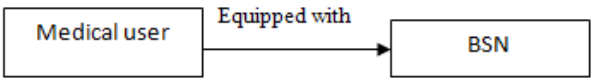


1. Medical users
2. Body Sensor Network (BSN)
3. Smartphone communication
4. Healthcare Center

A. Medical Users

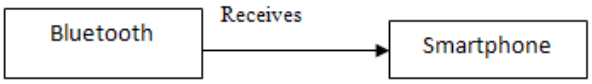
Normally the medical user personal healthcare information (PHI) is mainly invented for monitoring the patients without direct interaction with doctors. In an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smart-phone 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.

B. Body Sensor Network



This sensor will be equipped directly in the medical user. This BSN will transmit the user details for every time period that we have indicated. For example, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and other details will be captured by the medical users Smartphone.

C. Smartphone communication



For each data transmitted from BSN will be aggregated by the Smartphone that, the medical users having with them using Bluetooth communication. This received medical information or symptom will be transmitted to healthcare center periodically with the help of 3G network.

D. Healthcare Center

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 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.

IV. Models

In this section, we formalize the system model and security model.

1. System Model

In our system model, we consider a trusted authority (TA)and a group of l medical users $\mathbb{U} = \{U_1, U_2, \ldots, U_l\}$,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 $U_i \in \mathbb{U}$ is equipped with personal BSN and smart-phone, which can periodically collect PHI and report them.

2. Security Model

Access control indicates that although a passing-by person has a smart-phone 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 softwares does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite. only allows those medical users who have some similar symptoms to participate in the opportunistic computing. There a son 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. Feasibility Study

Feasibility study is the test of a system proposal according to its workability, impact on the organization, ability to meet user needs, and effective use of recourses. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible.

A. Technical Feasibility

The technology used can be developed with the current equipments and has the technical capacity to hold the data required by the new system.

- This technology supports the modern trends of technology.
- Easily accessible, more secure technologies.

Technical feasibility on the existing system and to what extend it can support the proposed addition.We can add new modules easily without affecting the Core Program. Most of parts are running in the server using the concept of stored procedures.

B. Operational Feasibility

This proposed system can easily implemented, as this is based on JSP coding (JAVA) & HTML .The database created is with server which is more secure and easy to handle. The resources that are required to implement/install these are available. The personal of the organization already has enough exposure to computers. So the project is operationally feasible.

C. Economical Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system. An entrepreneur must accurately weigh the cost versus benefits before taking an action. This system is more economically feasible which assess the brain capacity with quick & online test. So it is economically a good project.

The development of a computer based system or a product is more likely plagued by resources and delivery dates. Feasibility study helps the analyst to decide whether or not to proceed, amend, postpone or cancel the project, particularly important when the project is large, complex and costly.Once the analysis of the user requirement is complement, the system has to check for the compatibility and feasibility of the software package that is aimed at. An important outcome of the preliminary investigation is the determination that the system requested is feasible.

VI. Algorithm

The Diffie-Hellman algorithm

This algorithm uses arithmetic modulus as the basis of its calculation. Suppose Alice and Bob follow this key exchange procedure with Eve acting as a man in middle interceptor (or the bad guy).

Here are the calculation steps followed in this algorithm that make sure that eve never gets to know the final keys through which actual encryption of data takes place.

- First, both Alice and Bob agree upon a prime number and another number that has no factor in common. Lets call the prime number as **p** and the other number as **g**. Note that **g** is also known as the generator and **p** is known as prime modulus.
- Now, since eve is sitting in between and listening to this communication so eve also gets to know **p** and **g**.
- Now, the modulus arithmetic says that **r** = (**g** to the power **x**) mod **p.** So **r** will always produce an integer between 0 and **p**.
- The first trick here is that given **x** (with **g** and **p** known) , its very easy to find **r**. But given **r** (with **g** and **p** known) its difficult to deduce **x**.
- One may argue that this is not that difficult to crack but what if the value of **p** is a very huge prime number? Well, if this is the case then deducing **x** (if **r** is given) becomes almost next to impossible as it would take thousands of years to crack this even with supercomputers.
- This is also called the discrete logarithmic problem.
- Coming back to the communication, all the three Bob, Alice and eve now know **g** and **p**.
- Now, Alice selects a random private number **xa** and calculates (**g** to the power **xa**) mod **p** = **ra**. This resultant **ra** is sent on the communication channel to Bob. Intercepting in between, eve also comes to know **ra**.
- Similarly Bob selects his own random private number **xb**, calculates (**g** to the power **xb**) mod **p** = **rb** and sends this **rb** to Alice through the same communication channel. Obviously eve also comes to know about **rb**.
- So eve now has information about **g**, **p**, **ra** and **rb**.
- Now comes the heart of this algorithm. Alice calculates (**rb** to the power **xa**) mod **p Final key** which is equivalent to **(g to the power (xa*xb)) mod p** .
- Similarly Bob calculates **(ra to the power xb) mod p** = **Final key** which is again equivalent to **(g to the power(xb * xa)) mod p**.
- So both Alice and Bob were able to calculate a common **Final key** without sharing each others private random number and eve sitting in between will not be able to determine the **Final key** as the private numbers were never transferred.

When user U_j passes by the emergency location, U_0 sends $C = (C_1, C_2, C_3)$ to U_j. After receiving $C = (C_1, C_2, C_3)$, U_j will perform the following steps:

- Use his access control key $ak_j = (g^{x+at_{j1}}, g^{t_{j1}}, g^{t_{j2}}, h_1^{t_{j1}} h_2^{t_{j2}})$ to compute

$$\frac{e(C_1, g^{x+at_{j1}})}{e(g^{t_{j2}}, C_2) \cdot e(g^{t_{j2}}, C_3) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, C_1)}$$
$$= \frac{e(g^s, g^x g^{at_{j1}})}{e(g^{t_{j2}}, g^{as} \cdot h_1^{-s}) \cdot e(g^{t_{j2}}, h_2^{-s}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)}$$
$$= \frac{e(g^s, g^x) e(g^s, g^{at_{j1}})}{e(g^{t_{j2}}, g^{as}) e(g^{t_{j2}}, h_1^{-s}) \cdot e(g^{t_{j2}}, h_2^{-s}) \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)}$$
$$= \frac{e(g^s, g^x)}{e(g^s, h_1^{t_{j1}} h_2^{t_{j2}})^{-1} \cdot e(h_1^{t_{j1}} h_2^{t_{j2}}, g^s)} = e(g, g)^{xs}.$$

VII. Related Works

Opportunistic computing-The study of opportunistic computing has gained the great interest from the research community recently, and we briefly review some of them related to our work [7-10]. In [7], Avvenutietal. introduce the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node. Especially, their solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules, and each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes. In [8], Passarell aetal evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services, that are opportunistically contributed by providers and invoked by seekers. Then, they present a complete analytical model to depict the service invocation process between seekers and providers, and derive the optimal number of replicas to be spawned

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used. Although [7] and [8] are important for understanding how the opportunistic computing paradigm work when resources available on different nodes can be opportunistically gathered together to provide richer functionality, they have not considered the potential security and privacy issues existing in the opportunistic computing paradigm [9], [10]. Different from the above works, our proposed SPOC framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

VIII. Conclusion

In this paper, we have proposed a secure and privacy preserving opportunistic computing framework for m-Healthcare emergency, which mainly explain 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 smart phone-based experiments to further verify the effectiveness of the proposed SPOC framework and also to identify the place where the patient ,at the time of emergency.

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 withSymptoms-Matching: The Essential to the Success of Mhealthcare Social Network," Proc. Fifth Int'l Conf. Body Area Networks (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.*

[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.*

[11] *W. Du and M. Atallah, "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf.(ACSAC '01), pp. 102-111, 2001,*

[12] *J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '02), pp. 639-644, 2002.*

[13] *A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," Proc. Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), pp. 209-214, 2007.*

[14] *P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99), pp. 223-238, 1999.*

[15] *R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Comm.," IEEE Trans. Parallel Distributed and Systems, to be published.*

[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 J. Selected Areas in Comm., vol. 27, no. 4, pp. 365-378, May 2009.*

[17] *M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm., vol. 17, no. 1, pp. 51-58, Feb. 2010.*

[18] *J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," IEEE Trans. Parallel Distributed and Systems, vol. 21, no. 6, pp. 754-764, June 2010.*

[19] *"Exercise and Walking is Great for the Alzheimer's and Dementia Patient's Physical and Emotional Health," http:// freealzheimers support.com/wordpress/2010/06/exercise-andwalking/,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 Comm. Magazine, vol. 49, no. 4, pp. 28- 35, Apr. 2011.*

[21] *D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Ann. Int'l Conf. Cryptology Organized (CRYPTO'01), pp. 213-229, 2001.*

[22] *X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for vehicular communications," IEEE Trans. Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.*

[23] *R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6,pp. 2772-2785, July 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 Trans. Vehicular Technology, vol.*

61, pp. 86-96, 2012.

[25] http://www.uaproperty.com/articles/In-Ukraine-ambulancecome-patient-10-minute s.html, 2012.

[26] S. Ross, Introduction to Probability Models, Ninth Ed., 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," Proc. of INFOCOM '11, pp. 2147-2155, 2011.

[28] W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," Proc. of CRPIT '14, ser. CRPIT '14, pp. 1-8, 2002.

[29] I. Ioannidis, A. Grama, and M. Atallah, "A Secure Protocol for Computing Dot-Products in Clustered and Distributed Environments," Proc. of ICPP '02, pp. 379-384, 2002.

[30] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Prof. of INFOCOM' 11, pp. 1647-1655, 2011.

[31] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine- Grained Private Matching for Proximity-Based Mobile Social Networking," Prof. of INFOCOM '12, pp. 1-9, 2012.

[32] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-Preserving Personal Profile Matching in Mobile Social Networks," Proc. INFOCOM, pp. 2435-2443, 2011.

[33] K.-H. Huang, Y.-F. Chung, C.-H. Liu, F. Lai, and T.-S. Chen ,"Efficient Migration for Mobile Computing in Distributed Networks," Computer Standards and Interfaces, vol. 31, no. 1, pp. 40,47,2009.