ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

A Convenient Proposal Expansion for Healthcare Emergency

[I]U.Suganya, [II]V.Priya
[I]M.Phil Full time Research Scholar, [II]Associate Professor
[I,II]Dept. of Computer Science, Vivekananda College of Arts and Sciences for Women, Namakkal, Tamil Nadu, India.

Abstract
The cost of health care has become a national concern. Recent advances in wireless communication networking and IT have made it possible to monitor and overhaul the outcomes across diverse healthcare environment. Here we make use of the sensors and smart phones to provide continuous monitoring of the individuals without the need for them to be hospitalized. Based on the health conditions of the patients', the dedicated sensors are provided to monitor the patients' after which the sensed data is transmitted to the healthcare center using their smart phones. 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.

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

I. Introduction

In this paper, to 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 our aging 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 smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease . Instead, after being equipped with smartphone 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. For example, 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 via bluetooth. 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 react to 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. 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 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-Health care system is still challenging in emergency..

II. Related Work

The opportunistic computing has increased the great interest recently, and we have briefly reviewed them which are related to our work. In, Avvenuti et al have introduced the concept of opportunistic computing in wireless sensor network which solves the problem of storing and executing an application incase if it exceeds the memory available on a single node. The application code can be partitioned in a number of simple modules that opportunistically cooperate to carry out a complex task And each node executes the provided application by running the given tasks and providing service to the neighboring nodes. In , Conti deals with the Opportunistic exploitation of (pools of) resources. The nodes can be able to communicate even if a completed connected path never exits between them. Mobility of the nodes provides them the opportunity to communicate with each other. Each user can avail not only of the resources available on its own device, but can also on other resources of the environment. In Pazzi provides that the health information is monitored by the Sensors the sensed data to the health center using neighbor nodes. This can be transmitted to the health care centre only when there is a proper cooperation between the neighbor nodes. Although and are important for understanding how the concept of opportunistic computing paradigm work when

resources available on other neighboring nodes to complete the given task , they have not considered the security and privacy issues existing in the opportunistic computing .Different from all the above works, our proposed PPSPC framework aims at the security and privacy issues by providing encryption and provides the secure transmission of data and provides help at emergency situation in m-healthcare emergency.

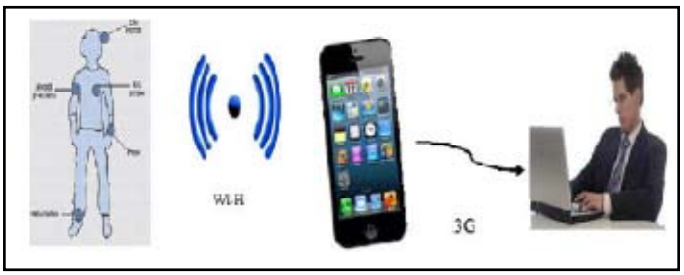
A. Disadvantages of Existing System

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 smart phone's energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, 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.

III. Proposed System

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-healthcare emergency.

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 1) apply opportunistic computing in m-Healthcare emergency to achieve high reliability of PHI process and transmission; and 2) develop user-centric privacy access control to minimize the PHI privacy disclosure.



Medical user Smartphone Healthcare Centre
Fig.1 :Overview of healthcare system

A. Advantages of Proposed System

The 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.

B. Implementation

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 1) apply opportunistic computing in m-Healthcare emergency to achieve high reliability of PHI process and transmission; and 2) develop user-centric privacy access control to minimize the PHI privacy disclosure.

Bilinear Pairings Let G and GT be two multiplicative cyclic groups with the same prime order q. Suppose GG and GGT are equipped with a pairing, i.e., a non degenerated and efficiently computable bilinear map e : G*G --> GT such that e(ga1, gb2)= e(g1, g2)ab € GT for all a,b €Zq* and any g1, g2€G. In group GG, the Computational Diffie-Hellman (CDH) problem is hard, i.e., given (g,ga, gb) for g € G and unknown a,b€ Zq , it is intractable to compute gab in a polynomial time. However, the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given (g, ga,gb,gc) for g 2 GG and unknown a; b; c 2 ZZ_ q , it is easy to judge whether c ¼ ab mod q by checking e(ga, gb) e(gc, g).

Definition1. A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter _ as input, and outputs a 5-tuple (q,g,G,GT,e), where q is a bit prime number, G and GT are two groups with order q,g €G is a generator, and e : G €G*GT is a non degenerated and efficiently computable bilinear map.

B. Algorithm1. Privacy-preserving Scalar Product Computation

Procedure PPSPC PROTOCOL

Input: U0's binary vector a = (a1, a2, . . . , an) and Uj's binary vector ~b ¼ ðb1; b2; . . . ; bnÞ, where n _ 26

Output: The scalar product ~a .~b =∑ni=0 ai .bi

Step-1: U0 first does the following operations:

choose two large primes α,β where β is of the length |α|=256 bits and β> (n +1) .α2, e.g., the length |β|> 518 bits if n =26

6: set K ¼ 0 and choose n positive random numbers (c1, c2, c3, … , cn) such that ∑ ni=1 ci < α- n

7: for each element ai € ~a do

choose a random number ri.α such compute ri.β such that |ri.β|~ 1024 bits, and calculate ki ¼ ri.β- ci

if ai=1 then

Ci = α+ci+ri .β, K = K + ki

else if ai=0 then

Ci =ci+ ri.β, K= K +ki

end if

end for

keep (β,K) secret, and send (α,C1, C2, C3, …. ; Cn) to Ui

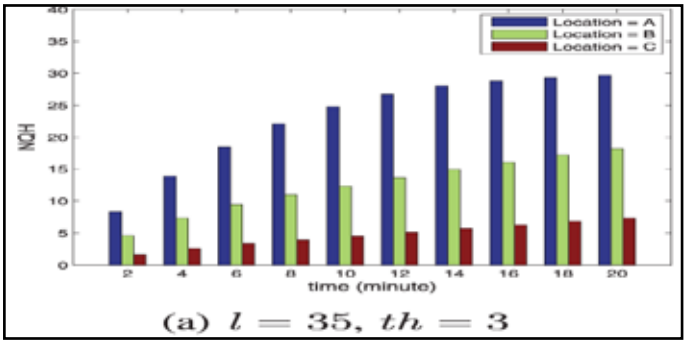
Step-2: Uj then executes the following operations:

for each element bi €~b do
if bi =1 then
Di =α. Ci= { α+ci+ri.β, if ai =1;
ci + ri.β; if ai=0:
else if bi = 0 then

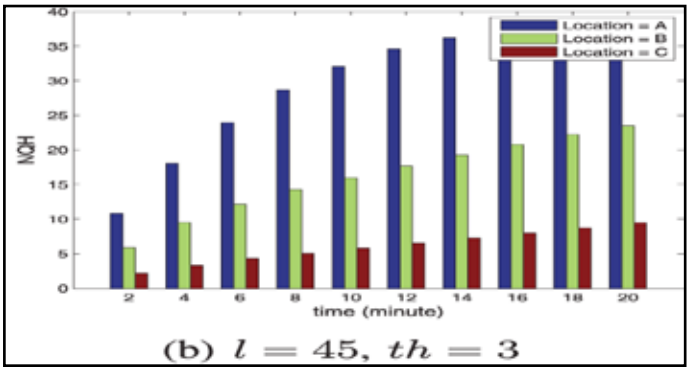
Di= ci= { α+ci+ri.β; if ai =1;
ci +ri.β; if ai = 0:
end if
end for
compute D =∑ni=1 Di and return D back to U0
Step-3: U0 continues to do the following operations:
compute E =D +K mod β
end procedure

IV. Result Analysis

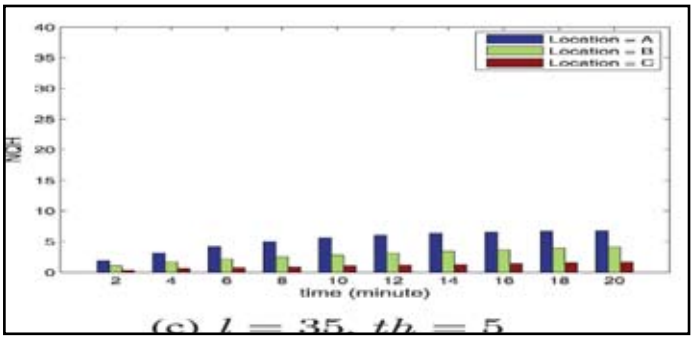
We compare the average NQHs at locations A, B and C varying with time from 2 to 20 minutes under different user number l and threshold th. From the figure, we can see, with the increase of time, the average NQH will also increase, especially for the location A. The



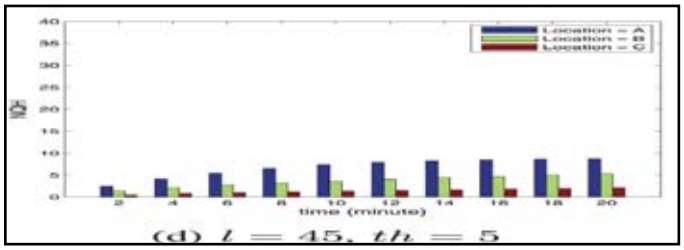
(a) $l = 35,\ th = 3$



(b) $l = 45,\ th = 3$



(c) $l = 35,\ th = 5$



(d) $l = 45,\ th = 5$

Fig. 2 : NQH varying with time under different l and th.

reason i 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 l in the simulation area increases, the user arrival rate at locations A, B, and C also increase. Then, the average NQH increases as well. By further observing the differences of the average NQH under thresholds th=3 and th=5, we can see the average NQH under th=5 is much lower than that under th=3, which indicates that, in order to minimize the privacy disclosure in opportunistic computing, the larger threshold should be chosen.

V. Conclusions and Future Work

We have proposed a secure and privacy preserving opportunistic computing 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 smart phone-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] *J. C. Hsieh, K. C. Yu, H. C. Chuang, and H. C. Lo, "The Clinical Application of an XML-Based 12 Lead ECG Structure Report System," Computers in Cardiology, pp. 533–536, Sept. 2009.*

[2] *Olivier Y. De Vel, "R-wave detection in the presence of muscle artifacts," IEEE Trans. Biomed. Eng., vol. BME-31, pp. 715–717, Nov.1984.*

[3] *Y.-C. Su, H. Chen, C.-L. Hung, and S.-Y. Lee, "Wireless ECG detection system with low-power analog front-end circuit and bio-processing ZigBee firmware," in Proc. IEEE Int. Symp. Circuits Systems (ISCAS), pp.1216–1219, June 2010.*

[4] *L. Zhang and X. Jiang, "The Reliability Analysis and Design of ECG Signal Acquisition Circuit Based on Pspice," Int. Conf. Bioinformatics Biomed. Eng. (iCBBE), pp.1–4, June 2010.*

[5] *L. Yongjun, L. Yu, X. Xiaorong, and T. Yafang, "Analysis and Implement of ECG Front-End Signal Processing Circuit," Int. Conf. Information Technology, Computer Engineering and Management Sciences (ICM), pp.309–312, Sept. 2011.*

[6] L. Yu, Z. Fengjuan, N. Zedong, and W. Lei, "ECG signal de-noising on node based a dedicated FFT circuit," IEEE 10th Int. New Circuits and Systems Conf. (NEWCAS), pp.461–464, June 2012.

[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] 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.