ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Performance Evaluation for High-Intensive PHI Process and Transmission in m-Healthcare

P. Shanmugapriya [1], M. Deva Priya[2]

M.Phil Research Scholar PG and Research Department of Computer Science, Government Arts College, Coimbatore, Tamilnadu, India[1]

Assistant Professor PG and Research Department of Computer Science, Government Arts College, Coimbatore, Tamilnadu, India[2]

Abstract: Wireless technology is being used extensively in health care. However, the development of m-Healthcare still faces many challenges including information security and privacy preservation. In order to create a secure privacy preserving opportunistic framework for patient health care monitoring system a smart time based body sensor networks with a set of proxies together is used. In this system, the patient blood pressure and pulse level is checked every time when the input arrives from the patient side. Once the patient input reaches the below level or the above level with the body sensor input settings, the server immediately send the information about the patient details including patient name, patient address and the contact number to the ambulance control number. Simultaneously, the server sends a password request to the concern doctor which is already set for the patient during registration. In return, the doctor sends an acknowledgement with a password to the server, the server recognizes the password which is sent by the doctor and if the password authenticated successfully, then the server immediately pass the preserved content about the patient to the doctor and pass the doctor details to the patient mobile vice versa. In order to produce a strong security scheme, one.com cloud drive server is used, where the default server side encryption is enabled and it also support an additional back bone to the proposed system. By implementing this system, the patient healthcare is monitored with more secure and in efficient manner.

Keywords: M-healthcare emergency, Opportunistic Computing, PHI, PPSPC, User–Centric Privacy Access Control

I. INTRODUCTION

In recent times, with the rapid development and implementation of wireless medical sensors, electronic healthcare (e-healthcare) has gained increasing popularity. Monitor and record some vital parameters of patients are of importance to know the patient's health condition. But malicious attacks happen occasionally, which may cause the patient-related data being leaked or modified such as the security issues of the distributed data storage in wireless body area networks (WBANs) and the privacy of the patient-related information stored in the database of the medical organization systems. Privacy issues related to transferring patient details is causing a great problem. Security related problems also providing a drawback in the existing system. Detailed security analysis shows that the proposed framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the effectiveness in term of providing high reliable PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency. A new privacy-preserving scalar product computation (PPSPC) technique is developed based on an attribute-based access control. This technique is used to decide who can participate in the opportunistic computing to assist in processing his/her overwhelming PHI data.

There are three main augmentation of this paper. First, a time based privacy-preserving opportunistic computing framework for m-Healthcare emergency. With this, 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. The user's medical information will be received at servers computer and corresponding action will be performed automatically. Second, to achieve user-centric privacy access control in opportunistic computing, presented an efficient attribute based access control and a novel non-homomorphic encryption based privacy-preserving scalar product computation (PPSPC) protocol, where the attributed-based access control can help a medical user in emergency to identify other medical users, and PPSPC protocol further control only those medical users who have similar symptoms to participate in the opportunistic computing while without directly revealing users' symptoms. Third, custom simulator is developed to validate the effectiveness of the proposed framework in m-Healthcare emergency. Extensive simulation results show that the proposed framework can help medical users to balance the high-reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency.

II. MODELS AND DESIGN GOAL

This section, formalizes the system model and security model, and identify our design goal as well

A. *System Model*

System model is considered with a trusted authority (TA) and a group of l medical users U ¼ fU$_1$; U$_2$; . . . ; U$_l$g, as shown in Figure 1, TA is a trustable and powerful entity

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

located at healthcare Centre, 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 [19]. Each medical user U_i 2 U is equipped with personal BSN and smart-phone, which can periodically collect PHI and report them to the healthcare Centre for achieving better health care quality. Unlike in-bed patients at home or hospital [16], [17], [18], medical users U in our model are considered as mobile ones, i.e., walking outside.

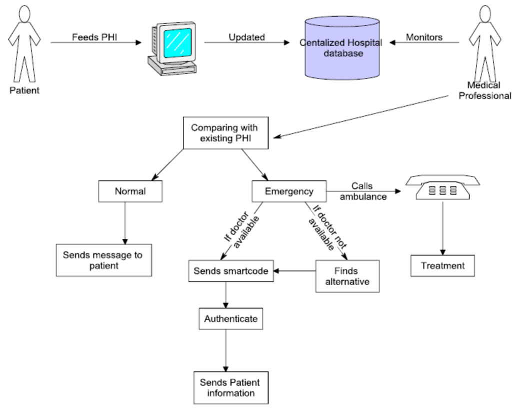

Fig.1. System Architecture

Smart phone and BSN are two key components for the success of m-Healthcare system. In order to guarantee the high reliability of BSN and smart phone, the batteries of BSN and smart phone should be charged up every day so that the battery energy can support daily remote monitoring task in m-Healthcare system [1], [20].

The smart phone could be used for other purposes, such as, phoning friends, surfing web pages, when an emergency suddenly takes place, the residual power of smart-phone may be insufficient for high-intensive PHI process and transmission. To handle this embarrassing situation, opportunistic computing provides a promising solution in m-Healthcare system, i.e., when other medical users find out one medical user U_i 2 U is in emergency, they will contribute their smart phones' resources to help U_i with processing and transmitting PHI.

B. *Security Model*

Opportunistic computing can be used to enhance the reliability for high-intensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him [11]. Specifically, in security model, it essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency, as shown in Fig.3.

Phase-I 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 [11]. Since the opportunistic computing requires smart phones that are installed with the same medical software's to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary software's does not make him as an ideal helper.

Phase-II access control only allows those medical users who have some similar symptoms to participate in the opportunistic computing[11]. The reason is that those medical users, due to with the similar symptoms, are kind of skilled to process the same type PHI [11]. 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.

C. *Design Goal*

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, 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.

III. PROPOSED FRAMEWORK

In this section, describes the proposed framework, which consists of three parts: system initialization, user-centric privacy access control for m-Healthcare emergency, and analysis of opportunistic computing in m-Healthcare emergency. Before describing them, first review the bilinear pairing technique [21], [22], [23], [24], which serves as the basis of the proposed framework.

A. *Bilinear Pairings*

Let G, G^T be two multiplicative cyclic groups with the same prime order q. Suppose G and G^T are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : G\times G \rightarrow G^T$ such that $e(g^a1, g^b2) = e(g1, g2)^{ab} \in G^T$ for all $a, b \in Z*q$ and any $g1, g2 \in G$. In group G, the Computational Diffie-Hellman (CDH) problem is hard, i.e., given $(g, g\ a, gb)$for $g \in G$ and unknown $a, b \in Z*q$, it is intractable to compute gab in a polynomial time. However, the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given $(g, g^a, g^b, g^c)$for g ∈ G and unknown a, b, c ∈ Z^*_q, it is easy to judge whether c = ab mod q by checking $e(g^a,g^b)?=e(g^c,g)$.

Definition 1: A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter κ as input, and outputs a 5-tuple (q, g,G,G^T , e), where q is a κ-bit prime number, G,G^T are two groups with order q, g ∈ G is a generator, and e : G × G → G^T is a non-degenerated and efficiently computable bilinear map.

B. System Initialization

For a single-authority m-Healthcare system under consideration, assume a trusted authority (TA) located at the healthcare centre will bootstrap the whole system.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Specifically, given the security parameter κ, TA first generates the bilinear parameters (q, g,G,G^T, e) by running Gen(κ), and chooses a secure symmetric encryption algorithm Enc(), i.e., AES, and two secure cryptographic hash functions H and $H^{|}$, where H,$H^{|}$: $\{0, 1\}^* \rightarrow Z^*_q$. In addition, TA chooses two random numbers (a, x) ∈ Z^*_qas the master key, two random elements (h1, h2) in G, and computes b = H(a), A = g^a, and e(g, g)^x. Finally, TA keeps the master (a, b, x) secretly, and publishes the system parameter params = (q, g,G,G^T , e,H,$H^{|}$, h1, h2,A, e(g, g)^x,Enc()).

Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, a binary vector a'= (a1, a2,….., an) in the n-dimensional symptom character space, where a_i ∈ _a indicates a symptom character, i.e., a_i = 1 if the medical user has the corresponding symptom character, and a_i = 0 otherwise. Therefore, for each medical user U_i ∈ U, when he registers himself in the healthcare centre, the medical professionals at healthcare center first make medical examination for U_i, and generate U_i's personal health profile a' = (a1, a2,…, an). Afterwards, the following steps will be performed by TA:

- Based on U_i's personal health profile a', TA: first chooses the proper body sensor nodes to establish U_i's personal BSN, and installs the necessary medical softwares in U_i's smart phone.
- Then, T:A chooses two random numbers (t_{i1},t_{i2}) ∈ Z^*_q , and computes the access control key aki = (g^{x+ati1}, g^{ti1}, g^{ti2}, h^{ti}_1 1 h^{ti2}_2) for $U_{i:}$
- Finally, TA uses the master key b to compute the secret key sk_i = H(U_i||b) for U_i.After being equipped with the personal BSN and key materials (ak_i, sk_i), U_i can securely report his PHI to healthcare center for achieving better healthcare monitoring by the following procedure.
- Ui first chooses the current date CDate, computes the session key k_i = H(sk_i||CDate) for one day, and distributes the session key k_i to his personal BSN and smart phone.
- Every five minutes, BSN collects the raw PHI data rPHI and reports the encrypted value Enc(ki, rPHI||CDate) to the smart phone with bluetooth technology.

Upon receiving Enc(ki, rPHI||CDate), the smart phone uses ki to recover rPHI from Enc(ki, rPHI||CDate).After processing rPHI, the smart phone uses the 3Gtechnology to report the processed PHI to healthcare center in the form of U_i||CDate||Enc(k_i,PHI||CDate).

C. User-Centric Privacy Access Control for m-Healthcare Emergency

When an emergency takes place in m-Healthcare, e.g., user U0 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. During the 20 minutes, the medical personnel need high intensive PHI to real-time monitor U0. However, the power of U0's smart phone may be not sufficient to support the high-intensive PHI process and transmission. In this case, the opportunistic computing, as shown in Figure 2, is launched, and the following user-centric privacy access control is performed to minimize the PHI privacy disclosure in opportunistic computing.

D. Analysis of Opportunistic Computing in M-Healthcare Emergency

Consider the ambulance will arrive at the emergency location in the time period t. To gauge the benefits brought by opportunistic computing in m-Healthcare emergency, analysed how many qualified helpers can participate in opportunistic computing within the time period t, and how many resources can the opportunities computing provide. Assume that the arrival of users at the emergency location follows a Poisson process {N(t), t ≥ 0} having rate λ. For a given threshold th, Nq(t) = n and Nq(t) = m are respectively denoted as the number of qualified helpers and the number of non-qualified helpers within [0, t]. For any arriving user at time τ ∈ [0, t], the probability that the user is a qualified helper is P(τ).

IV. SECURITY ANALYSIS

In this section, analysed the security properties of the proposed framework. In specific, following the security requirements discussed earlier, our analyses will focus on how the proposed framework can achieve the user centric privacy access control for opportunistic computing in m-Healthcare emergency.

The proposed framework can achieve the phase-I access control. In the phase-I access control; the single attribute encryption technique is employed. Since e(g, g)xs can be recovered only by a registered medical user Uj ∈ U with his access key akj = (gx+atj1 , gtj1 , gtj2 ,htj11 htj22) from (C1 = gs,C2 = As ▪ h−s1,C3=h−s2), if Uj can recover e(g, g)xs, he can be authenticated as a registered medical user.

In addition, the timestamp in the returned Auth = H_(e(g, g)xs||timestamp) can also prevent the possible replaying attack. Therefore, the phase-I access control can be achieved in the proposed framework.

V. PERFORMANCE EVALUATION

In this section, the performance of the proposed framework is evaluated using a custom simulator built in Java. The simulator implements the application layer under the assumptions that the communications between smart phones and the communications between BSNs and smart phones are always workable when they are within each other's transmission ranges. The performance metrics used in the evaluation are

- 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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

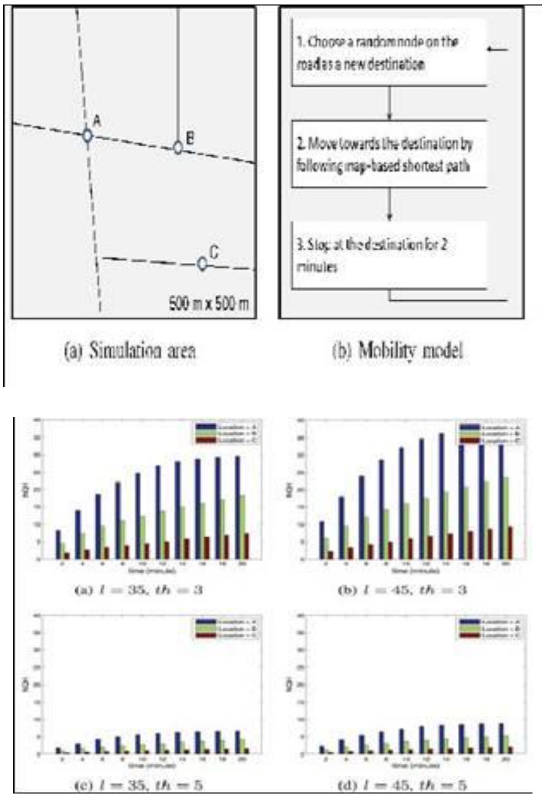

Fig.2. Simulation area and mobility model under consideration

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 framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

VI. SIMULATION RESULTS

In this section, conducted simulations to verify the proposed algorithm and analysis. First, using a sample to show the performance gap between offline and online scenarios of the LMM problem. Then, demonstrated that if the prediction of user mobility can be made, the performance can be improved significantly. In the simulations, total l users U = {U0,U1,…., Ul−1} are first uniformly deployed in an interest area of 500 m×500 m, as shown in Fig. 5(a). Each user Ui ∈ U is equipped with his personal BSN and a smart phone with a transmission radius of 20 meters, and independently moves along the road with the velocity v ∈ [0.5, 1.2]m/s in the area by following the mobility model described in Figure 2(b). Assume that the symptom character space n = 16, each user is randomly assigned 6-8 symptom characters. Let the emergency of user U0 take place at time t = 0, he sets the threshold th as {3, 5}, and waits the qualified helpers participating in the opportunistic computing before the ambulance arrives in 20 minutes.

Note that, in the simulations, consider all users will stop when they meet U0's emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, we consider U0's emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations. The detailed parameter settings are summarized in Table 1.

TABLE I. SIMULATION SETTINGS

Parameter		Setting
Simulation area		500 m × 500 m
Simulation	warm-up,	10 minutes, 20 minutes
Duration		l = {40, 60}, v = 0.5 − 1.2
Number, velocity of		m/s
Users		th = {3, 5}
Similarity threshold		20 m, 20 m
Transmission of smart		
phone, BSN		every 10 seconds
Raw PHI data		A, B, and C
generation interval		
Emergency location		

A. *Simulation Results*

In Figure 3, compared the average NQHs at locations A, B and C varying with time from 2 minutes 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 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 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.

However, since the high reliability of PHI process is expected in m-Healthcare emergency, minimizing the privacy disclosure in opportunistic computing is not always the first priority. In Fig. 7,

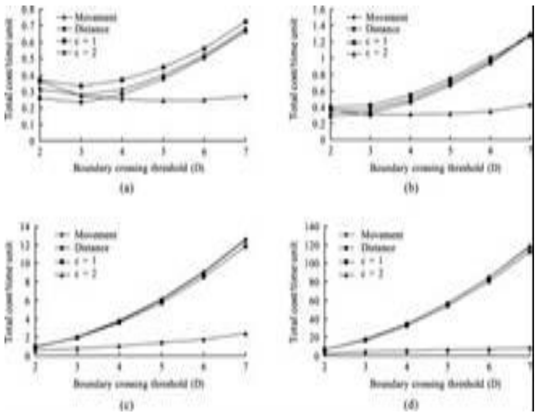

Fig.3. RCR varying with time under different l and th Ploted the corresponding RCR varying with the time under different user number l and threshold th.

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

VII. RESULT AND DISCUSSION

The administrator can control and view the patient and doctors message. Administrator system (server) stores the details of patient's and doctor's code number, mobile number, details, sent message details, date and time of that exact message sent, subject of the message, ambulance details.

Every patients should register in the server and they get code number. A registered patients can send a message such as their health status to the server with the help of that code number. The server once receives a message form patients immediately it sends corresponding acknowledgement to the patients. At the same time appropriate message automatically send to doctor and ambulance in case of any emergency found.

The results of m-healthcare system is screened out efficiently in the below screenshots. The fig.4 illustrates the login window. The initial step of the implementation is providing Admin login in order to authorize the process. The admin user name and password is provided. After logging in to the system, the admin can view the frame work which shows the overall process of the project. The admin can select the task as per the need.

Fig.4. Admin Login Window

The figure 5 represents the patient registration window. It contains various information about the patients such as patient id, name, address, phone no, email id.

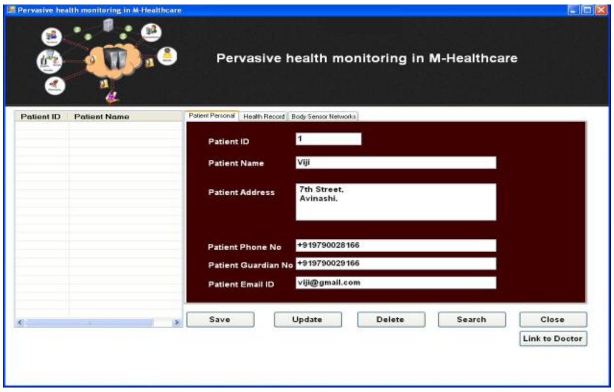

Fig.5. Patient Registration Window

The figure 6 illustrates that the patient can enter his personal details, health record and can select the desired body sensor that he is actually in need of based on his/her body conditions.

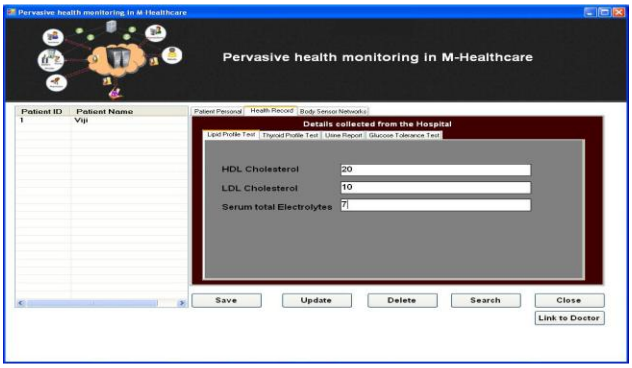

Fig.6. Pervasive health monitoring in m-healthcare

The Figure 7 illustrates patient doctor relationship. Each patient is linked with a unique doctor.

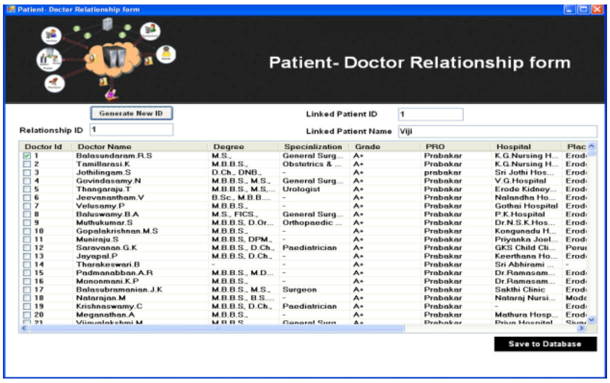

Fig.7. Patient doctor relationship

The figure 8 illustrates the configuring wireless port. Wireless port need to be configured for setting up the connection.

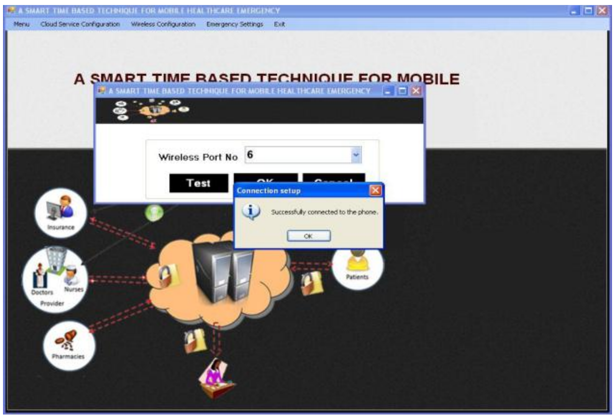

Fig.8. Configuring the wireless port

After entering the patients details , record is saved.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

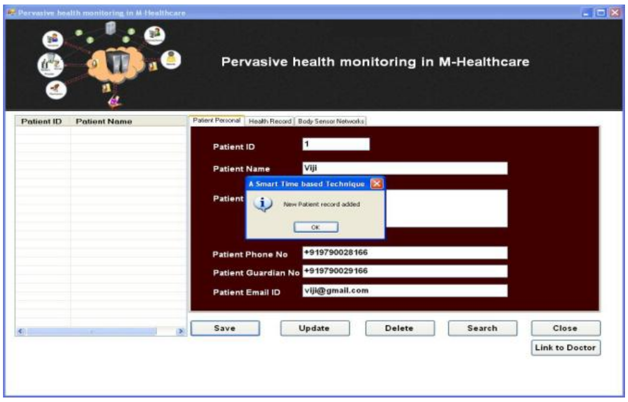

Fig.9. Adding patient details

Any modification done in the record of patient is updated for future usage shown in figure 10.

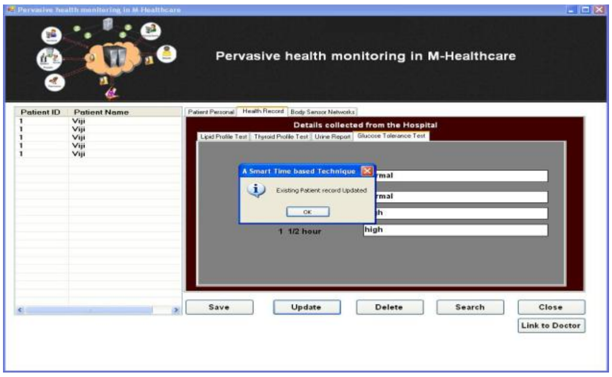

Fig.10. Updating the patient record

Each patient is linked with a unique doctor and a relationship id is created shown in figure 11.

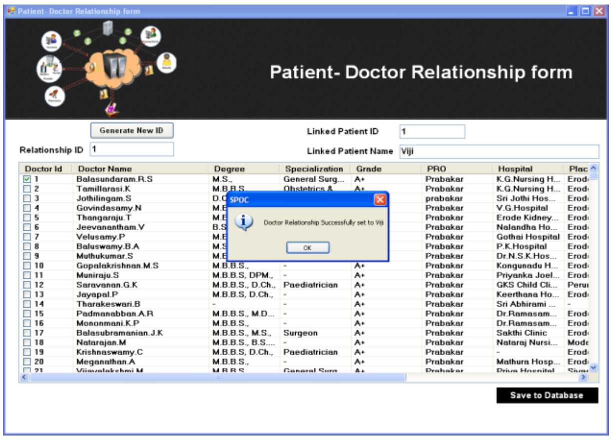

Fig.11. Linking the doctor with the patient

The patient can send the input and if it is normal then message will be sent to the patient shown in figure 12.

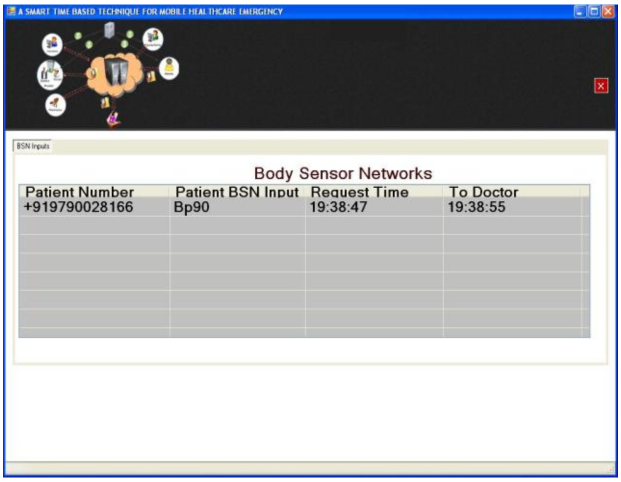

Fig.12. Receiving input under normal condition

The patient can send the input and if he/she is in emergency condition an intimation message will be sent to the ambulance shown in figure 13.

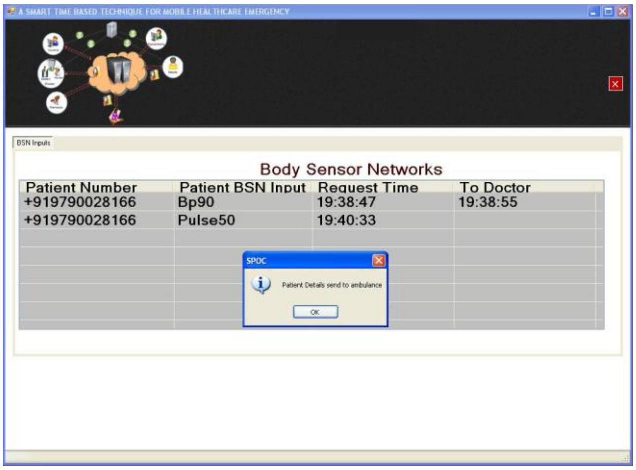

Fig 13. Receiving inputs under emergency condition

For secure transmission of patient's details we have provided authentication for the corresponding doctor.

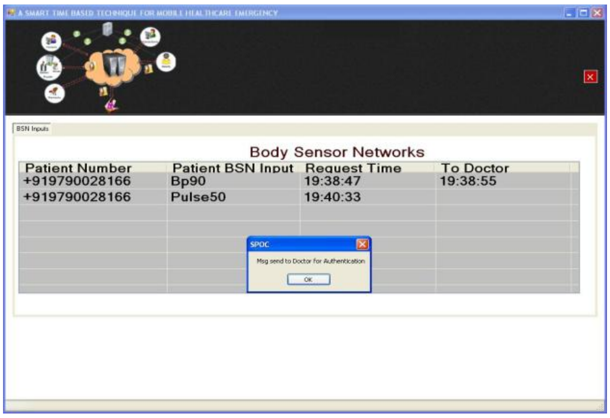

Fig.14. Authentication

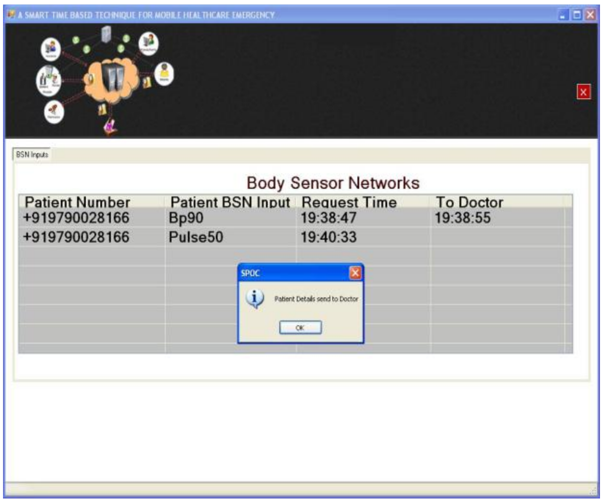

Fig. 15 Transferring patient details

After authenticating the doctor, doctor's details will be sent to the patient.

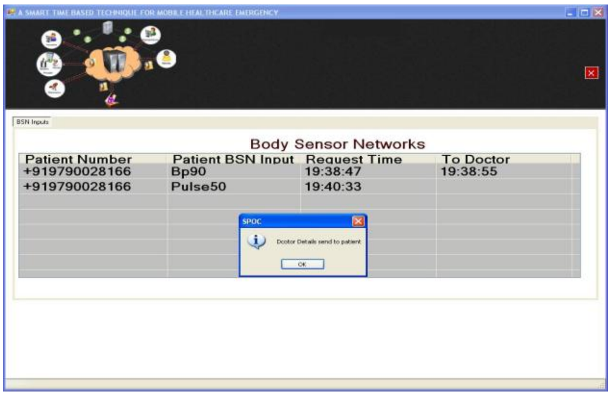

Fig.16. Sending doctor's details

For authenticating the doctor password needs to be set up.

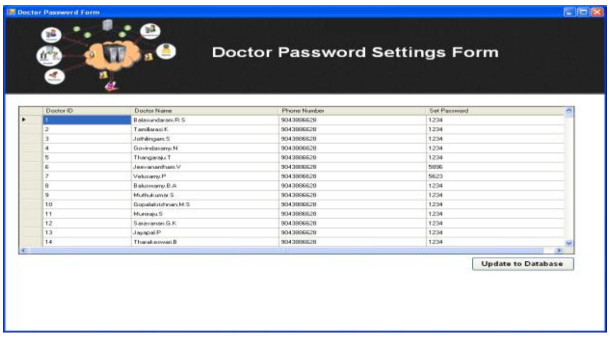

Fig.17. Setting password for doctor

All linked patient and doctor details will be generated.

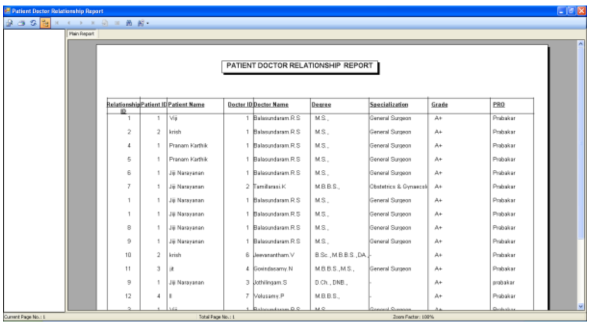

Fig.18. Patient doctor relationship report

Details of doctor has been generated.

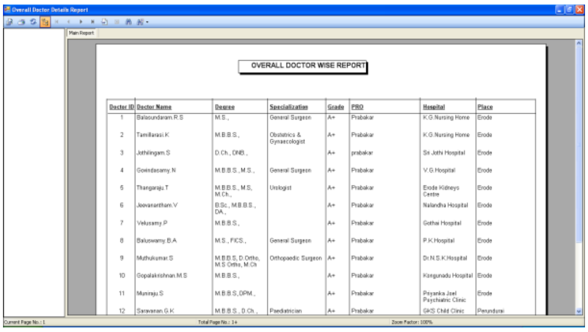

Fig.19. Overall doctor details report

VIII. CONCLUSIONS

It is concluded that the proposed application a time based privacy preserving opportunistic computing framework for m-Healthcare emergency works well and satisfy the end users, 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 framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency. Patient can able to know their current health status through continuous monitoring by giving periodic updates. It helps in reducing the cost and time involved for medical transportation. Thus it helps in improving the performance of the system.

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 with Symptoms-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.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

[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 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 Aus- tralasian 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://free-alzheimers-support.com/wordpress/2010/06/exercise-and-walking/, 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 Commu- nications," 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-ambulance-come-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 Environ- ments," 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] Rongxing Lu, Xiaodong Lin, Xuemin Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 3, pp. 614-624, March 2013, doi:10.1109/TPDS.2012.146.