INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PRIVACY PRESERVING COOPERATIVE STATISTICAL EXAMINATION FOR MEDICAL DATA

P J SRAVYA[1], Mrs. G.VICTO SUDHA GEORGE[2]

1.M.Tech, Department of Computer Science & Engineering, Dr.MGR Education And Research Institute University, Maduravoyal, Chennai, India, sravyapakala@gmail.com
2. Assistant Professor, Department of Computer Science & Engineering, Dr.MGR Education And Research Institute university, Maduravoyal, Chennai, India, sudhajose72@gmail.com

Abstract

In this paper we have proposed a system that detects body condition using body sensor equipment for M-healthcare facility. The detected information is processed using the smart phone for known illness or the records are sent to authorize medical center via Wi-Fi. Privacy-preserving scalar product computation protocol is used to preserve the personal health information of users. The PHI of the patient is encrypted using triple DES while transmission.

Keywords: Mobile-healthcare, Body sensor equipment, Privacy-preserving, Smart phone, Authority center.

1. Introduction

In present aging society, mobile application has been more popular for providing quality health services of pervasive computing; Two methodologies like implantable body sensor equipment and wearable body sensor equipment are used in detecting chronic medical condition of the patient. The patient can be monitored by the Mobile application through smart phones. Medical application will check the condition of the patient such as temperature, blood pressure. Specifically medical user need not go to the hospital for monitoring their health conditions. BSE equipment is clamped to patient body so that patient themselves can check the condition and when they are in critical condition medical agents can help them to monitor their PHI through health care authority center. This application having high-quality of measurement professionals can monitor at any place and any time.

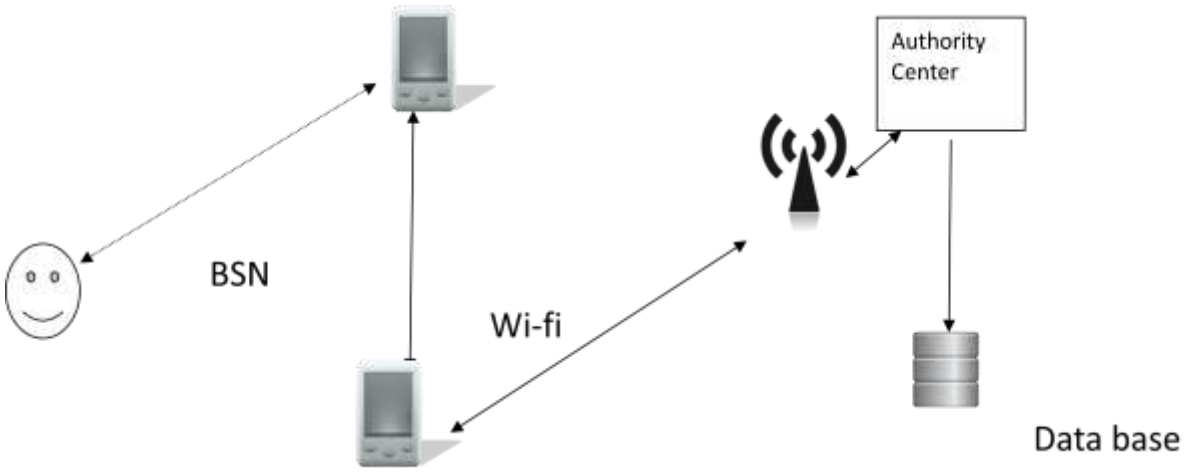

Figure 1: System architecture

BSE first detect the health parameters and send using smart phone via wireless transaction through Bluetooth. Further the parameters are transmitted to health care center via Wi-Fi network. PHI values are continuously monitored. Before ambulance or helper reaches the location, BSE can quickly calculate the personal health information for each and every one minute with high-intensive report to health authority center. To avoid traffic in authority center the patients with similar symptoms are handled with same reply type.

In this paper we introduce privacy-preserving statistical analysis for medical data of mobile health care using embedded system. Where we have used PPSPC protocol, which certainly give efficient process and security for PHI of medical user and speedup the process and parallel increasing the data to be sent for trusted authority centre without any delay.

2. Related work

Research on body sensor network has grown tremendously in recent years. A single-authority in healthcare is under process, we consider trusted authority will completely bootstrap the system. Generally given with security parameter, trusted authority first defines the bilinear parameter and selects a secure symmetric encryption i.e, user centric privacy access control and two secure cryptographic hash functions.

The user centric access control as the algorithm doesn't helps to transmit the PHI values of patients who are suffering in critical situation. In this BSN is too busy in reading the values and difficult in producing large amount of value are transmitted at a given time period in which the user centric access control is not ready to encrypt the reading and it takes long procedure to send value to healthcare centre. In mobile healthcare system medical user's PHI need to monitor the parameter and reported to healthcare center directly, while the issues is to maintain patient's PHI securely and only the medical agent must read them.

2. Proposed system

Comparing previous related work here BSE plays a major role .An single-authority in healthcare is under process. We consider trusted authorities will completely bootstrap the system, generally given with security parameter. Trusted authority first define the bilinear parameter and select a secure of symmetric encryption i.e., HMAC and two secure cryptographic hash function.

In 'resent work' we choose a secure symmetric encryption algorithm. In 'present work' we use embedded system which is enhanced to user centric privacy access control encrypt the PHI values. Because while values of medical user is transmitted from BSE to embedded Kit through Bluetooth and other mobile user should not come to known the medical user PHI, We maintain medical user PHI parameter securely through PPSPC protocol. Finally, trusted authority store data secretly in database and send to smart phone. By binary vector in n-dimensional, symptom of medical users can be characterized with Vi=1 i.e., if the corresponding medical user having similar symptom and

Vi=0 otherwise. The medical agent at healthcare center will first make examine Ui, and aggrete Ui's PHI. Based on personal health profile upon Vi's, Healthcare center first calculate the health parameter to Ui's BSE and installs the medical application in smart phone device.

2. User centric two-phase privacy access control:

Opportunistic computing for m-health care emergency can enhance high-intensive of PHI profile. To reduce the processed values privacy of two-phase user-centric access control.

Phase-I:

The idea of phase-1 is to check out medical user smart phone has enough battery consumption.

Phase-II:

Notes if nonmedical user participates in accessing opportunistic computing, will not welcomed to login. It allows only authorized medical user to participate.

Phase-III:

Calculate the PHI and allows medical user those who has some similar symptoms, (or) the user who have same type of PHI.

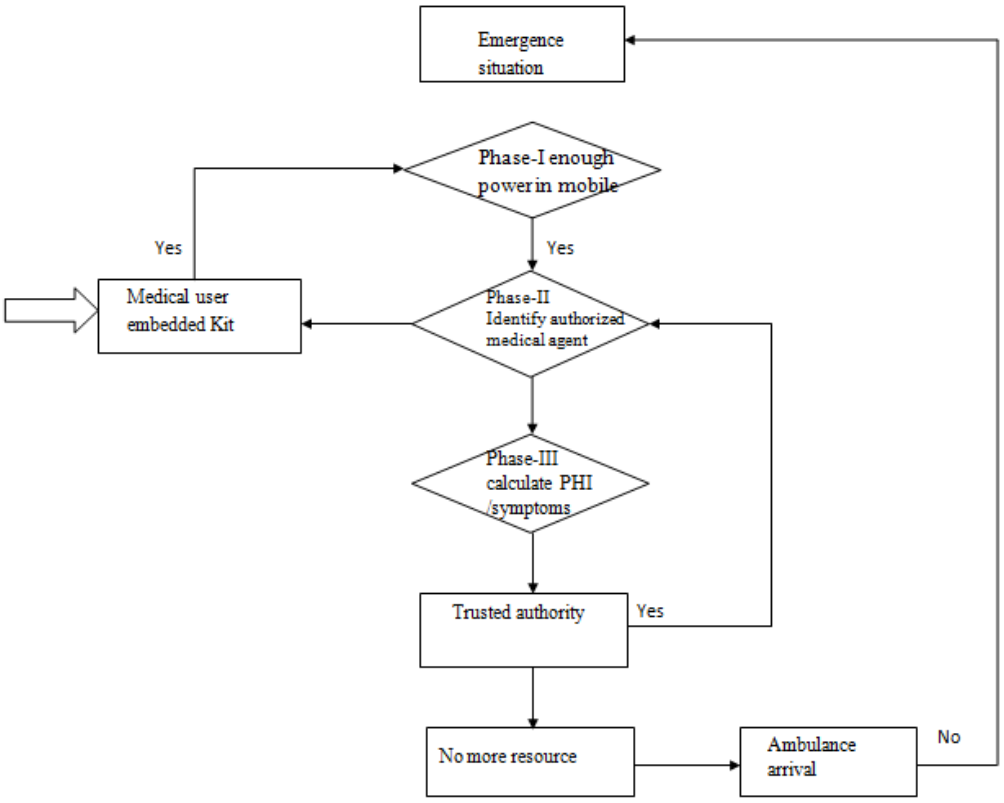

Figure 2: Computing user-centric two-phase privacy access control for M-health care emergency

5. Description of the system

a. SPOC Initialization

The authority centre will initialize the whole system. When the person is ill (or) in any emergency case, BSE helps us to monitor personal health information with high-intensive support, All this process is done in between mobile and authority centre, where by mobile is connected to internet through Wi-Fi by SOA architecture.

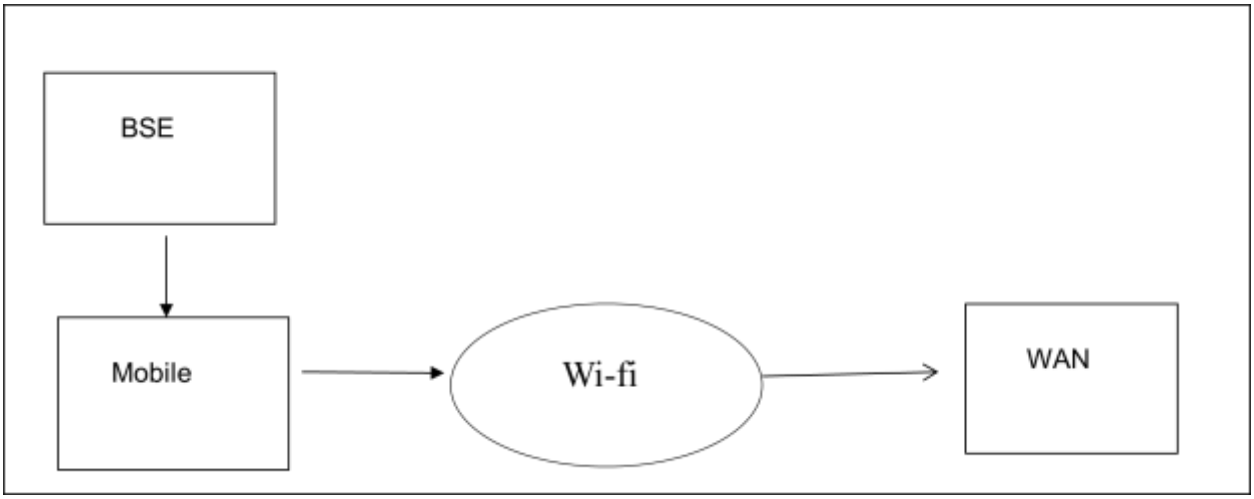

Figure 3: SPOC Initialization

b. M-Health application

The important components of mobile-health care system are BSE and smart phone. BSE detects the health information of the patient. The PHI is computed using the medical kit. The medical kit is connected to smart phone via Bluetooth. Then the detected values from medical kit, will pass on to smart phone and then searches in agent's personal mobile database. If the patient value is not matched in the database of agent's mobile then it approach the trusted authority center. In mean while medical agent should maintain battery with 50%, since the smart phone would be used for many other purpose like surfing net, phoning to friend. If the charge drops below 50% we will not be able connect to authority center. In such case opportunistic computing is implemented in which the phone of nearby agent is approached for connection establishing with authority center. The data is encrypted using Triple DES before transmission. Triple DES uses 192 key. So it has the advantage of proven reliability and that eliminates many of the attacks.

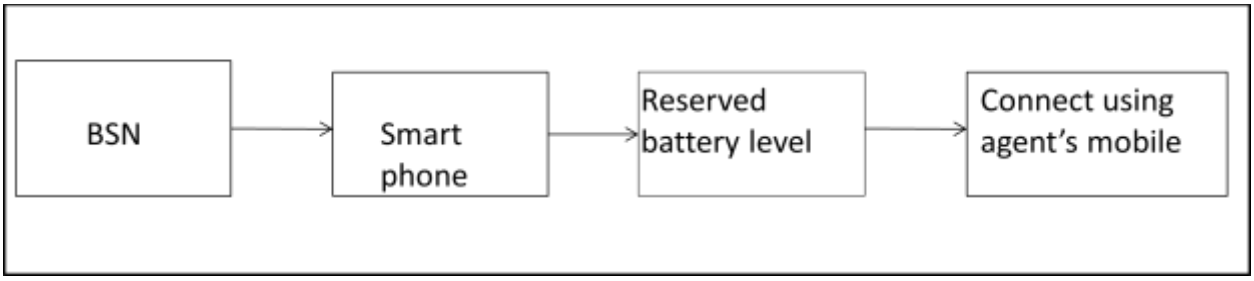

***Figure* 4**:M-Health application

C .phase control

In this phase the actual reading from the processed data is verified for some set of similar symptoms to participate in the opportunistic computing. The goal of phase access control is to identify medical user in emergency. In have the advantage of proven reliability and a longer key length that eliminates many of the attacks. Key length 192bits

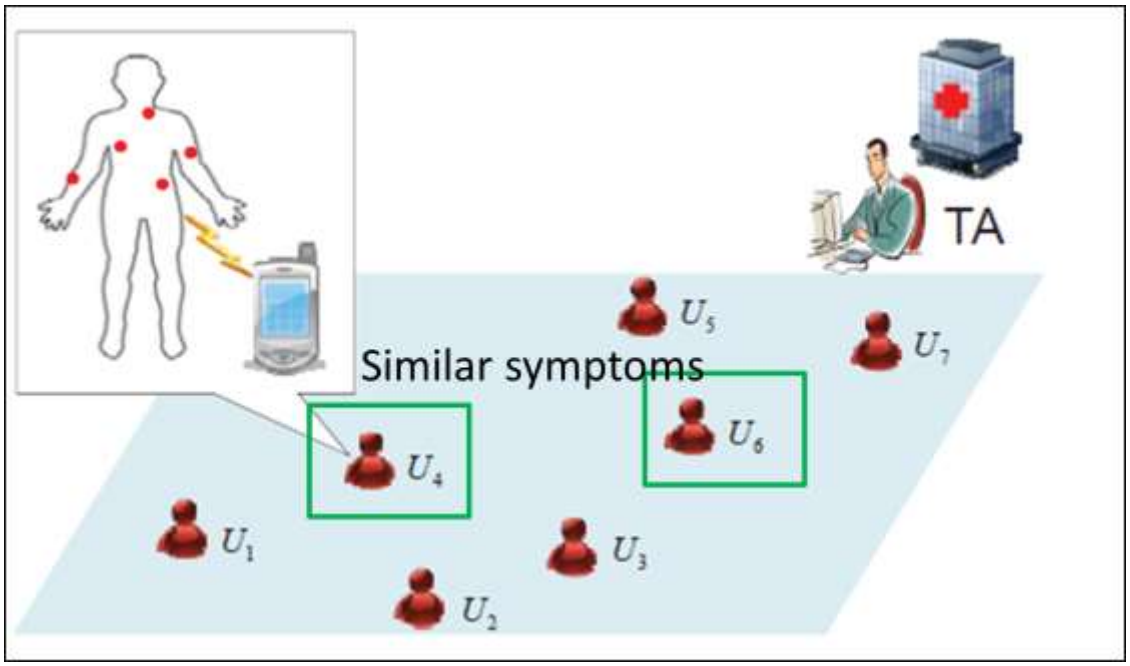

Figure 5: Phase control

2. Conclusion:

In this paper, we have explained about secure and privacy preserving opportunistic computing framework for M-Healthcare, This paper describes the usage of opportunistic computing to add high-intensive of PHI values in emergency which discloses the privacy during the opportunistic computing.

3. Future work:

Smart phone-based technology to identify and analyse the effectiveness of SPOC framework. And also PPSPC protocol provides security for PHI values only to transmit via authorized user agents. In addition we will work on internal dilemma like diabetes, heart disease and other internal attacks.

7. Reference:

[1] 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.

[2] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *INFOCOM*, 2011, pp.2435–2443.

[3] 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.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for m-healthcare social network," *MONET*, vol. 16, no. 6, pp. 683–694, 2011.

[5] 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.

[6] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in *Prof. of INFOCOM' 12*, 2012, pp. 1–9.

[7] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Prof. of INFOCOM'11*, 2011, pp. 1647–1655.

[8]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.