IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Privacy Preserving Co-operative Statistical Analysis for Computing Medical Data

Charumathi.M[1], Harini.K[2], Anbarasi.D[3]

[1, 2, 3]**Department of Information Technology, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India**

Abstract

Mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives of people, where small wearable or 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 , in a mobile 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, the medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. Each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature , can be first collected by the BSN, and then generated by smart phone via Bluetooth. Finally, they are transmitted to the remote healthcare center using the nearby access point via wi-fi network. When the PHI is being transmitted there are many possibilities that a third person may hack the information. To avoid this scenario we introduce a new Privacy Preserving Scalar Product Computation (PPSPC) technique in the client side also.

Index Terms- *Mobile healthcare , Personal Health Information (PHI) , PPSPC.*

1. Introduction

In our current scenario, m-healthcare has established a milestone where it has been regarded as an important application. In the m-healthcare system the body sensor nodes and the smartphones are used to monitor the patients' who have medical conditions such as diabetes and heart disease [2],[3],[4],[5],[6]. These medical users need not go to hospital to get them monitored instead they can be monitored even when they are walking or sitting at home[7][8][9]. Every medical user's health information i.e their Personal Health Information(PHI) such as heartbeat, blood sugar level, blood pressure, temperature are collected by the Body Sensor Nodes(BSN) and then these sensors send these information to their smartphones via bluetooth. On receiving this information , the smartphones send those information to the healthcare centre via the nearest access point available using 3G networks. The healthcare centre react to the user's life threatening situation and dispatch ambulance and healthcare centre personnel to the emergency location.

Though it appears simple, there are many challenges which arise in m-healthcare. The PHI which is to be reported should not be disclosed. However when the patient is in emergency, the body sensor nodes will be busy reading a variety of values which is being generated in a short period.
These datas which are generated should be reported to the healthcare centre immediately in order to get the medical help from them. However, since smartphone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smartphone'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[1].

2. System model

In this paper, see fig 1, we propose a new secure and privacy preserving opportunistic computing framework, called SPOC, to address these challenges First, we propose SPOC, a secure and privacy-

reserving opportunistic computing framework for m-Healthcare emergency.
Second, to achieve user-centric privacy access control in opportunistic computing, we present an efficient attribute based access control and a novel non-homomorphism encryption based privacy-preserving scalar product computation (PPSPC) protocol.
Third, to validate the effectiveness of the proposed SPOC framework in m-healthcare emergency, we also proposed to develop a Application built for Android using java.

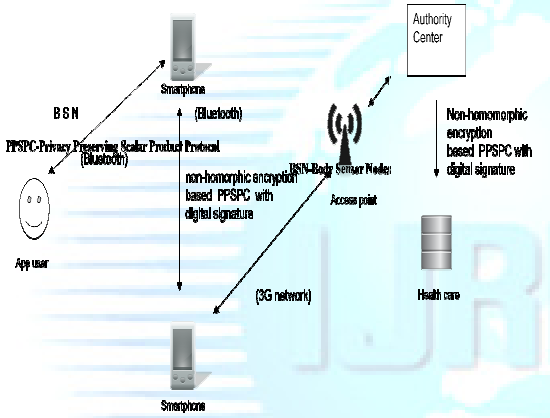

Fig. 1 System architecture

3.Proposed framework

In the existing system, see fig1 and 2, the area of transmission from user to healthcare centre is not secure since protocol is provided only to the server side. To overcome this problem the privacy-preserving scalar product computation protocol is provided in user side as well as in server side.

3.1 SPOC initialization

SPOC is abbreviated as Secure and Privacy-preserving Opportunistic Computing. This SPOC is an application which was developed as .apk application which is suitable for all android smart phones with version 2.2 and above.

This application is the one which helps in dispatching details automatically to the nearby user when the battery backup of the smart phone is less. There is a database called mySQL Lite which helps to store the database of all the related first aid required for the values read by the kit.

An application SPOC has to be installed in the smart phone. The PHI information of the user is stored in the phone. When an emergency takes place that is when a user falls down, the healthcare centre will monitor the emergency and the ambulance will arrive to the user within 20 minutes. During the 20 minutes, the present PHI information has to be transmitted to the health care centre. During this process when the battery power is less than 50% in the user's phone , then using Bluetooth the information is transmitted to opportunistic user from where it has been sent to the healthcare centre.

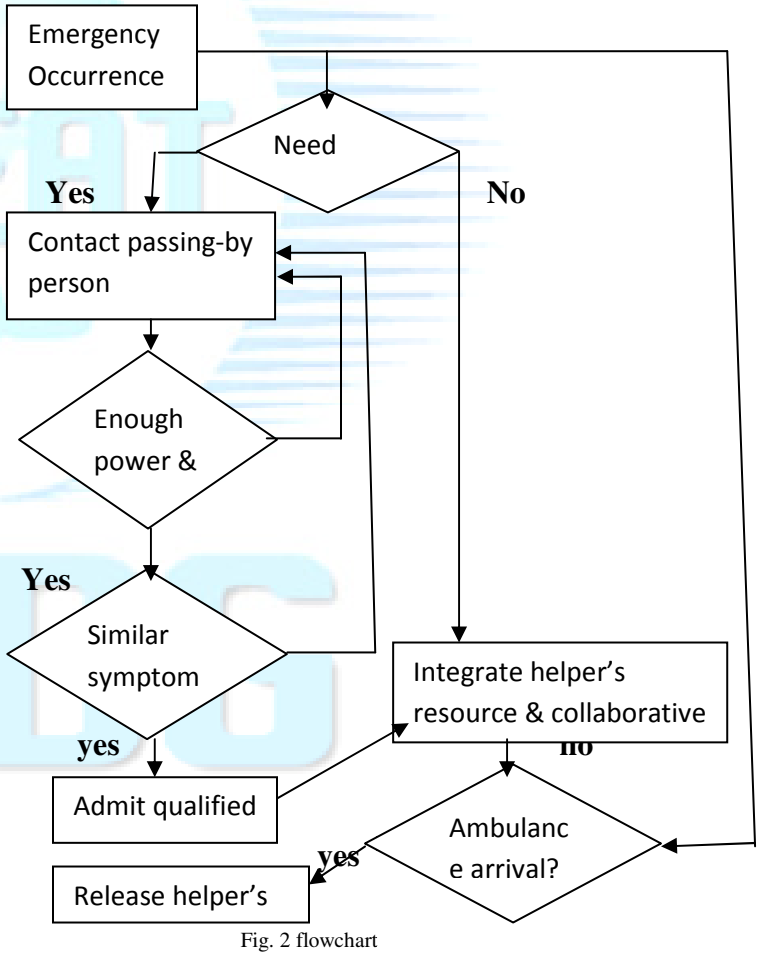

Fig. 2 flowchart

3.2 M-Health Application

Once the SPOC application is installed in the smart phones, it can be used in the mobile healthcare[1]. The users with the SPOC can be recognized as authentic users who can help in medical emergency when a need arises. In this module we introduce a kit called Body Sensor kit, which helps to monitor the Personal Health Information of the individual.

This body sensor kit can be plugged to any individual and can read their Personal Health Information. This body sensor kit helps to direct the PHI readings to the smart phone and then smart phone direct them to the healthcare centre.

BSN and smart phone 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. In general, since the BSN is dedicated for remote monitoring, after being charged every day, BSN can deal with not only the normal situations but also the emergency cases in m-Healthcare. However, since the Smart phone could be used for other purposes, e.g., phoning friends, surfing WebPages, when an emergency suddenly takes place, the residual power of smart phone may be insufficient For high-intensive PHI process and transmission. To deal with this embarrassing situation, opportunistic computing provides a promising solution in m-Healthcare system, i.e., when other Medical users find out one medical user is in emergency, they will contribute their smart phones' resources to help him with processing and transmitting PHI.

Algorithm-Privacy-preserving Scalar Product Computation
1: **Procedure** PPSPC PROTOCOL
2: **Input**: U0's binary vector $\vec{a}$=(a1,a2,….,an) and Uj's binary vector $\vec{b}$=(b1,b2,….bn) , where n≥2^6
3: **Output**: The scalar product $\vec{a}.\vec{b}=\sum_{i=0}^{n} ai.bi$
4: **Step-1**: U0 first does the following operations:
5: choose two large primes α, β, where α is of thelength |α|= 256 bits and β >(n+1).α^2,e.g., the length |β| > 518 bits if n = 2^6
6: set K = 0 and choose n positive random numbers (c1, c2, c3,…., cn) such that

$$\sum_{i=1}^{n} ci < \alpha - n$$

7: **for** each element ai €$\vec{a}$**do**
8: choose a random number ri, compute ri.β suchthat |ri . β| = 1024 bits, and calculate ki = ri . β - ci
9: **if** ai=1 **then**
10: Ci = α+ci+ri . β, K= K + ki
11: **else if** ai = 0 **then**
12: Ci = ci + ri .β, K = K + ki
13: **end if**
14: **end for**
15: keep (β ,K) secret, and send (α,C1, C2, C3,…., Cn) to Ui
16: **Step-2**: Uj then executes the following operations:
17: **for** each element bi £ b **do**
18: **if** bi = 1 **then**
19: Di =α. Ci={α^2+ ci .α + ri.α.β, if ai = 1;
ci.α + ri.α.β, if ai = 0
20: **else if** bi = 0 **then**
21: Di = Ci={ α + ci + ri.β, if ai=1
Ci + ri . β , if ai = 0
22: **end if**
23: **end for**
24: compute D =$\sum_{i=1}^{n} Di$ and return D back to U0
25: **Step-3**: U0 continues to do the following operations:
26: compute E = D + K mod β
27: **return** E-(E mod α^2)/α^2 as the scalar product $\vec{a}.\vec{b}=\sum_{i=0}^{n} ai.bi$
28: **end procedure**

Once Uj passes the phase-1 access control , U0 and Uj continue to perform the phase-2 access control to check whether they have some similar symptoms.[1] Suppose the personal health profiles of medical users U0, Uj are $\vec{a}$ =(a1,a2,…..an) and $\vec{b}$=(b1,b2,….,bn), respectively.U0 first defines an expected threshold th for the number of common symptom characters.

Then, in order to compute $\vec{a}.\vec{b}$ in a privacy-preserving way.U0 and Uj invoke our newly designed PPSPC protocol in Algorithm. Since the PPSPC protocol ensures neither U0 nor Uj will disclose their personal healthcare profiles to each other during the computation of $\vec{a}$.$\vec{b}$, it can efficiently achieve privacy preserving access control.

3.3 Personal Health Information (PHI)

This module deals with the phase control and also the personal health information which is being transmitted to the healthcare centre.

In this phase the actual reading from the processed page is verified for some set of similar symptoms to participate in the opportunistic computing. The reason 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, th will be set high to minimize the privacy disclosure. However, if the location has low traffic, th should be low so that the high-reliable.

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. The PHI data which is received is compared with the pre-recording stored data in the data Center.

The algorithm which was used in SPOC paper[1] is used omly in the server side whereas in our paper we have applied this security technique once the data leaves the smartphne thus makin a third person less chance of hacking into this. Thus the details of a person's PHI is less likely to be disclosed. Thus maintain the efficiency of our proposed work.

4. Performance evaluation

In this section we evaluate the performance of our model with the existing system proposed by others. We have compared some 3 papers form the existing sytem. They are, Mobile Patient Monitoring: The MobiHealth System, A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network , SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency(fig.3)

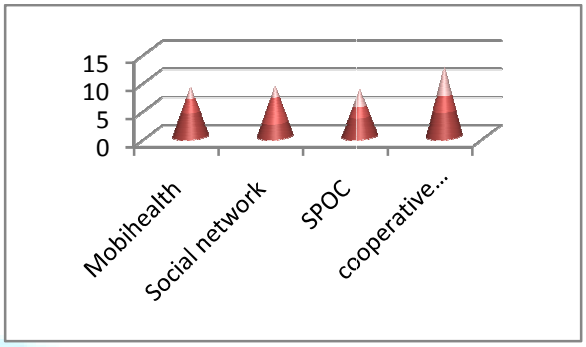

Fig. 3 Performance graph

When compared with these papers on a scale of 15 all the 3 papers from the existing model have been rated lower than our proposed work in this paper. Thus our model has proved to be a more efficient one as the performance graph shows.

5. Conclusion

In this paper we have implemented a security technique that is being used in the client side in order to prevent a third person hacking into the PHI of the individual. In the existing systems the security was provided in the server side only . we have included that algorithm with the digital signature in our work in the client side. This has proved to be more efficient when compared the performance level of existing systems n our paper.

In our future work we tend to carry out these on pervasive computing inorder to serve people better with these kind of medical emergencies which are prevailing.

References

[1] Rongxing Lu, Member, IEEE, Xiaodong Lin, Senior Member, IEEE, andXuemin (Sherman) Shen, Fellow, IEEE,'' SPOC: A Secure and Privacy-PreservingOpportunistic Computing Frameworkfor Mobile-Healthcare Emergency''IEEE transactions on parallel and distributed systems, vol. 24, no. 3, march 2013.

[2] A. Toninelli, R. Montanari, and A. Corradi, "Enabling SecureService Discovery in Mobile Healthcare Enterprise Networks,"IEEE Wireless Comm., vol. 16, no. 3, pp. 24-32, June 2009.

[3] 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 AreaNetworks (BodyNets '10), 2010.

[4] Y.Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients viaa Secure and Mobile Healthcare System," IEEE Wireless Comm.,vol. 17, no. 1, pp. 59-65, Feb. 2010.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Schemewith Symptoms-Matching for mHealthcare Social Network,"
Mobile Networks and Applications—special issue on wireless andpersonal comm., vol. 16, no. 6, pp. 683-694, 2011.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and SecureSharing of Personal Health Records in Cloud Computing UsingAttribute-Based Encryption," IEEE Trans. Parallel and DistributedSystem, to be published.

[7] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A StrongPrivacy-Preserving Scheme against Global Eavesdropping forEhealth Systems," IEEE J. Selected Areas in Comm., vol. 27, no. 4,
pp. 365-378, May 2009.

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

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