Privacy Preserving Scalar Product Computation for Mobile Healthcare Emergency

Aparnaa.M, Sacred HeartAmir.C, Vigneshwari. K, VishnuKumar.A

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. However the Smart phone which are used for various purpose when is not available to transmit the data due to some reasons , we make use of opportunistic computing where the data is transmitted using a neighbors' Smartphone. The m-healthcare still faces many challenges which include Information security and privacy preservation. To overcome the above shortcomings we use a encryption technique to preserve the privacy of users' health information

Index Terms—About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

The introduction of telecommunication technologies such as wireless and mobile networks has stimulated wide applications of mobile health care system. It is important to know as much about how the health care systems works as possible. In more health care systems, sensors are used for monitoring the patients Personal Health Information (PHI). Nowadays various sensors are available for monitoring the various health problems. Depends upon the person's health condition the sensors are chosen. For example Heart rate sensor,

Temperature sensor and EEG sensors are different type of sensors [1],[2],[3],[4]. The sensors are already defined to the particular job such as collecting the personal health information and transmit it to the health care centre. As a result a large amount of personal health information data will be generated by sensor in very short period. Since the sensors contain the low charge, it cannot directly transmit the data over the long distance to the health care centre Mobile phones with integrated technology such as WIFI, camera, Bluetooth and 3G and other similar capabilities along with the embedded computing devices are available worldwide with reasonable cost. Hence we are introducing the smart phone to receive the sensed data and transmit it to the health care centre.

Manuscript received on April, 2013.

Aparnaa.M, Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India,

Sacred Heartamir.C Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India,

Vigneshwari.K, Information Techonology, Vel Tech Hightech Dr.Rangaragan Dr.Sakunthala Engineering College, Chennai, India,

The smart phone can transmit the data to the health care centre using 3G transmission with High speed and High reliability. Based on this data the medical professional will respond to the user as and when required.

As per our concept, the smart phone will transmit the data (PHI) for every 5 minutes under normal conditions[5] whereas in case of emergency the smart phone will transmit the sensed data for every 10 seconds . Since the smart phone is used for various purposes such as phoning, chatting with friends, surfing etc the battery charge of the smart phone may get reduced automatically and there may be a chance to get switched off. To avoid such cases then we make use of the opportunistic computing.

Medical user Smartphone Healthcarecenter

Fig.1.Overview of m-healthcare system

In this paradigm, all pervasive and available communication opportunities are exploited to provide computing services to meet application needs by leveraging available computing resources that are available in the reachable environment. Here the wifi will use the resources of other smart phone to transmit the sensed data to health care center using opportunistic computing.

Security is one of the important requirement for any type of communication. If there is no proper security in the data transmission, then there is every chance for the unauthorized person to access the patients' personal health information. When the user's smart phone gets switched off the WIFI will make use of other smart phone to transmit the sensed data hence in such cases there is a chance of others to access the personal health information of the user. Hence, we make use of an encryption algorithm to encrypt the user's health information and then transmit to health center through the smart phone. Since the data is encrypted and then transmitted through the smart phone no one can access personal health information of the other user.

II. SYSTEM MODEL

In our system, a medical personnel at the health care centre who is considered trustworthy is responsible for initializing and controlling the entire health care system. A user who wishes to get the benefits of the mobile healthcare system registers himself as a medical user under a particular health care centre, then a medical professional examines the user and generates his health profile. Based on the health profile, the users are then provided with the particular type of sensors such as heart rate, blood sugar level and other materials. Once being equipped with the sensors the users can move anywhere

unlike in hospital [15], [16], [17] .The sensors begin to collect the sensed data and transmit them to the user's smart phone which is then transmitted to the health care center. The sensors and the smart phone plays a vital role in mobile monitoring of patients. The sensors are used only for sensing hence they can be charged up every day and used whereas the smart phones are used for various purposes, the power of the smart phone may not be sufficient under emergency circumstances. Hence we make use of opportunistic computing where whenever a medical user is in emergency other medical users in the nearby area can contribute their resources.

A. PPSPC framework

In this section, we propose our PPSPC framework which focuses on initializing the system, the scenario depicting healthcare care monitoring under normal conditions and the health care monitoring during emergency situations.

Fig.2.Sytem model of m-healthcare system

1. Initializing the system:

According to our work, the person at the health care centre is responsible for initializing the entire system. The authority at the health care center generates the bilinear parameters () by running gen(sp) using the security parameter (sp).He also selects the encryption algorithm that is to be used, two secure cryptographic hash functions H and H´, two random elements (h_1,h_2) in G_1 is choosen also the master key is selected by choosing two random numbers (a,b) that belongs to Z_q .
Using the above elements the authority computes x=H(a),A=g^a,e(g,g)^b. The master key(a,x,b) is kept secretely and the remaining parameters are revealed parameters= (q,g,G,G_T,e,H,H',h_1,h_2,A.e(g,g)^b,*Encryption()*).
The medical user MU_i is examined thoroughly and based on this a health profile is generated according to which the users are provided with sensors and the necessary medical software is installed in the users Smartphone. Then the access control key is generated by the authority at the health care center using two random numbers $(r_{i1},r_{i2}) \in Z_q$ which is given as $ak_i=(g^{b+ar_{i1}}, g^{r_{i1}}, g^{r_{i2}}, h_1^{r_{i1}}, h_2^{r_{i2}})$ for MU_i.user MU_i. The user is equipped with the sensors and the required keys including aki and ki to report their health data to the health care center.

2. Health Monitoring Under Normal Scenario:

The medical user MUi chooses the current date CD and computes the session key (ski), Ski=H(ki||CD) and is given to the sensors and Smartphone. The data, rdata collected for every five minutes by the sensors are encrypted using the session key, Encrytion(ski,rdata||CD) to the Smartphone using Wi-Fi technology. The Wi-Fi technology increases the coverage. The Smartphone on receiving the encrypted data uses the session key(ski) to decrypt the data so as to process the rdata after which the data is sent to the healthcare center using 3G technology MUi||CD||encryption(ski,data||CD). The authority after receiving the processed data uses the master key (x) for computing MUi's secret key ki=H(MUi||x) and uses this to compute ski=H(ki||CD).This session key is used to recover the processed data data||CD from encrypted(ski,data||CD).The date is corrected and the authority sends the processed data to the medical professionals.

3. Health Monitoring Under Emergency Situation:

When MU_0 faces an emergency such as abnormal raise in the heartbeat and becomes unconscious, then the authority at the healthcare centre monitors all these changes and act to this situation immediately by sending the medical professional according to the medical user's need. Before the arrival of the medical professional the user has to be monitored continuously for which the user's Smartphone requires high power for transmitting the user's health information due to which there are many chances that the resources in the user's Smartphone may not be sufficient. During such a situation the user contacts a nearby medical user who is accepted as a helper if he is qualified as a helper and get his resources to transmit his health information to the health care centre. To preserve the privacy of the medical user's health information we encrypt the data before it reaches the helpers Smartphone. To find if a person passing by is a medical user the medical user MU_0 performs the following:

1. The user MU_0 chooses a random number $r \in Z_q^*$ and computes e(g,g)^{br} and c=(c_1,c_2,c_3) as
$c_1= g^r$ $c_2=A^r.h_1^{-r}$ $c_3=h_2^{-r}$

2. when another MU_j passes by the emergency location,MU_0 sends c=(c_1 c_2 c_3) to the MU_j .Once MU_1 receives c=c_1 c_2 c_3 he performs the following.

Uses his access control key $ak_j=(g^{b+ar_{j1}}, g^{r_{j1}}, g^{r_{j2}}, h_1^{r_{j1}}h_2^{r_{j2}})$ and computes the following

$$=\frac{e(c_1,g^{b+ar_{j1}})}{e(g^{r_{j1}},c_2).e(g^{r_{j2}},c_3).e(h_1^{r_{j1}}h_2^{r_{j2}},c_1)}$$

$$=\frac{e(g^r,g^b,g^{ar_{j1}})}{e(g^{r_{j1}},g^{ar},h_1^{-r}).e(g^{r_{j2}},h_2^{-r})e(h_1^{r_{j1}}h_2^{r_{j2}},g^s).}$$

$$=\frac{e(g^r,g^b).e(g^r,g^{ar_{j1}})}{e(g^{r_{j1}},g^{ar}).e(g^{r_{j1}},h_1^{-r})e(g^{r_{j2}},h_2^{-r}).e(h_1^{r_{j1}}h_2^{r_{j2}},g^r)}$$

$$=\frac{e(g^r,g^b)}{e(g^r,h_1^{r_{j1}}h_2^{r_{j2}})^{-1}.e(h_1^{r_{j1}}h_2^{r_{j2}},g^r)}$$

$$=e(g,g)^{br}$$

Computes the H'(e(g,g)^{br} || ts in which ts is the current timestamp and send back authentication || ts to MU_0. After the user receives authentication || ts at timestamp ts', the user MU_0 checks the validity of the time interval between ts' and ts to prevent replay attack. If |ts'-ts| $\leq \Delta T$ where ΔT is the transmission delay.MU_0 accepts authentication || ts and rejects otherwise then MU_0 uses the stored e(g,g)^{br} to compute authentication' = h'(e(g,g)^{br}|| timestamp) and checks authentication' = authentication if it fails,MU_j is not authenticated as a medical user.

It is clear that if a person is not medical user then he cannot generate $g(g,g)^{br}$ to produce a valid authentication to pass MU_o's authentication.

B. *ANALYSIS OF BENEFITS OF OPPORTUNISTIC COMPUTING IN MOBILE HEALTH CARE EMERGENCY*:

In this section , we analyze the benefits provided by the opportunistic computing to a user who is at emergency. Let us consider that the medical professionals will arrive after a time period t_1 to help a user in emergency. Assuming that the users arrival follows a poisson distribution$\{N(t_1),t_1\geq 0\}$ the rate of arrival of the user is taken as μ.The number of other users who are eligible to help a user at emergency is given as $N_h(t_1)=n_0$ and the number of users who pass by that scenario but are not eligible to help is given as $N_h(t_1)=n_1$.Therfore the total number of users who arrive at the scenario before the arrival of the ambulance with the medical professionals between the time period t_0 and t_1 could be n_0+n_1. The probability that a user arriving at time τ can help a user at emergency is $P(\tau)$.The following theorem can give the expected number of users who can help a user at emergency and expected resources that can be contributed by them.

Theorem 1:

The number of medical users who are expected to contribute resources within $[t_0,t_1]$ is $E[N_h(t_1)]=\mu t_1 p$ where $p=1/t_1\int_{t_0}^{t1} P(\tau)\ d\tau$

Proof:

The total users arriving within the time period $[t_0,t_1]$ is given as $N(t_1)=N_h(t)+N_h(t_1)=n_0+n_1$ and the time τ is uniformly distributed in the time period $[t_0,t_1]$.while defining $p=P\{$a user who arrives in$[t_0,t_1]$ is a eligible person to help$|N(t_1)=n_0+n_1\}$, we have $p=1/t_1\int_0^{t1} P(\tau)\ d\tau$.The users arrive independently and so $P\{N_h(t_1)=n_0, N_h(t_1)=n_1 \mid N(t_1)=n_0+n_1\}$ will give the number of users who are qualified to help during the total n_0+n_1 Bernoulli's experiment.

$$P\{ N_h(t_1)=n_0, N_h(t_1)=n_1\}$$

$$=\binom{n0+n1}{n0}p^{n_0}(1-p)^{n_1}e^{-\mu t_1}\frac{\mu t_1^{n0+n1}}{(n0+n1)!}$$

$$=\frac{(n0+n1)!}{n0!n1!}p^{n_0}(1-p)^{n_1}\cdot e^{-\mu t_1(p+1-p)}\frac{\mu t_1^{n_0}\mu t_1^{n_1}}{(n_0+n_1)!}$$

$$=e^{-\mu t_1 p}\frac{(\mu t_1 p)^{n_0}}{n_0!}\ e^{-\mu t_1}\frac{(1-p)\mu t_1(1-p)^{n_1}}{n_1!}$$

The above equation indicate that both $N_h(t_1)$ and $N_h(t_1)$ are independent poisson process and their rate is $\mu t_1 p$ and $\mu t_1(1-p)$.Hence the number of users who are expected to help a medical user in emergency by contributing their resources is given as

$$E[N_h(t_1)]=\mu t_1 p \text{ where } p=\frac{1}{t_1}\int_{t_0}^{t_1} p(\tau)\,d\tau.$$

Let us assume that the resources that can be contributed by a user who is eligible to help a medical user in emergency be γ per unit time.The following theorem gives the resources that are expected to be contributed by the opportunistic computing before the arrival of the medical professional.

Theorem 2:

The resources that are expected to be contributed by the medical users who are eligible to help a user in emergency is $\frac{\mu t_1^2 p}{2}.\gamma$.

Proof:

Consider if the j^{th} helper arrive at the time τ_j to the emergency location then the total resources $R(t_1)$ that can be contributed by all the helpers who are qualified is given as $\sum_{j=1}^{N_h(t_1)}(t_1-\tau_j).\gamma$.Since

$$= E\{R(t_1)|N_h(t_1)=n_0\}$$

$$=E\{\sum_{j=1}^{N_h(t_1)}(t_1-\tau_j).\gamma|N_h(t_1)=n_0\}$$

$$= E\{\sum_{j=1}^{n_0}(t_1-\tau_j).\gamma|N_h(t_1)=n_0\}$$

$$=n_0t_1\gamma - E\{\sum_{j=1}^{n_0}\tau_j.\gamma|N_h(t_1)=n_0\}$$

$$= n_0t_1\gamma - \frac{n_0t_1\gamma}{2}$$

$$=\frac{n_0t_1\gamma}{2}$$

From Theorem 1 we know $E(N_h(t_1))=\mu t_1 p$ $E[R(t_1)]=\sum_{n_0=0}^{\infty}(P\{N_h(t_1)=n_0\}\,|E\{R(t_1)N_h(t_1)=n_0\})$

$$\sum_{n_0=0}^{\infty}P\{N_h(t_1)=n_0\}.\frac{n_0t_1\gamma}{2}$$

$$=\frac{t_1\gamma}{2}\cdot E(N_h(t_1))=\frac{\mu t_1^2 p}{2}.\gamma$$

$$= E\{\sum_{j=1}^{n_0}(t_1-\tau_j).\gamma|N_h(t_1)=n_0\}$$

$$=n_0t_1\gamma - E\{\sum_{j=1}^{n_0}\tau_j.\gamma|N_h(t_1)=n_0\}$$

$$= n_0t_1\gamma - \frac{n_0t_1\gamma}{2}$$

$$=\frac{n_0t_1\gamma}{2}$$

III. RELATED WORK

The opportunistic computing has increased the great interest recently, and we have briefly reviewed them which are related to our work [2], [4], [5]. In [4], 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 [5], 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 [2] 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 [4] and [5] 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.

IV. EXPERIMENTAL WORK

The health care monitoring is very important during m-Healthcare emergency with minimal privacy disclosurein today's world. So the sensors are provided to the medical user which senses the health information about the medical person. The output will be then collected from sensors and they are transmitted to the user's smart phone through wifi , it is then transmitted to the health care centre by means of 3g transmission. In case of any failure in the smart phone such as when it gets switched off, the wifi router will search for other medical user's smart phone to transmit the data to the health care centre by means of opportunistic computing paradigm. This information is passed to the Health care centre for every 5 minutes under normal conditions and for every 10 seconds during the emergency conditions. Once the information reaches the health care centre, medical professional who continuously monitors the health information about the medical user will aid them at the emergency situation by sending the professional at the emergency location or by providing the ambulance.

V. FUTURE ENHANCEMENT

The Smart phones that are available today are op en to every individual and can be programmed easily. Application delivery channels including app store have brought a great change in transforming mobile phone from a normal cell phone to an app phone which enables us to download a variety of applications based upon our need. One of the interested features of these Smart phones is the use of increased number of sensors embedded within them such as GPS, microphone, accelerometer, gyroscope etc. which enables a wide variety of sensing applications in various fields such as gaming, mobile healthcare, entertainment etc. So, we can make use of these features to make Smartphone itself to act as sensors by embedding the required medical based sensors into Smartphone rather than using sensors as a separate component. For example, for a heart patient an ECG sensor in his Smartphone would be helpful to a heart patient to sense the changes in his heart rate. Similarly different type of sensors as required by the patients' health profile can be embedded within the Smartphone for various medical complications.

VI. CONCLUSION

According to this paper we have introduced the PPSPC framework for m-Healthcare emergency in which smart phones are used to transmit the sensed data by the sensors to the health care centre by using the opportunistic computing paradigm in which the available resources and energy can be opportunistically gathered to process the computing-intensive Personal Health Information (PHI).

REFERENCES

[1] A. Toninelli, R. Montanari, and A. Corradi, "Enabling secure servicediscovery in mobile healthcare enterprise networks," IEEE WirelessCommunications, vol. 16, pp. 24–32, 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," in Proc. BodyNets'10, Corfu Island, Greece, 2010.

[3] 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.

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

[5] 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.

[6] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp. 1–6.

[7] 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.

[8] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010.

[9] M. Conti and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, 2010.

[10] W. Du and M. Atallah, "Privacy-preserving cooperative statistical analysis," in Proc. of ACSAC '01, 2001, pp. 102–111.

[11] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. of ACM KDD'02, pp. 639–644.

[12] A. Amirbekyan and V. Estivill-Castro, "A new efficient privacypreserving scalar product protocol," in Proc. of AusDM '07, pp. 209–214.

[13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. of EUROCRYPT'99, 1999, pp. 223–238.

[14] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Transactions on Parallel Distributed and Systems, to appear.

[15] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy preserving scheme against global eavesdropping for e-health systems," IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp.365–378, 2009.

Ms. Aparnaa.M Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Ms. Sacred Heart Amir.C Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Ms. Vigneshwari.K Studying a Bachelor of Engineering, in the department of IT at Veltech high tech Dr.Rangarajan Dr.Sakunthala Engineering college, Avadi, Chennai.

Mr. A.VishnuKumar received her B.E., Degree from IFET college Engineering, which is affiliated to Anna University in 2007. he received his M.E., Degree from Govt. College of Engineering - Anna University in 2009. At present working as Assistant Professor in Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Avadi from 2009 to tilldate. He doing his Ph.D. in Anna University and his research work is progressively going on in the area of Cloud Computing