Integrated Intelligent Research (IIR)
International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.47-49
ISSN: 2278-2389

SPOC: A Secure and Private-pressuring Opportunity Computing Framework for Mobile – HealthCare Emergency Using Smart Phone

M.Sankareswari[1] ,V.Sarala Devi[2]

[1]Research Scholar, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
[2]Assistant Professor, Department of Computer Applications, Dr. M.G.R. Educational and Research Institute University, Chennai
Email- sankareswari4@gmail.com, saralavinoraj@reddiffmail.com

Abstract- Today we have an abundant increase in the development of Information and Technology, which in-turn made the Humans body even to carry a Mini-Computer in their Palms with Screen touch, Ex: Smart phone's & Tablets etc., and parallel with the rich Enhancement in the Wireless Body Sensor Units, it is quite useful to the Enrichment of the Medical Treatment to be perfectly useful, comfortable via Smart Phones Using the networks (2G & 3G) carriers and made the treatment very easy even to the Common person in the society with the low cost money. With these the healthcare Authorities can treat the Patients (medical users) remotely where the patients reside at home or company or school or college or anywhere or at various places they work. This type of a treatment called for M-Healthcare (Mobile- Healthcare). Although in the m-healthcare service there are many security and data Private problems to be overcome. Here we have A Secure and Private- Preserving Opportunistic Computing Framework called M-HealthCare, for Mobile-Healthcare Emergency. Using the Smart phone and SPOC, the Software or Hardware like computing power and energy can be gathered opportunistically to process the intensive Personal Health Information (PHI) of the medical user when he/she is in critical situation with minimal Private Disclosure. And also we introduce an efficient user-centric Private access control in SPOC Framework which is based on attribute access control and a new private-preserving scalar product computation (PPSPC) technique and Makes a medical user (patient) to participate in opportunistic computing in transmitting his PHI data. Elaborated security analysis describes that the proposed SPOC framework can efficiently achieve user-centric Private access control in M-Healthcare emergency. In this paper we introduce Private-Preserving Support for Mobile Healthcare using Message Digest where we have used MD5 algorithm ,which can certainly achieves an efficient way and minimizes the memory consumed and the large amount of PHI data of the medical user (patient) is reduced to a fixed amount of size compared to AES which parallels increases the Speed of the data to be sent to TA without any delay which in-turn the professionals at Healthcare center can get exactly the Recent tablet user PHI data and can save their lives in correct time. As the algorithm is provided tight security in transmitting the patients PHI to TA. In respective performance evaluations with extensive simulations explains the MD (message digest) effectiveness in-term of providing high-reliable Personal Health Information (PHI) process and transmission while reducing the Private disclosure during Mobile-Healthcare emergency.

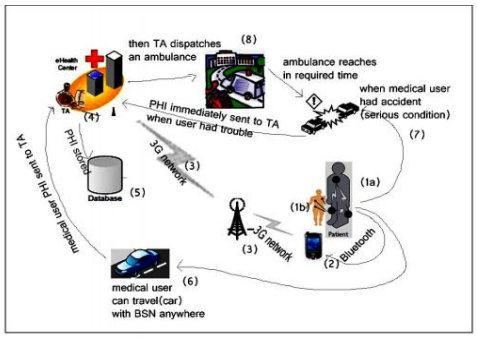
Keywords: Healthcare, Computing, Private Preserving, Message Digest, Mobile-Healthcare, Remote Healthcare.

I. INTRODUCTION

Today in the world we have an abundant development the side of the Information and Technology. By which comparatively increased in the enrichment of the Body Sensor Nodes (BSN), Smartphone"s, and sensor Units. The Pharmacy field achieved a lot of improvement and advancement in saving the People lives using the latest technology based on the body sensor nodes, body sensor Units and Smartphone"s. The sensor nodes are made in a small Where as in m-healthcare system the patients (medical users) who are registered at the healthcare centre and implanted the sensor nodes and appended with a Smart phone device can be easily monitored remotely and there is no need of wasting their valuable time here and they can move anywhere they require and can have their works be done. Likewise the medical user (patient) can achieve a high quality medical healthcare remotely. The professionals at the healthcare centre are supposed to monitor the patient's condition at regular intervals of time.Things to be done at this particular time spending at the hospitals and clinics, the patient or the medical user can attain a high quality of the medical healthcare remotely by monitoring at the healthcare centre by a TrustedAuthority (TA). The above scenario can come under the mobile healthcare system (m-healthcare). The m-healthcare is completely and purely remote based monitoring to the people who are regularly affected from the Chronic medical problems like, heart diseases and diabetes, blood oxygen saturation .In general the Real-time, continuous patient monitoring, Patients have to wait for a Longer period of time losing their important

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.47-49
ISSN: 2278-2389

For Example, The patient who is suffering or facing from chronic diseases such as heart attacks and diabetes heart rate variability, respiration rate, skin conductance,Skin temperature, arterial blood pressure, and blood alcohol concentration. Any people have registered at the healthcare centre available. Once the patient is registered in user id any people is to be treated as a medical user like which there can be a n number of medical users registered and for each user there given a user id by which the trusted authority (TA) at the healthcare centre monitors the PHI data periodically. The medical user registration if completed he/she can be implanted to body wearable miniaturized body sensor nodes and a Smart phone device with the software available in it.



Now the patient can move to a anywhere place where any person decides at anytime and can achieve a high quality medical treatment. The sensor nodes (BSN) which are implanted to body gathers all the typical readings at first as minimum such as heart rate, pulse, sugar, blood sugar level, blood pressure and body temperature, eye problem etc, and via Bluetooth transmits to the mobile device and then transmitted to the healthcare center via 3G networks with the user id. The healthcare centre professionals can identify the readings of which medical user is sent and when the user in Emergency required actions taken by sending an ambulance and a medical representative with the vehicle and can protect the user life and thus the medical user can achieve a high quality medical healthcare service.

II. LITERATURE SURVEY

When the medical user is at normal situation [6] the sensor nodes can send the PHI data readings to the healthcare centre for every 10 minutes of regular intervals of time and if the patient (medical user) situation is serious then the body

Sensor nodes are in busy getting the readings from the patient's body in less period of time and transmit a huge and large amount of data for every 5-10 seconds in regular time intervals. Where the medical user provided Smart phone is used as a normal phone like we can use it for phoning, chatting, playing videos, listening music and browse internet. Due to which the resources of the mobile like power, battery gets down and in emergency happens unfortunately and it might happen at low probability. Any medical emergency, when all of us take in to 10, 000 emergency cases into account, the common event amount will reach 50, that's not minimal and outstandingly indicates the actual reliability regarding m-Healthcare system is demanding throughout emergency.

III. GG AND GGT

Bilinear Pairings

Let GG and GGT 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. In group GG, the Computational Differ-Hellman (CDH) problem is hard; it is intractable to compute gab in a polynomial time. However, the Decisional Differ-Hellman (DDH) problem is easy, it is easy to judge.

System Initialization

For a single-authority in m-Healthcare program under consideration, we arrange a trusted authority stated at the healthcare centre will bootstrap the entire system. Especially, by giving the security parameter, TA first attains the Bilinear parameters; and selects a secure symmetric encryption, i.e., MD5, and two secure cryptographic hash functions H and H0 . In addition, TA chooses two random numbers as the master key, two random elements in GG, and computes we use MD5 algorithm which is enhancement to the AES. Where as in the AES the PHI data of the medical user collected by the sensor nodes at the emergency situation is a large amount of data within a less period of time and the AES having to encrypt the PHI data is very delay and lot of time and memory space is wasted and by which the TA is unable to view the current status of the medical user. But

IV. TA ALGORITHMS

Depending upon Ui‟s personal health information, TA first selects the exact body sensor nodes to govern Ui‟s personal BSN, and installs the required medical software's in Uri's Smart phone device. Then, TA selects two random numbers and performs to compute the access control key for Ui. Finally, TA uses the master key b to compute the secret key. Ui first selects the current date CDate, computes the session key for a single day, and distributes the session key ki to his personal BSN and Smart phone device. For every five minutes, BSN gathers the raw PHI data and sends the encrypted results; to the Smart phone device. On getting the Smart phone device uses ki to recover rPHI from Enc. After performing rPHI, the Smart phone device uses the 3G technology to submit the performed PHI data undergone to healthcare center. When the TA receives Ui at the healthcare center, he first goes with the master key b to compute Ui‟s secret key ski, and uses ski to compute the current session key after performing that, TA uses kit to recover PHI from Enc. If the recovered

International Journal of Web Technology
Volume: 04 Issue: 01 June 2015 Page No.47-49
ISSN: 2278-2389

CDate is corrected, TA sends PHI to the medical representatives for monitoring.

V. OUTPUT

The concept of this paper is implemented and different results are shown below, the propose paper's concepts shows efficient results and has been efficiently tested on different Datasets.The results shown below in Figure 4, 5, & 6, are performed on various datasets and are picturised according to the results obtained.

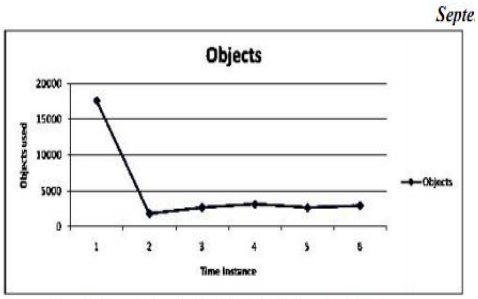


Fig. 4 Time taken by Node to initialize by objects.

Here fig.4 graph is obtained by taking under considerations of the number of datasets to be taken for a particular time instance. Likewise a number of datasets for a six time instances, for every single time instance a lot of datasets are performed, as per the data obtained the graph is drawn.

Time Instance	Objects
1	17632
2	1800
3	2659
4	3137
5	2629
6	2892

Here in fig.5 the graph drawn shows a relation between the time instances and the memory used. Similar as the above graph the datasets are to be considered for every single time instance and six instances are taken for our convenience.

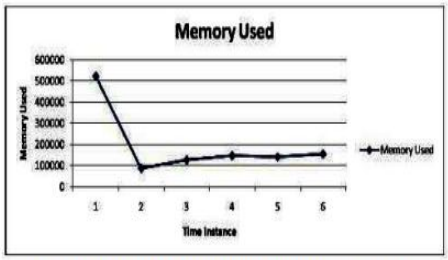


Fig.5 Time taken by Node to compute Memory Used

The fig.6 indicates the graph related to the time instances and the free memory that is left. The above fig.4 clearly depicts the graph of the instances that are used by each and every single node and the objects whereas in fig.5 it shows the graph between the time instances of each and every single node and the memory utilized.

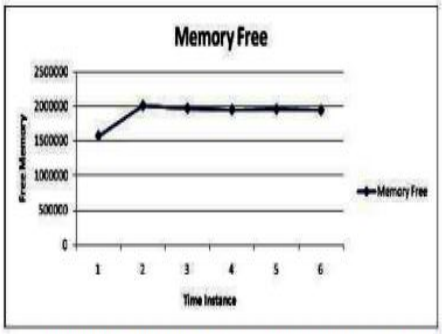


Fig. 6 Time taken by Node Communicating and Free Memory

VI. CONCLUSIONS

In this paper, we had explained the secure and Robustness ,scalability and private preserving opportunistic computing framework for m-Healthcare emergency, which clearly explains the usage of opportunistic computing to gain a high achievement of PHI process and transmission when in emergency and which mainly reduces the Private exposure during the opportunistic computing. Elaborated security analysis gives that the exhibited SPOC framework will attain the efficient user-centric Private access control.In our further work, we are able to perform on Smart phone-based experiments to Identify and verify the effectiveness of the exhibited SPOC framework and m-healthcare. Adding to this, we also will security and scalability reasons of PPSPC with inner system attacker, with which the protocol is not followed by the inner System attackers, are not purely honest.

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," MONET, 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-basedencryption," IEEE Transactions on Parallel and Distributed System, to appear.