SSTC: Secure and Seclusion-Upholding Timeserving Computing for Physical Health Information

Saikat Saha*, Mr. Sanjeev Kumar Tomar, Mr. Kunal Gupta****

*Computer Science, Amity University
**Asst. Prof., Computer Science, Amity University

Abstract- Now a day's Wireless Sensor is booming research area and used in most of the sensitive application. Mobile Healthcare is one of the most important, sensitive and necessary research point in WSN. Mobile Healthcare (m-Healthcare) helps the Healthcare Centre to provide a better Healthcare Solution to the Medical User. Although m-Healthcare is flourishing, the Security is most challenging problem in Mobile Healthcare. In this paper we propose a Secure and Seclusion-Upholding Timeserving Computing (SSTC) for Physical Health Information in mobile Healthcare. In case of medical emergency how the physical health information is transferred securely using SSTC has been discussed in this paper. SSTC will also provide a timeserving method while it's needed at the time of medical emergency. SSTC will provide minimum disclosure of patient's highly sensitive Physical Health Information.

Index Terms: Mobile Healthcare (m-Healthcare), Physical Health Information (PHI), Body Sensor, Private Key.

I. INTRODUCTION

Wireless Sensors are one of the main component of mobile healthcare system. Sensors used in m-Healthcare are known as the wearable body sensors. These wearable body sensors are implanted in the patient's body. Body sensor senses the various condition of patient's body like blood pressure, heart beat, blood sugar, body temperature and others. These data are known as the physical health information. The highly sensitive physical health information is then transmitted to authorised medical healthcare centre. According to the received PHI medical experts present in the medical centre will provide a remote healthcare solution.

Fig. 1 PHI Transmission Scenario in m-Healthcare

But in case of medical emergency m-Healthcare faces various problem like privacy of transferred data, power effectiveness of the transmitting device. While the emergency occurs body sensors senses the various condition of patient very rapidly and generate a huge data that is needed to transmit via 3G network to the authorised healthcare centre. To send these huge data a transmitting device (mobile) should have enough power. But mobile is used for various purpose like calling, web browsing, navigating etc. and battery power may be drained. In that case patient's mobile will use the passing by person's mobile phone who has enough power in his mobile phone battery to send the highly sensitive physical health information to the authorised healthcare centre. If a passing by person has no subscription of the medical healthcare solution provided by the healthcare centre then the person can't be selected for the further process of transmitting the physical health information. Another factor that will be consider for selecting other sources is how much trust worthy is the passing by person depending upon the similarity in their physical health information. The selection of other devices is shown in the fig. 2.

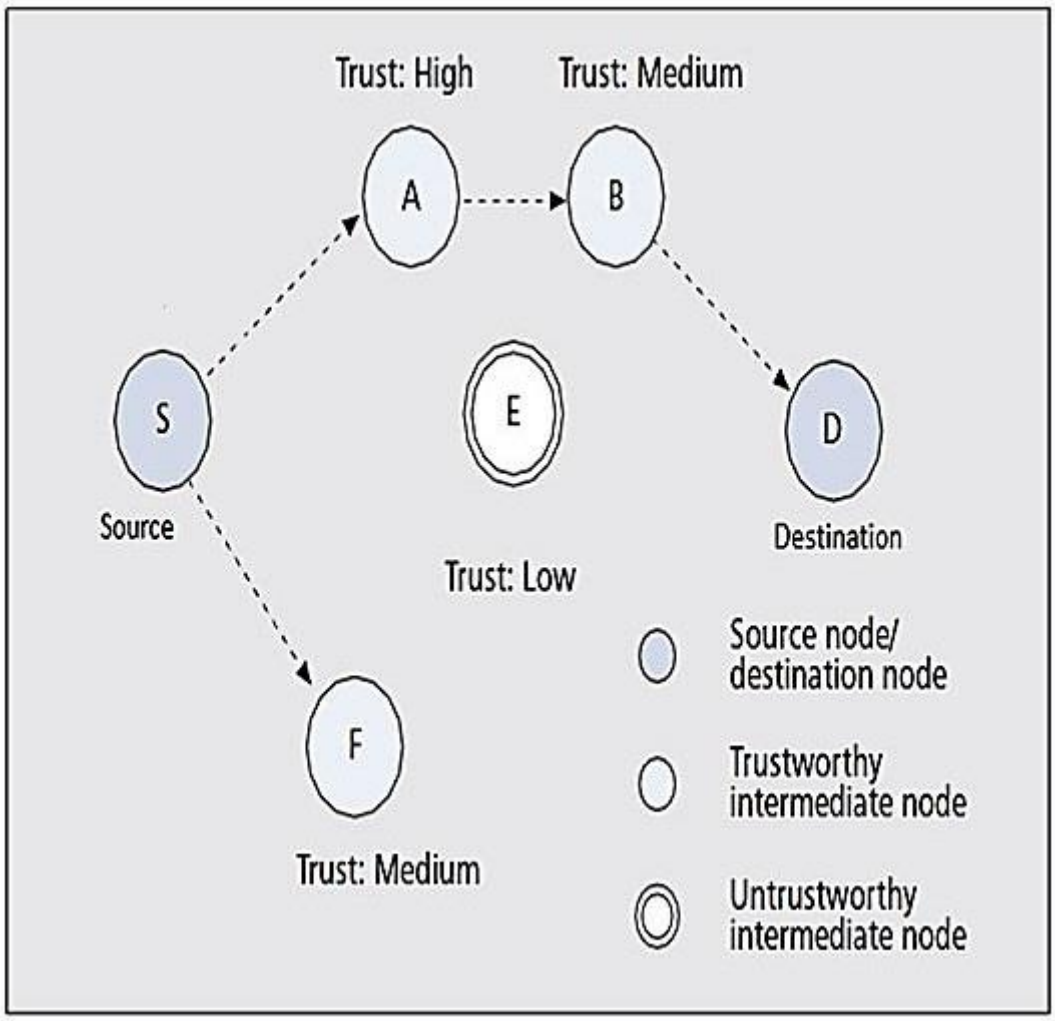


Fig. 2 Selection of Other Power Source

I. PROPOSED SYSTEM

To overcome the security issues and the low power of transmission device we proposed the Secure and Seclusion-Upholding Timeserving Computing. It will work in two steps:

i. Data Encryption
ii. Tackle Power Issue.

i. Data Encryption:

Using the symmetric key physical health information will be encrypted. At the time of subscription for a m-Healthcare solution a private key will be distributed to the medical user. Medical user will share the private key only with the authorised m-Healthcare centre. Data collected by the body sensor will be encrypted by the medical user using the shared private key and the encrypted PHI will be send to the helping node. Helping node will not be able to read the sensitive physical health information as they are encrypted with the medical user's private key. Helping node will forward the encrypted data to the m-Healthcare Centre. These data can easily be decrypted here as they have the user's private key. Symmetric key provides the security to the patient's health information.

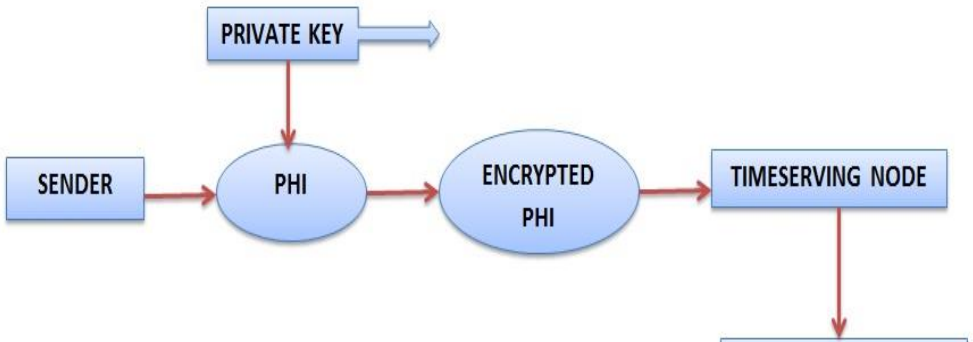


Fig. 3 PHI Encryption

ii. Tackle Power Issue:

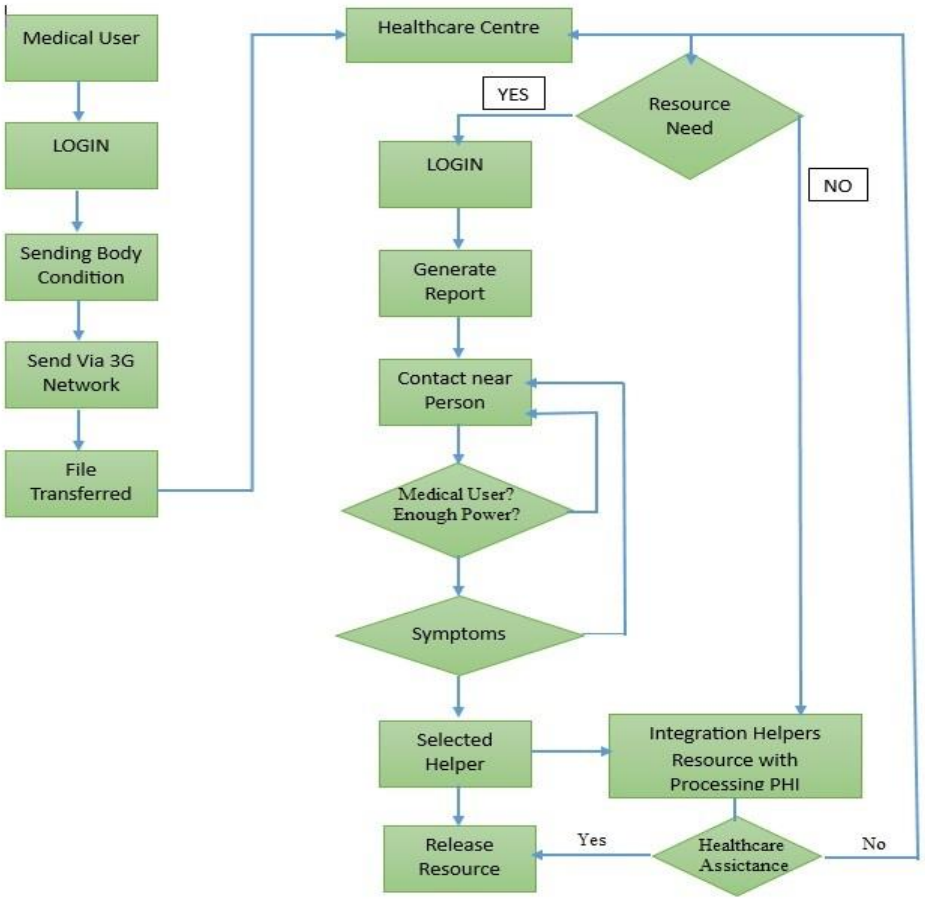
Lower power of transmitting device is solved using the passing by Timeserving Devices. While the medical user don't have enough power to transmit the data, it looks for the other timeserving devices which are medical user. Selection of trust worthy helping node is shown in fig. 2. These trust worthy devices help in forwarding the encrypted PHI to the m-Healthcare Centre.

II. BLOCK DIAGRAM & PROCEDURE

Procedure of the Computing:

1. Body sensor will gather the body condition.
2. Generate the PHI.
3. If power is sufficient, send the PHI to the Healthcare Centre.
4. Else Contact the passing by person.
5. Check whether the passing by person is a medical user or not.
6. If the person is not medical user discard it.
7. If the person is a medical user check whether the transmitting device has enough power.
8. Check for the similar symptoms.
9. If a threshold is achieved then the node is selected for the PHI transmission.
10. Send the PHI using the timeserving Node.
11. Receive medical assistance from the authorized medical Healthcare Centre.

Block Diagram:



III. RESULTS

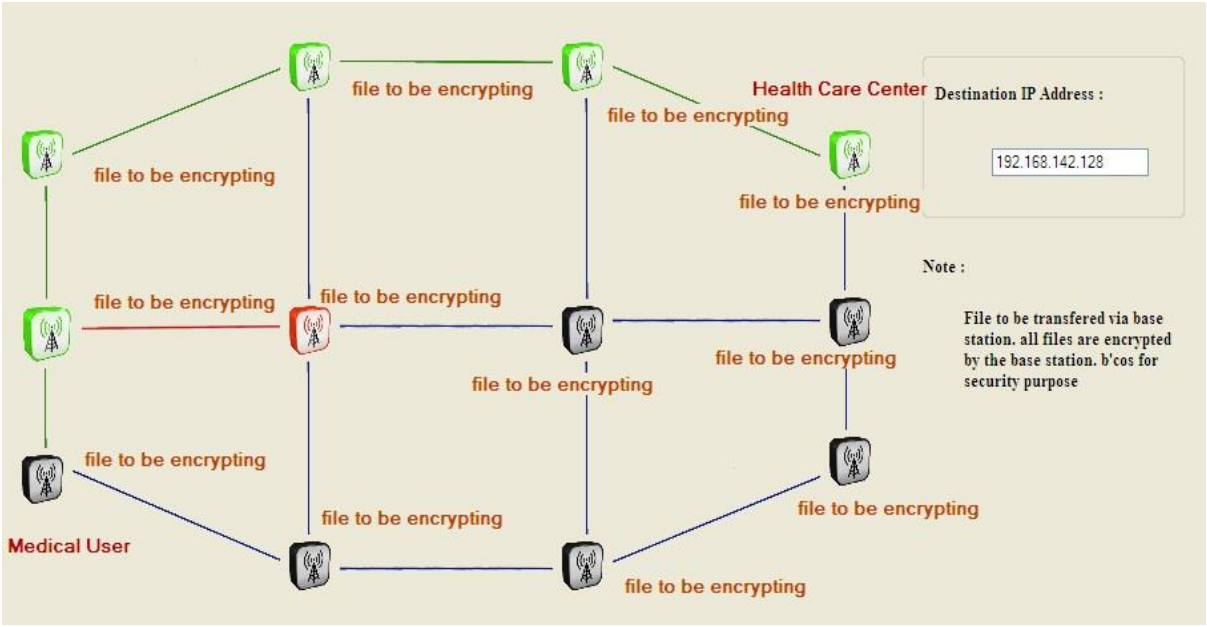


Fig. 4 Encrypted PHI Transmitted Via Trusted Node

In case of emergency Medical User will encrypt the PHI, so that helping nodes could not able to read the data. These encrypted data will be transmitted via helping nodes. Timeserving helping nodes are selected on the basis of SSTC. Here in the result Red node represents the timeserving node which is not qualified for helping. Green nodes represent the qualified timeserving helping nodes. These nodes will help the medical user to transmit the highly sensitive encrypted physical health information to the authorised Healthcare Centre. After decrypting the data with the help of the key, that is shared at the time of subscription with the medical user, healthcare centre will provide mobile assistance to the medical user.

IV. Conclusion and Future Work

In this paper we proposed a computing to secure the medical user's highly sensitive physical health information. The transmission power and the security of sensitive physical health information is the main issues in transmitting physical health information. For an effective mobile Healthcare service physical Health Information are needed to be transmitted at the time of emergency case while the medical users transmitting power is not enough in order to send the rapidly generated highly sensitive physical health information. Proposed SSTC is simple way to handle these kind of emergency cases effectively. In future asymmetric key encryption can be used for better security and low computational cost.

Acknowledgment

I would like to express my special thanks of gratitude to Mr. Sanjeev Kumar Tomar, Mr. Kunal Gupta, as well as our HOD who gave me the golden opportunity to work on the topic Secure and Seclusion-Upholding Timeserving Computing for Physical Health Information, which also helped me in doing a lot of Research and I came to know about so many new things. I am really thankful to them. Secondly I would also like to thank my parents and friends who helped me a lot in finishing this research within the limited time.

References

[1] Saikat Saha, M. Tech, Sanjeev Kumar Tomar, asst. prof., "Issues in transmitting Physical Health Information in m-Healthcare", International Journal of Current Engineering and Technology, Vol.3, No.2 (June 2013).
[2] The Privacy and Security Gaps in Health Information Exchanges A White Paper by the AHIMA/HIMSS HIE Privacy & Security Joint Work Group.
[3] Ajit Appari and M. Eric Johnson, "Information security and privacy in healthcare: current state of research", Int. J. Internet and Enterprise Management, Vol. 6, No. 4, 2010.
[4] Marco Avvenuti, Paolo Corsini, Paolo Masci and Alessio Vecchio, "Opportunistic computing for wireless sensor networks", IEEE Wireless Communications, June 2007.
[5] C.-C. Lin et al., "A Healthcare Integration System for Disease Assessment and Safety Monitoring of Dementia Patients," IEEE Trans. Info. Tech. Biomedicine, vol. 12, 2008, pp. 579–86.
[6] U. Varshney, "Pervasive Healthcare and Wireless Health Monitoring," Mobile Net. Apps. vol. 12, 2006, pp. 113–27.
[7] W.-B. Lee and C.-D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," IEEE Trans. Info. Tech. Biomedicine, vol. 12, 2008, pp. 34–41.
[8] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51–58, 2010.