ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

# *Highly Secured and Efficient HSOC for Mobile Healthcare System*

**K. Muthukrishnaveni**[1]
M.E
Network Engineering
Francis Xavier Engineering College
Tirunelveli – India

**Dr. S. Gomathi**[2]
M.E., Ph.D.
Associate professor, Dept of CSE
Francis Xavier Engineering College
Tirunelveli – India

***Abstract:*** ***The combination of mobile phone and BSN (Body Sensor Node) has become an exciting new area of m-healthcare and it has provided an entirely new route for providing m-healthcare services. But still there is a problem of providing security and privacy preservation in these services. Therefore in order to provide these features, in this paper, we propose a new scheme called HSOC (Highly Secured Opportunistic Computing) for m-healthcare. With HSOC, the resources of mobile phones such as energy and computing power can be opportunistically gathered in order to process the computing-intensive personal medical information (PMI) with minimal privacy disclosure during the emergency time and the malicious nodes can be detected and removed. To provide the high reliability of PMI process and transmission and to leverage the PMI privacy disclosure, an efficient user-centric two-step privacy access control has been introduced in HSOC structure, which is based on an attribute based access control and a new complete confidentiality and authenticated dot product (CCADP) technique. It allows a medical user to decide who can participate in opportunistic computing to assist in processing his overwhelming PMI data. In order to detect and remove the malicious node, an IDPS (Intrusion Detection and Prevention System) is introduced in HSOC. The security analysis of this work shows that it can greatly achieve user-centric two-step privacy access control in m-healthcare. In addition, the performance evaluations through more simulations demonstrate the HSOC's efficiency in terms of providing high-reliable-PMI process and transmission while reducing the privacy revelation during m-Healthcare process and the detection and removal of malicious node by the IDPS.***

***Keywords: Mobile-healthcare, CCADP, opportunistic computing, IDPS, user-centric two-step privacy access control.***

## I. INTRODUCTION

In the latest world, mobile healthcare system is emerging as an important application to provide healthcare service to protect the life of human beings. For this purpose mobile healthcare system uses mobile phone and Body sensor nodes to observe the patients' medical conditions such as BP, sugar, diabetes, heart disease and so on [1], [2], [3],[4]. Especially in the mobile healthcare system, the patients are not needed to be observed inside the home or hospital environment. Instead of that, the patients are equipped with the mobile phone and wireless body sensor network (BSN) which is formed by wearable body sensor nodes, so that the patients can move outside and could get the superior healthcare observation from the medical professionals anytime and anywhere. For example, as shown in Fig.1, the personal medical information (PMI) of each patient such as BP, sugar are first observed by BSN, then grouped by mobile phone via Bluetooth. Finally, this PMI is transmitted to the healthcare center through 3G networks. As per these received PMI data, the medical professionals at the healthcare center can observe the patients' health conditions continuously and could quickly response to the patients' serious situations and save their life by sending ambulance and medical personnel to the patients' location in a correct time.

Even though mobile healthcare system is more useful to the patients by providing superior healthcare observation, there are some challenges existing during medical emergency. In order to understand the challenges faced by the mobile healthcare

 

system, let us consider the following example. In normal conditions, for every five minutes the patients' PMI is reported to the healthcare center. However, when there is an emergency condition, the patient's PMI is reported to the healthcare center for every 10 seconds. During this time, the patient's BSN will observe the PMI busily and a large amount of PMI data will be generated in less time and high-intensive monitoring is performed before the arrival of ambulance and medical personnel. However, since mobile phone is used for many other applications, the mobile phone's energy could be considered as insufficient during the emergency condition. Even though this type of unexpected event may occur with the lowest probability when we consider more number of emergency cases. If we consider 1000 cases the average will be around 50 which is not negligible and clearly indicates that there is a challenge in the reliability of mobile healthcare system.

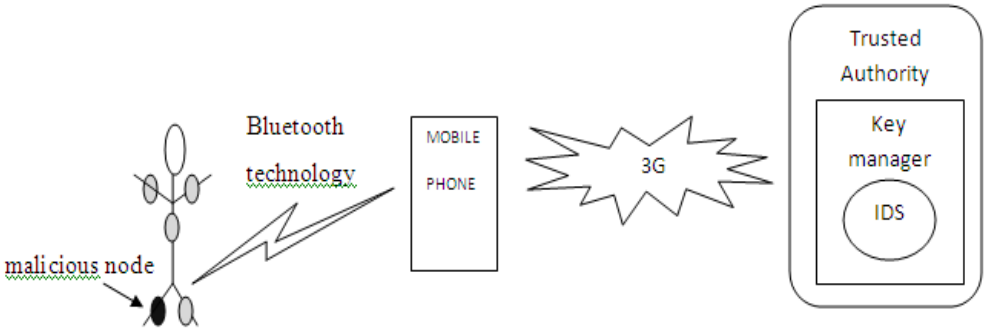


Fig. 1 Ubiquitous health monitoring in m-Healthcare system

Recently, opportunistic computing plays a major role as a new ubiquitous computing model, and it has received much interest [6], [7], [8]. Particularly opportunistic computing employs the available device in the environment to build up a platform for the execution of computing-intensive task. For instance, if the energy available in the mobile phone to execute the processing of PMI exceeds the required energy level, it will use the energy of the available device; here it is mobile phone to perform the service [6]. It is very clear that the opportunistic computing model can be implemented to face the challenge of reliability issue in PMI process and transmission. However, the PMI is very sensitive to the patients and during the processing of the raw PMI; the privacy of PMI would be revealed. Therefore, the high reliability of PMI process with minimal privacy revelation during the opportunistic computing becomes a challenging issue in mobile healthcare system. The existing Secrecy Preserving Techniques in the mobile healthcare environment are homomorphic based which leads to high computation cost and high communication overhead [3] and are not provided with high security. In addition, if any node in the body sensor network becomes malicious by any virus attack, it could send falsified data to the trusted authority. So it is also becoming a serious issue in the mobile healthcare system.

In this paper, a new scheme, Highly Secured Opportunistic Computing structure called HSOC has been proposed to meet these issues. It is based on non-homomorphic encryption technique which provides less communication overhead and low computation cost. With this proposed scheme, the patient can get help from the qualified helpers by the user-centric two-step privacy access control with increased reliability of PMI processing and minimized revelation of the patient's privacy and if there is any malicious node, it is identified and removed by the Intrusion Detection and Prevention System (IDPS).The actual contribution of this paper are as follows.

- First, to make use of the available mobile phone which are contacted opportunistically, we propose HSOC, Highly Secured Opportunistic Computing for mobile healthcare system. With HSOC, the PMI is collected and is revealed during opportunistic computing, and therefore to reduce the PMI privacy revelation, user-centric two-step privacy access control consisting of two steps has been used to allow only qualified helpers to participate in opportunistic computing based on identical symptoms.

 

- Second, in the opportunistic computing, to achieve the user-centric two-step privacy access control, we introduce a novel non-homomorphic encryption-based complete confidentiality and authenticated dot product (CCADP) technique, where the attribute based access control can help the patient to identify other users in emergency, and CCADP protocol can further allow only those qualified helpers who have identical symptoms [2].

- Third, to identify the malicious node in the Body Sensor Network, an Intrusion Detection and Prevention System is enabled in the key management system of the trusted authority. The IDPS will detect the malicious node after decrypting the encrypted data sent by the BSN through the mobile phone and 3G network.

- Fourth, to evaluate the efficiency of the HSOC structure, we develop a custom simulator built in NS2. More simulation results show that the proposed technique ensures high reliability of PMI processing and reduced revelation of patient's privacy.

The remainder of this paper is as follows: in Section 2, we discuss about the system model and security model, and recognize our design target. Then, we present the HSOC structure in Section 3, followed by the performance evaluation in Section 4. Finally, we draw our conclusions in Section 5. Even though, a nearby person has a mobile phone with him, his mobile phone cannot be used for opportunistic service unless he is a qualified helper. It is very important that the helper's mobile phone should be installed with the same proper medical software to participate in the opportunistic computing. The absence of this software will not make him as an ideal helper. Therefore, the Step-I privacy access control is given the higher priority. Step-II access control permits those users who have identical symptoms to take part in the opportunistic computing. The main reason is that those qualified helpers have identical symptoms such that it is easy to process the same kind of PMI. Here, the threshold T is used as the self-control parameter. During the emergency time at a location with more traffic, the threshold T will be set high to reduce the patient's privacy revelation and if the location has less traffic , the threshold T is set to be low such that the reliability of PMI processing and transmission is first guaranteed.

## II. ARCHITECTURE AND DESIGN TARGET

In this section, we learn about the architecture model, security design, and identify our design target as well.

### *A. Architecture model and security design*

In our system design, we consider a trusted authority (TA) and a group of patients U1, U2, U3, U4, U5….; TA is a legitimate and efficient entity placed at healthcare centre, in which the key manager is present installed with an IDPS, which is used for detecting and removing the malicious node. The intrusion detection and prevention system has a package with an ability to identify the virus-attacked node and it can be removed from the network or it can be blocked from further proceedings. The TA is mainly responsible for the initialization of the system, for providing correct body sensor nodes and to provide key materials to the medical users. All the patients are provided with personal BSN and mobile phones, which can continuously collect the patient, are PMI and send it to the authorized centre for better healthcare system [1], [2]. Here, the patients are considered as the mobile ones i.e., the patient can walk or move anywhere. The success of the mobile healthcare system depends on the BSN and the mobile phones which have to be charged up every day so that we can achieve a better healthcare quality every day. The mobile phone is used for many other purposes. Therefore the power may become insufficient for PMI processing and transmission during emergency time. To meet this hardest situation in the mobile healthcare system, if any of the medical user $U_y$ find out some other medical user $U_x$ in an emergency condition, they will contribute their mobile phone's resource to help $U_x$ for processing and transmitting of PMI [7], [8], [9]. Opportunistic computing is mainly used to provide the reliability of highly sensitive PMI process and transmission in mobile healthcare system. Since the PMI of the patient is very sensitive, even at the emergency condition the patient is not interested to reveal his PMI to all other passing-by medical users [2]. Instead of that, the patient is ready to reveal his PMI to the medical users who have equal symptoms like him. This thing could be achieved by opportunistic computing with reduced revelation of highly sensitive patient's PMI.

 

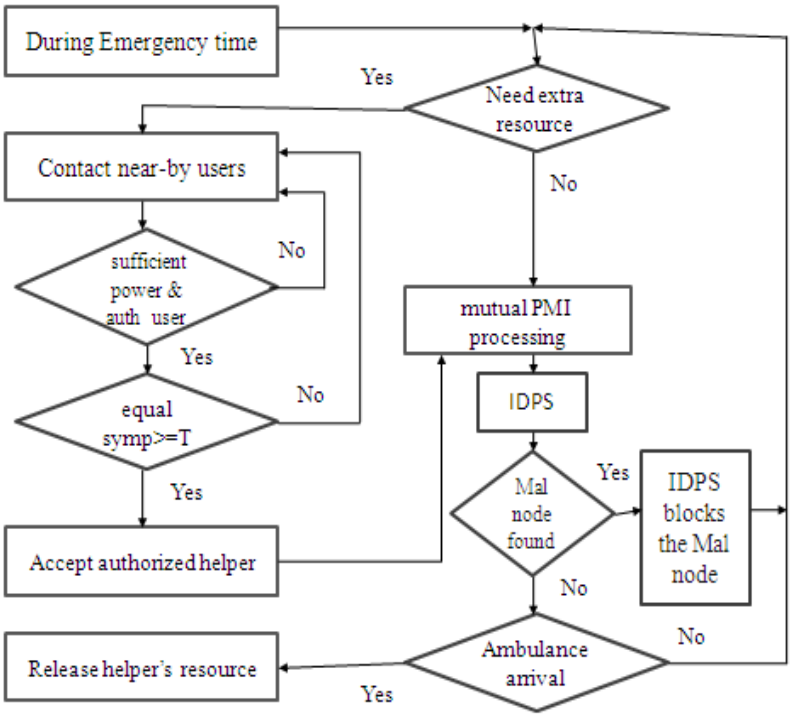


Fig. 2 Two-step privacy access control for mobile healthcare system with opportunistic computing

Especially, in our security design, we have shown that the two-step privacy access control is required for reaching the high reliability of PMI process and transmission in the mobile healthcare system. In addition, the Intrusion detection and prevention system (IDPS) will check for malicious node or if any node is attacked by any virus or not. If so, it will block the attacked node and proceed the further processing as shown in Fig. 2.

### *B. Design Target*

Our design target is to build up a Highly Secured Opportunistic Computing structure to provide high reliability of the patient's PMI processing and transmission with reduced revelation of patient's privacy and detecting the malicious node to prevent the transmission of forged data to the trusted authority. Purposely, we use 1.Opportunistic computing in mobile healthcare system [6] to have the high reliability of PMI processing and transmission; 2. Build up user-centric two-step privacy access control for reducing the revelation of the patient's privacy. And 3. Introduce IDPS at the trusted authority to detect any malicious node and block it from further proceedings to prevent the transmission of forged data to the trusted authority.

## III. PROPOSED HSOC STRUCTURE

In this section, we discuss about the proposed HSOC structure which consist of four parts: scheme initialization, two-step privacy access control, detection and prevention of malicious node by IDPS and security analysis of HSOC structure in the mobile healthcare system. Before describing them, we first discuss about the bilinear pairings [10], which is the basis of the proposed HSOC structure.

### *A. Bilinear Pairings*

Let A and A' be two multiplicative cyclic groups with the same prime order q. Suppose A and B are equipped with a pairing, i.e., a nondegenerated and efficiently assessable bilinear map e : A xA'→At such that $e(a1^a , a2^b) = e(a1, a2)^{ab}$ belongs to A t for all a,b €Fq and any a1,a2 €A

 

### B. Description of HSOC

#### 1) Scheme Initialization

Let us consider a healthcare center which will bootstrap the whole system. The trusted authority will be there in the healthcare center in which the IDPS is installed with an IDPS package. Specifically, given the security factor k, TA first generates the bilinear parameters by running gen(k) , and chooses a secure symmetric encryption algorithm Enc(), i.e., AES, and two secure cryptographic hash functions H and H', where H;H' : $\{0,1\}^* \rightarrow F_q^*$.In addition, TA chooses two random numbers (a,x)€ $F_q^*$ as the master key key, two random elements (h1,h2) in A and computes b=H(A),E=$g^a$,and e(g,g)$^x$. Finally, TA keeps the master (a,b,x) secretly, and publishes the system parameters.

Let us assume that there are about n symptom characters in the mobile healthcare system. Each patient's medical profile will be represented by the vector format. It will be a binary vector, example is a'=($a_1$,$a_2$,…$a_n$) where $a_i$€a' shows that a symptom character $a_i$=1 if the patient has a particular symptom and $a_i$=0 if the patient don't have that particular symptom. Therefore for every patients, the medical professionals will first check their medical conditions and will provide the correct BSN and their medical profiles are generated. After then, the following steps will be performed by the trusted authority.

- After checking the $U_x$ patient's health condition, the medical professional will provide the appropriate body sensor nodes and installs the necessary medical software in the patient's mobile phone.
- Then the trusted authority chooses two random numbers and generate the access control key for the user $U_x$. .
- Finally, TA make use of the master key b to compute the secret key W=H($U_x$||b) for $U_x$.

After getting the correct body sensor nodes and being provided with the key materials i.e., access control key AK and secret key W, the patient $U_x$ can securely report to the trusted authority and can achieve the better healthcare observation by the following procedure:

- The current date is first chosen by the patient $U_x$ for the computation of the session key G=H(W||current date) for a particular day and this session key G is distributed to the BSN of the patient and to his mobile phone.
- For every five minutes, the BSN gather the raw PMI data and reports the encrypted value Enc(G,raw PMI|| current date) to the mobile phone through the Bluetooth technology.
- After receiving the Enc(G,raw PMI|| current date), the mobile phone uses G to recover raw PMI from Enc(G,raw PMI|| current date). After processing raw PMI, the mobile phone uses the 3G technology to send the processed PMI to healthcare center in the forn of $U_x$||current date||Enc(G,raw PMI|| current date).
- When the Trusted Authority receives $U_x$||current date||Enc(G,raw PMI|| current date) at the healthcare center, it first uses the master key b to compute $U_x$'s secret key W=H($U_x$||b), and uses W to compute the current session key G=H(W||current date). After that, trusted authority uses G to recover raw PMI||current date from Enc(G,raw PMI||current date). If the recovered current date is correct, trusted authority sends PMI to the medical professionals for observation.

#### 2) Two-step Privacy Access Control

When there is an emergency in the healthcare system, the patient $U_x$ will fall down suddenly, the healthcare center will monitor the serious condition and will immediately send the ambulance and the medical professional to the patient's location. Usually, the ambulance will reach the patient's location at about 20 minutes. During that time, the medical professional needs to observe the patient's more-intensive PMI. However, the power of the mobile phone may not be sufficient to transfer the more-intensive PMI processing and transmission. In this scenario, the opportunistic computing as shown in the Fig.3, is executed,

 

and the following two-step privacy access control is used to identify the authorized medical user and to reduce the revelation of the patient's PMI privacy during opportunistic computing.

***Step-I access control*:** The main target of step-I access control is to identify the authorized medical user [1]. For that purpose, the $U_x$'s mobile phone first chooses a random number s and compute the authentication key $e(a,a)^{xs}$ and $N=(N_1,N_2,N_3)$.

When user $U_y$ passes by the emergency location, $U_x$ sends $N=(N_1,N_2,N_3)$ to $U_y$ and $U_y$ will perform the following steps:

$U_y$ Use his access control key AK to compute the authentication key $e(a,a)^{xs}$. The computation time taken to generate this authentication key will be about some timestamp and it will be sent to the patient $U_x$'s mobile phone along with the authentication key at timestamp'. It will be in the form of authentication key=H'$(e(a,a)^{xs}||$timestamp).

When user $U_x$ receives (authentication key||timestamp) at timestamp', $U_y$ first check out the soundness of the time interval between timestamp' and timestamp in order to prevent the replay attack. If |timestamp'-timestamp|$<\Delta_{time}$ , where $\Delta_{time}$ denotes the required valid time delay for transmission. $U_x$ accepts and process the authentication key||timestamp and rejects otherwise. $U_x$ uses the stored $e(a,a)^{xs}$ to compute authentication key'=H'$(e(a,a)^{xs}||$timestamp). If the received authentication key matches with the $U_x$'s authentication key, $U_y$ is authenticated as an authorized medical user, and passes the step-I access control.

***Step-II access control*:** If $U_y$ passes the step-I access control, $U_x$ and $U_y$ go on with to perform the step-II access control to verify whether there are some identical symptoms or not [3]. Let the personal health profiles of the patient $U_x$ and $U_y$ are $a'=(a_1,a_2,\ldots a_n)$ and $b' =(b_1, b_2, ..b_n)$, respectively. $U_x$ first fix an expected threshold value T for a number of identical symptom characters. Then, for computing a'. b' in a highly secured way, $U_x$ and $U_y$ invoke our newly designed CCADP protocol in algorithm in 1. Since the CCADP protocol ensures neither $U_x$ nor $U_y$ will reveal their personal medical profiles to each other during the calculation of a'.b' and it can efficiently achieve highly secured access control. For example, if the calculated value a'. b' $\geq$ T, $U_x$ passes the step-II access control and becomes an authorized helper.

Then, $U_x$ assigns the current session key $G_x$ =H($W_x$||current date) to $U_y$. With the session key $G_x$, $U_y$ can decrypt and process the raw PMI sent from $U_x$'s personal body sensor node, and also transfer the processed PMI to healthcare center to minimize the load of $U_x$'s mobile phone. However, if the calculated value a'. b' <T, $U_y$ is not an authorized helper to take part in opportunistic computing. Note that the threshold value T is not permanent, if the remaining power of $U_x$'s mobile phone can last for some more time, T can be fixed comparatively high to reduce the revelation of the patient's PMI privacy. However, if the remaining power is less, T can be fixed low in such a way that the reliability and PMI processing and transmission is first guaranteed.

***Algorithm 1.*** complete confidentiality and authenticated dot product protocol.

1. **process** CCADP PROTOCOL
2. ***Input*:** $U_x$'s binary vector $a'=(a_1,a_2,\ldots a_n)$ and $U_y$'s binary vector $b' =(b_1, b_2, ..b_n)$ where $n\leq 2^6$
3. ***Output*:** The dot product a'.b' = $a_i$. $b_i$ where ( i=0 1,….n.)
4. ***Step-1*:** $U_x$ first perform the following calculation:
5. chooses two large primes $\boldsymbol{\rho}$,$\lambda$ where $\boldsymbol{\rho}$ is of the length $|\boldsymbol{\rho}|$=256 bits and $\lambda > (n+1).\boldsymbol{\rho}^2$.
6. set K=0 and choose n positive random numbers ($C_1$, $C_2$, $C_3$…….,$C_n$) .
7. for each element $a_i \in a'$ **do**
8. choose a number $r_i$, compute $r_i.\lambda$ such that $|r_i.\lambda| \approx 1024$ bits, and calculate $k_i= r_i.\lambda - c_i$
9. **if** $a_i$=1 then

 

10. $C_i=\boldsymbol{\rho}+c_i+r_i.\lambda$, $K=K+k_i$
11. **else if** $a_i=0$ **then**
12. $C_i=c_i+r_i.\lambda$, $K=K+k_i$
13. **end if**
14. **end for**
15. keep ($\lambda$, K) secret, and send ($\boldsymbol{\rho}$, $C_1$, $C_2$, C…,$C_n$) to $U_y$.
16. **step-2:** $U_y$ then does the following calculation:
17. **for** each element $b_i$€ b'**do**
18. **if** $b_i=0$ **then**
19. $D_i=\boldsymbol{\rho}.C_i=\boldsymbol{\rho}^2+c_i.\boldsymbol{\rho}+r_i.\boldsymbol{\rho}.\lambda$ if $a_i=1$ (or) $D_i=\boldsymbol{\rho}.C_i=c_i.\boldsymbol{\rho}+r_i.\boldsymbol{\rho}.\lambda$ if $a_i=0$
20. **else if** $b_i=1$ **then**
21. $D_i=C_i=\boldsymbol{\rho}+c_i.\boldsymbol{\rho}_+r_i.\lambda$ if $a_i=1$ (or ) $D_i=C_i=c_i._+r_i.\lambda$ if $a_i=0$
22. **end if**
23. **end for**
24. compute $D_i$ where (i=0,1,…n) and return D back to $U_x$.
25. **step-3:** $U_x$ continuously perform the following calculation:
26. compute V=D+K mod $\lambda$
27. **return** V-(Vmod $a^2$)/ $a^2$ as the dot product**,** a'.b'= $a_i$. $b_i$ where (i=0,1,…n).$\sum_{i=0}^{n} ai\,.\,bi$
28. **end procedure**

***Intrusion detection and prevention system***

In the mobile healthcare system, there is a possibility of so many attacks in the body sensor network [5]. Any node in the body sensor network can be attacked by any type of virus and will become a malicious node. The malicious node is not supplied with the key materials by the key manager in the trusted authority i.e., the access control key AK and the secret key W is not provided to this malicious node. But this malicious node will generate a session key G' by using its own falsified secret key W' and it is distributed to the mobile phone. Now the forged data is encrypted by this malicious node using its own falsified secret key W'. The encrypted forged data will be in the format of Enc (G',forged data|| current date), where G' is the duplicate session key. The duplicate session key will be in the format of G'=H(W'||current date), where W' is the duplicate secret key. Now using the falsified session key the mobile phone will process the forged data and send it to the trusted authority using CCADP protocol. The key manager in the trusted authority has been installed with the proper Intrusion Detection and Prevention System (IDPS) i.e., IDPS package to check the authenticity of the node. After receiving the encrypted forged data, the key manager in the trusted authority will detect the forged data being encrypted with the duplicate keys and the identification of the malicious node is also detected and it will take necessary steps to block the further proceedings of the malicious node and it is removed from the body sensor network by proper acknowledgement to the mobile phone of the corresponding patient.

 

## IV. PERFORMANCE EVALUATION

In this section, we analyze the performance of the developed HSOC structure using a custom simulator built in NS2. When the body sensor nodes and the mobile phones are within their transmission ranges [1], it is assumed that, both the devices could be always workable with sufficient energy and power. The performance metrics used here are 1) the average number of authorized helpers, which shows how many authorized helpers can take part in the opportunistic computing within a given period of time, 2) the average resource utilization ratio (RUR), which is defined as the fraction of the resources utilized by the authorized medical user in emergency to the total number of resources used in the opportunistic computing for PMI processing within a given period of time.

In our proposed HSOC structure, the CCADP protocol used relies on non-homomorphic based encryption technique and is very efficient in terms of computation cost and communication overhead. The computation cost will be about 2n multiplications, where n is the total number of identical symptoms. The communication overhead will be about (n+1).1024 + 256 bits.

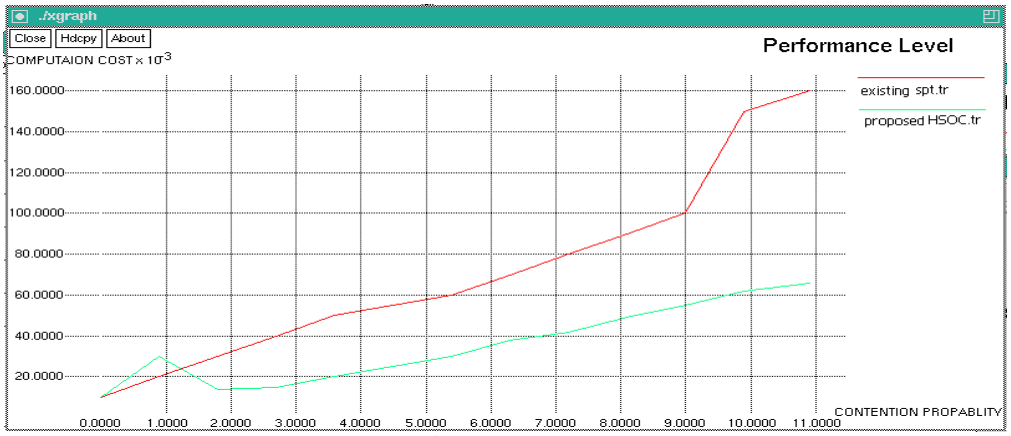


Fig. 3 comparison graph of computation cost between HSOC and SPT

In Fig. 3, the comparison of computation cost between the existing SecrecyPreserving Technique and our proposed HSOC structure is shown. From the fig, it is apparent that the CCADP protocol being employed in the Proposed HSOC structure is efficient in the case of computation cost.

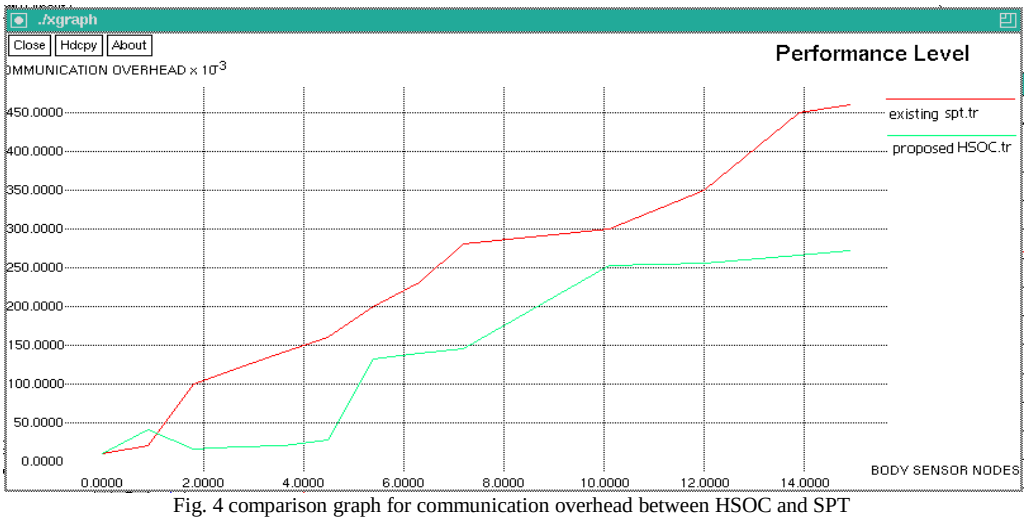


Fig. 4 comparison graph for communication overhead between HSOC and SPT

In Fig. 4, the comparison graph of communication overhead between the existing Secrecy Preserving Technique and the proposed HSOC structure is shown. From the fig, it is apparent that the communication overhead of the proposed CCADP protocol is less when compared with the existing secrecy Preserving Technique. So it is very obvious that the CCADP protocol is efficient in the case of communication overhead.

 

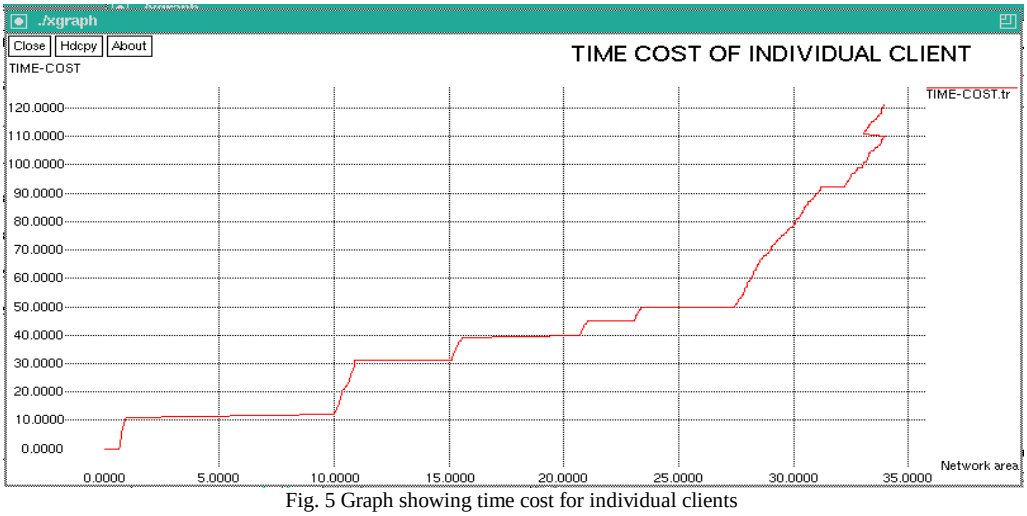


Fig. 5 Graph showing time cost for individual clients

During opportunistic computing, the patient's emergency condition is known to the passing-by users when they pass through that location and each individual user will stop at the target location for few minutes. The time cost will be computed for each individual clientas shown in the Fig. 5. Once the key materials are distributed to the body sensor nodes and the patient's mobile phone, the raw PMI data of the patient is transmitted to the trusted authority with the generation of private key using the access control key, AK and secret key W. The comparison graph of key generation cost between the existing Secrecy Preserving Technique and proposed HSOC structure for each node is shown in the Fig. 6.

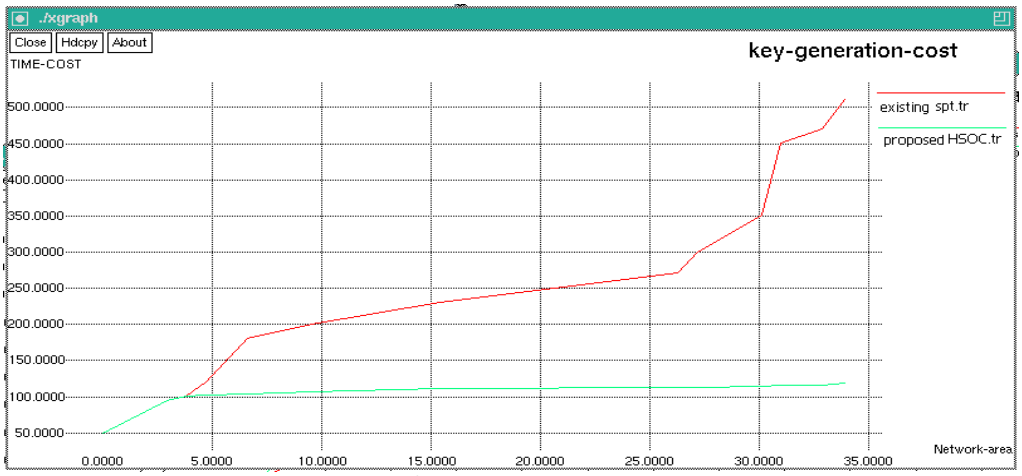


Fig. 6 Comparison graph for key generation cost between HSOC and SPT

## V. CONCLUSION

In this paper, a highly secured opportunistic computing structure have been proposed for mobile healthcare environment, which primarily tells about the opportunistic computing technique to have high reliability of PMI processing and transmission while reducing the revelation of the patient's privacy during the occurrence of opportunistic computing. Thorough security study shows that the proposed HSOC structure can fulfill the two-step privacy access control along with the detection and prevention of malicious node using the IDPS package being installed in the key manager of the trusted authority. In addition, via extensive performance analysis, we have also confirmed the proposed HSOC structure can balance the more-intensive PMI processing and transmission and reduced revelation of the patient's PMI privacy using CCADP protocol with low computation cost and low communication overhead. So, obviously it is very clear that the CCADP protocol is the best protocol in the mobile healthcare environment. In our future work, we plan to do experiments using mobile phones to further prove the efficiency of the developed HSOC structure.

 

## References

1. Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing framework for Mobile-Healthcare Emergency" IEEE transactions on parallel and distributed systems, vol.24,no.3, march
2. 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.
3. 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.
4. 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.
5. X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "Sage: A Strong privacy preserving scheme against Global Eavesdropping for E-health system", IEEE. J Selected Areas in comm.., Vol. 27, No. 4, pp. 365-378.
6. M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, " Opportunistic Computing for Wireless Sensor Networks," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), pp. 1-6, 2007.
7. A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance Evaluation of Service Execution in Opportunistic Computing," Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.
8. M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.
9. M. Conti and M. Kumar, "Opportunities in Opportunistic Computing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.
10. A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," Proc. Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), pp. 209- 214, 2007.
11. www.google.com

## AUTHOR(S) PROFILE

**K.Muthukrishnaveni** is doing her M.E in Francis Xavier Engineering College at Tirunelveli. She received her B.tech degree in Electronics and Communication Engineering from Kalasalingam University, India in 2012. She is an active member of the Computer Society of India (CSI). Her areas of interests are Networking, Mobile Computing, Wireless Networks and Digital Communication.

**S.Gomathi** received her B.E degree in Computer science and Engineering from Manonmanium Sundaranar University, India, in 2003 and her master's degree in Computer science and Engineering from the Noorul Islam Engineering College, TamilNadu, India in 2005. Her research interests include distributed computing and grid computing systems. Currently she is working as an associate professor in Francis Xavier Engineering College,TamilNadu,India.

 