Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.408 – 413

RESEARCH ARTICLE

ESPOC: Framework for M-Healthcare Emergency

B. Veeranna[1], V. Gouthami[2]
[1]Pursuing M.Tech in CSE & JNTU Hyderabad, India
[2]Department of CSE ARTI, Warangal, Telangana, India
[1] veeranna1200@gmail.com, [2] gautami.velakanti@gmail.com

Abstract - With the popularity of smart phones and its apps usage the advancement of wireless body sensor networks (BSNs) and the mobile Healthcare (m-Healthcare), now a day's healthcare providers have transformed into a pervasive environment for better health monitoring even though the major challenge in the mobile healthcare includes information security and privacy preservation. In this paper, we propose a fascinating extended secure and privacy-preserving opportunistic computing framework named as SPOC for m-Healthcare emergency. ESPOC provides smart phone resources that make use of computing power and energy that can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency even with minimal privacy disclosure. In this paper we propose an efficient user-centric privacy access control in ESPOC framework that is based on an new attribute-based access control and a new privacy-preserving scalar product a computation technique that provides knowledge on participate of opportunistic computing to assist in processing his overwhelming PHI data to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare. Detailed security analysis shows proposed framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency.

Keywords— BSN, m-Healthcare, electronic health records, healthcare

I. INTRODUCTION

In the present day world the total healthcare expenditure exceeds Rs. 4.5 trillion which is being consumed by an average of 10% of GDP only in India and is increasing day by day at an average of 5% every year. However, this spend is highly skewed.

This wide disparity in spend means that challenges faced by health systems are somewhat different in the developing and developed world where the global Mobile Health market may be worth up to Rs300bn by 2015 while others predict a market of Rs. 600bn as the advancements in the field of mobile Healthcare (m-Healthcare) system since it contains important applications of pervasive computing to improve health care quality and save many lives with the usage of miniaturized wearable and 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[1].

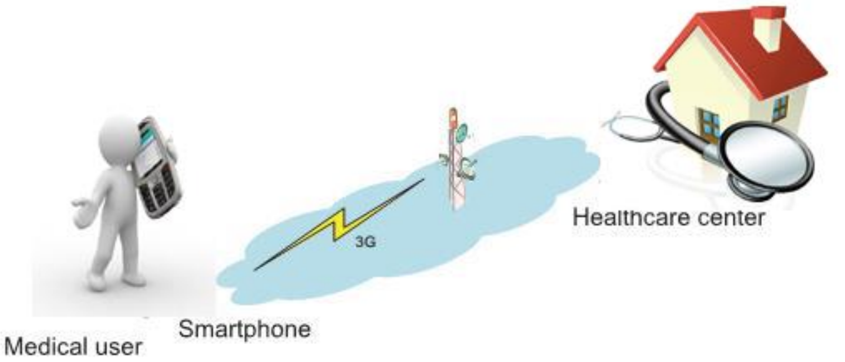


Fig. 1 Continuous health monitoring in M-healthcare system

A m-Healthcare system medical user does not need to be monitored at a specific location such as at home or hospital environment when he or she has being equipped with a smart-phone and a wireless body sensor network (BSN) formed by body sensor nodes that are implanted on him/her having which a medical user can walk outside and receive the high-quality healthcare monitoring information from medical professionals at regular intervals as and when required or when necessary as shown in above figure fig1. Each and every mobile medical user's personal health information (PHI) is stored and monitored such as heart beat, blood sugar levels, blood pressure, temperature, psychological situations and many others can be first collected by BSN and then aggregated by smart-phone via Bluetooth or Wi-Fi later which are further transmitted to the remote healthcare centre via a 3G network.

Based on these collected of PHI data of various users or medical professionals at healthcare center continuously mines and monitors medical users' health conditions and as well quickly react with notifications as and when required hence each Mobile health care system will have a limited number of slots where a user can book a slot and get monitored all the time which may show significant impact on the local communities.

In spite of much advancement in mobile technologies and health care systems mobile health has failed to reach the scale of adoption that many stakeholders or investors have hoped for in the developed world as the complexities of healthcare systems in the developed world requires an appreciation of the working of the funding mechanisms, sometimes healthcare can be funded directly by a patient or their family members or indirectly by private aided insurance systems or may be publically funded by nationalized health services or insurance providers and the latter option of indirect funding often uses formal reimbursement mechanisms to pay for healthcare services and requires insight into how scientific evidence is used to support the uptake of new interventions or services one of such examples in Telangana state is Rajeev Aurogyasri scheme running for the poor people who are below poverty line.

In this paper we propose a solution space for the above said problem space a new extended secure and new privacy preserving opportunistic computing framework (ESPOC) in which each medical user in emergency can achieve his or her own privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the reliability of PHI process and minimize PHI privacy admission in m-Healthcare emergency.

ESPOC is designed to be more secure and privacy-preserving computing framework for m-Healthcare emergency by which the resources available on other requested medical users smart-phones can be used to deal with the designed intensive PHI process in emergency situations to minimize the PHI privacy disclosure ESPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.

ESPOC is designed such a way that it can easily achieve user-centric privacy access control in computing that comprises of attribute oriented access control and a non-homomorphic encryption technique based on privacy-preserving scalar product computation protocol and a attributed oriented access control can help a medical user in emergency to identify other medical users and can further control only those medical users who have similar symptoms to participate in the opportunistic computing without directly revealing users' symptoms[2].

Lastly the effectiveness of the proposed ESPOC framework in m-Healthcare emergency is implemented in PHP and the results have been generated using WEKA 6.0 where the results shows that the proposed ESPOC framework can help medical users to balance the high-reliability of PHI process and minimizing the PHI privacy disclosure in mHealthcare emergency services worldwide but not only in India.

II. RELATED WORK

In our proposed model we will try to overcome these hurdles where some of the key questions such as user safety, expected benefits, cost of aaps and smart phone and the overall impact on the healthcare system and the recommendations to support the use of an intervention or service are typically based on the trade- offs between the proposed benefits versus the risks and economic burden associated with the intervention or service in question. If just in case the benefits outweigh the risks and burden the experts are likely to recommend the intervention or service where the uncertainty associated with the tradeoffs [3].

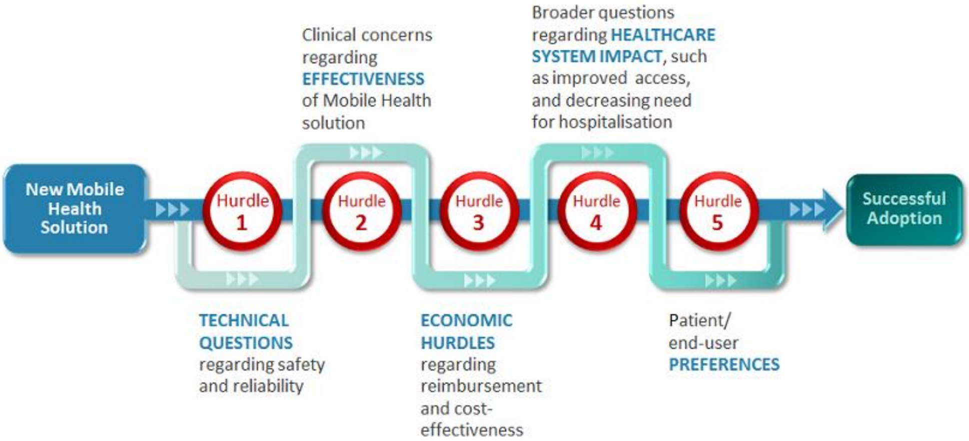

Clinical concerns regarding EFFECTIVENESS of Mobile Health solution
Broader questions regarding HEALTHCARE SYSTEM IMPACT, such as improved access, and decreasing need for hospitalisation
New Mobile Health Solution
Hurdle 1
Hurdle 2
Hurdle 3
Hurdle 4
Hurdle 5
Successful Adoption
TECHNICAL QUESTIONS regarding safety and reliability
ECONOMIC HURDLES regarding reimbursement and cost-effectiveness
Patient/ end-user PREFERENCES

Fig. 2 Hurdles of ESPOC

ESPOC considers a trusted Partner (TP) and a group of n medical users are depicted as U ={U_1,U_2,⋯,U_nl}, by which a powerful entity is located at healthcare center which is mainly responsible for the management of the whole m-Healthcare systems such as initializing the system, allocating or installing proper body sensor nodes and key materials to medical users where each medical user $U_i \in U$, where $0 \leq I \leq n$. With ESPOC the personal BSN and smart-phone sends reports periodically after collecting PHI to the healthcare center for achieving better health care quality [3].

ESPOC can enhance the reliability for high intensive PHI process and transmission in m-Healthcare emergency since PHI is very sensitive where a medical user even in emergency will not expect to disclose his PHI to all passing-by medical users instead he or she may only disclose his PHI to those medical users who have some similar symptoms with him or her where situation can be handled by opportunistic computing with minimal privacy disclosure.

III.PROPOSED SYSTEM

In this section we provide solution space for the above problem space using ESPOC framework that comprises of three parts firstly system initialization, secondly user-centric privacy access control for m-Healthcare emergency, and thirdly analysis of opportunistic computing in m-Healthcare emergency and al the three of them are implemented using bilinear pairing technique which is the core part of our framework [4].

Bilinear pairings are implemented on classes of elliptic curves over a finite field where a field generates a sub-exponential index calculus attack which can be intern used to attack the problem this can be illustrated in the below equations:

A pairing is map entity e: G_1 X $G_2 \rightarrow G_{T,}$ where G_1, G_2 and G_T are groups

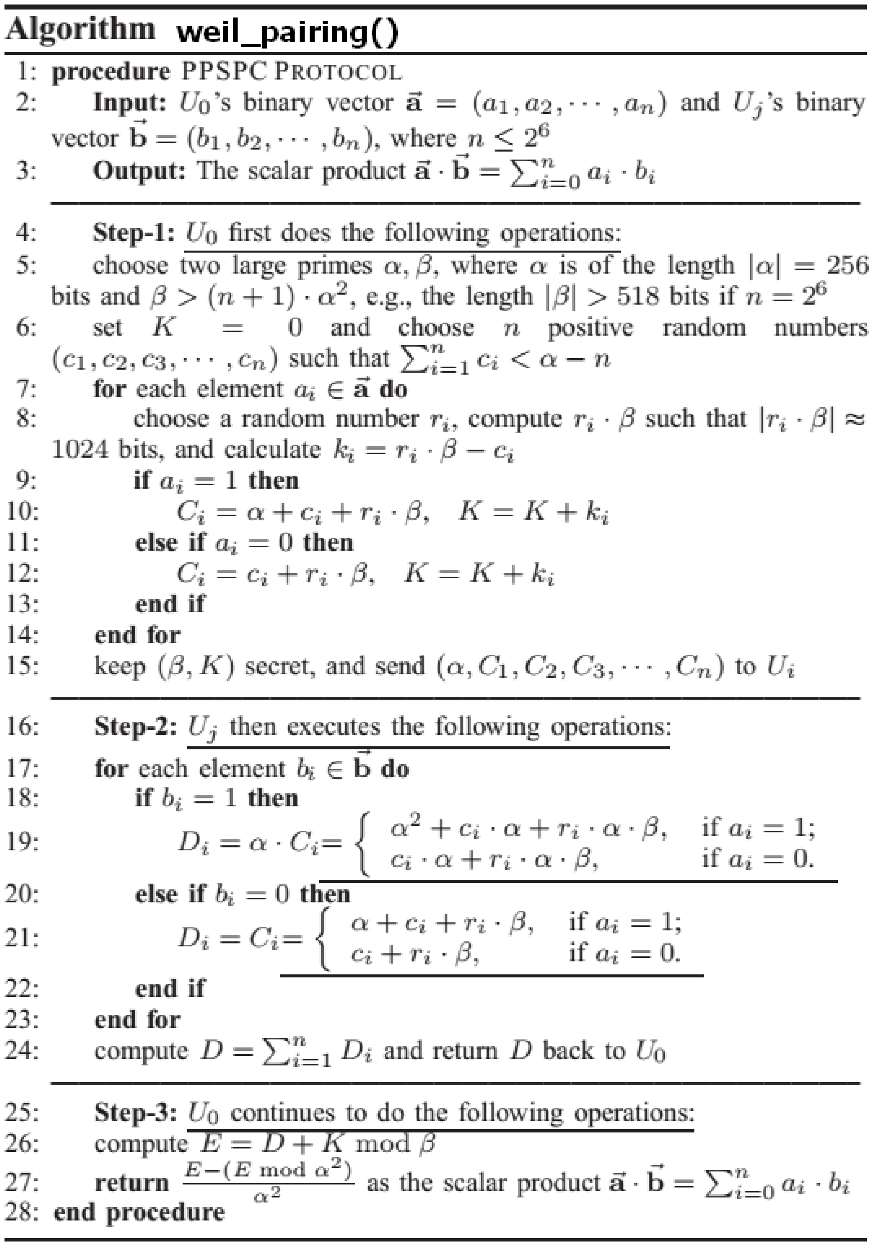
A pairing is symmetric: $G_1 = G_2$, . When $G_1 \neq G_2$ the pairing is said to be asymmetric.

The weil_pairing is a function that maps a pair of points in an n-iterative group of an elliptic curve to an n^{th} square root of unity in some extension field of the field the curve was defined over if we specify more specifically then let ∑ /=F_q be an elliptic curve and let n be a prime divisor of #∑ (F_q) which is a co-prime factor to char(F_q) and the resulting weil_pairing() is a map that is generated based on the below mentioned equation:

$$e : \mathcal{E}(\overline{\mathbb{F}}_q)[n] \times \mathcal{E}(\overline{\mathbb{F}}_q)[n] \to \overline{\mathbb{F}}_q^*.$$

Sometimes we will use the notation e_n instead of e to specify directly the order of the torsion group on which the pairing is defined where the weil_pairing() maps points to a certain extension feld F_{q*}k, which should be large enough to make sure ∑ (F_qk) that contains all n-iterative points as in reality we do not need the full algebraic closure of F_q hence the embedding degree is the degree k of this field extension. When n≠q-1, then k is the smallest integer such that $n \leq j \leq q$ or k contains all n^{th} square roots of unity. If $n \leq j\ q \leq 1$ then in some instances k = 1 and in other instances k = n.

The algorithm used is:



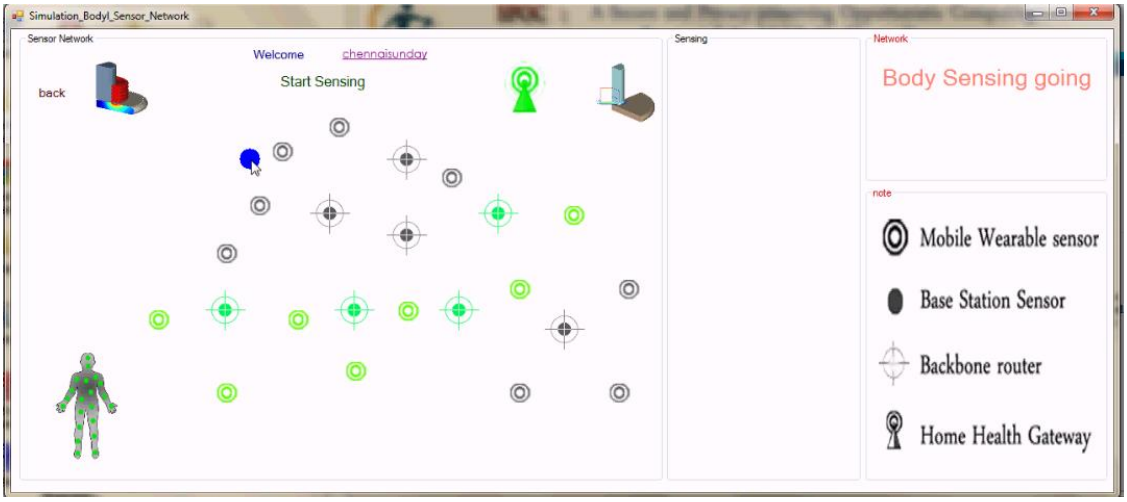
Algorithm weil_pairing()

```
procedure PPSPC PROTOCOL
    Input: $U_0$'s binary vector $\vec{\mathbf{a}} = (a_1, a_2, \cdots, a_n)$ and $U_j$'s binary vector $\vec{\mathbf{b}} = (b_1, b_2, \cdots, b_n)$, where $n \leq 2^6$
    Output: The scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} = \sum_{i=0}^{n} a_i \cdot b_i$
    ----------------------------------------------------------------
    Step-1: $U_0$ first does the following operations:
    choose two large primes $\alpha, \beta$, where $\alpha$ is of the length $|\alpha| = 256$ bits and $\beta > (n+1) \cdot \alpha^2$, e.g., the length $|\beta| > 518$ bits if $n = 2^6$
    set $K = 0$ and choose $n$ positive random numbers $(c_1, c_2, c_3, \cdots, c_n)$ such that $\sum_{i=1}^{n} c_i < \alpha - n$
    for each element $a_i \in \vec{\mathbf{a}}$ do
        choose a random number $r_i$, compute $r_i \cdot \beta$ such that $|r_i \cdot \beta| \approx 1024$ bits, and calculate $k_i = r_i \cdot \beta - c_i$
        if $a_i = 1$ then
            $C_i = \alpha + c_i + r_i \cdot \beta, \quad K = K + k_i$
        else if $a_i = 0$ then
            $C_i = c_i + r_i \cdot \beta, \quad K = K + k_i$
        end if
    end for
    keep $(\beta, K)$ secret, and send $(\alpha, C_1, C_2, C_3, \cdots, C_n)$ to $U_i$
    ----------------------------------------------------------------
    Step-2: $U_j$ then executes the following operations:
    for each element $b_i \in \vec{\mathbf{b}}$ do
        if $b_i = 1$ then
            $D_i = \alpha \cdot C_i = \begin{cases} \alpha^2 + c_i \cdot \alpha + r_i \cdot \alpha \cdot \beta, & \text{if } a_i = 1; \\ c_i \cdot \alpha + r_i \cdot \alpha \cdot \beta, & \text{if } a_i = 0. \end{cases}$
        else if $b_i = 0$ then
            $D_i = C_i = \begin{cases} \alpha + c_i + r_i \cdot \beta, & \text{if } a_i = 1; \\ c_i + r_i \cdot \beta, & \text{if } a_i = 0. \end{cases}$
        end if
    end for
    compute $D = \sum_{i=1}^{n} D_i$ and return $D$ back to $U_0$
    ----------------------------------------------------------------
    Step-3: $U_0$ continues to do the following operations:
    compute $E = D + K \bmod \beta$
    return $\frac{E - (E \bmod \alpha^2)}{\alpha^2}$ as the scalar product $\vec{\mathbf{a}} \cdot \vec{\mathbf{b}} = \sum_{i=0}^{n} a_i \cdot b_i$
end procedure
```

The above algorithm is the only algorithm used in the proposed ESPOC that is efficiently designed to get effective results and provides the solution space for the given problem space as provided in the literature survey and the algorithm is divided into three steps where first step acquires the data required and some data is also generated on random basis for encrypting the data and in second step the acquired data is cleaned and fits in two steps where bi value is 0 or 1 and the last step generates the scalar product for the proposed algorithm.

IV. EXECUTION AND RESULTS

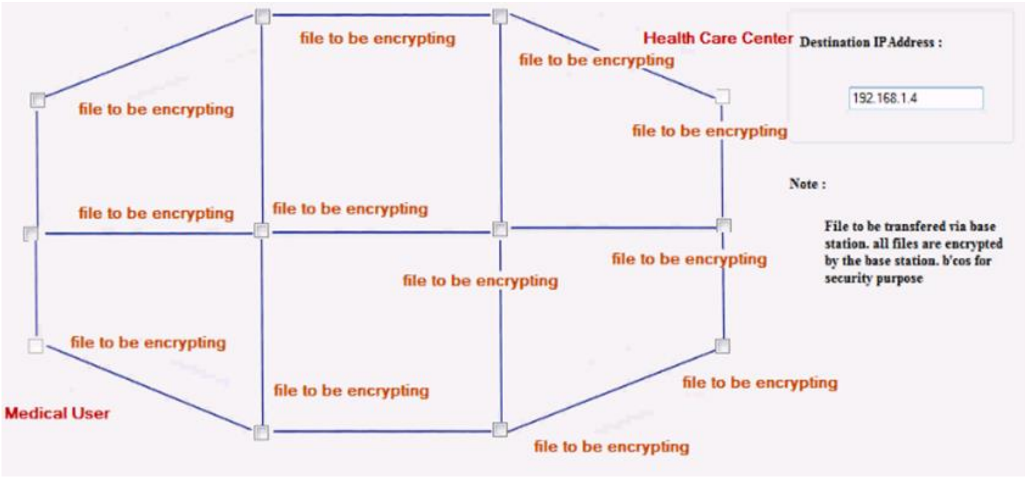
The ESPOC is implemented in PHP 5.0 using mysql 5.0 as the database and also in order to perform data mining on the data received the tool selected and used is Weka 6.0 as it is open source and free to use and the results depicted are shown below:



Body Sensing going

Fig. 3 Body Sensing simulation

The above figure depicts the body sensing units and the below figure depicts which files to be encrypted and which are not and to be shared at the time of emergency in ESPOC system.

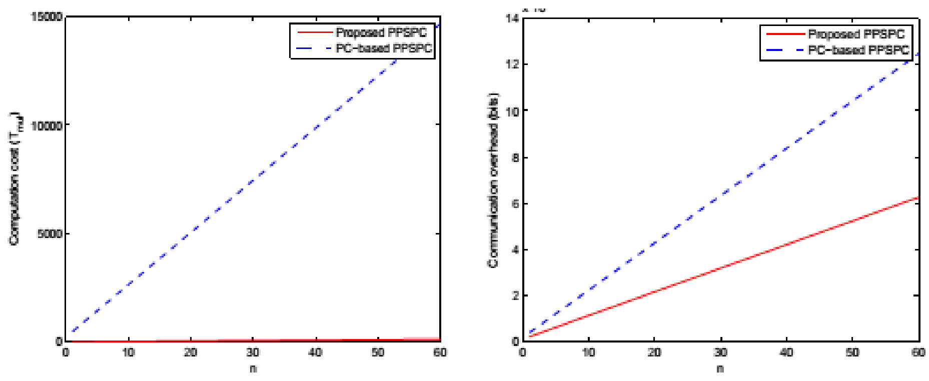


Destination IP Address : 192.168.1.4

Note :

File to be transfered via base station. all files are encrypted by the base station. b'cos for security purpose

Fig. 4 encrypting files status in ESPOC.



(a) Computation comparison (b) Communication comparison

Fig. 5 Computation and communication comparisons between the proposed ESPOC and SPOC

In the above Fig.5, we compare the average visiting locations with varying or continuously changing time intervals such as from 2 minutes to 20 minutes under different number of users and variant threshold values as per the figure when the increases the average frequency value will also increase based on the location A, the main reason for this depicted results is when all users move in the simulation area by following the same mobility model a congestion may be created due to high traffic.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a solution space for the problem space an extended secure and privacy preserving opportunistic computing (ESPOC) framework for m-Healthcare emergency which mainly exploits how to computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing using the smart-phone to achieve an efficient user-centric privacy access control through extensive performance evaluation.

In our future work we prefer to carry on smart-phone based experiments to further verify the effectiveness and optimization of the proposed ESPOC framework by concentrating more on the security issues with internal attackers who will not honestly follow the protocol.

REFERENCES

[1] A. Toninelli, R. Montanari, and A. Corradi, “Enabling secure service discovery in mobile healthcare enterprise networks,” IEEE Wireless Communications, vol. 16, pp. 24–32, 2009.

[2] W. Du and M. Atallah, “Privacy-preserving cooperative statistical analysis,” inProc. of ACSAC ’01, 2001, pp. 102–111.

[3] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, “Sage: a strong privacypreserving scheme against global eavesdropping for ehealth systems,” IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365–378, 2009.

[4] D. Boneh and M. K. Franklin, “Identity-based encryption from the weil pairing,” inProc. of CRYPTO’01, 2001, pp. 213–229.

[5] K.-H. Huang, Y.-F. Chung, C.-H. Liu, F. Lai, and T.-S. Chen, “Efficient migration for mobile computing in distributed networks,”Computer Standards & Interfaces, vol. 31, no. 1, pp. 40–47, 2009.