Secure Opportunistic Computing Privacy Preserving Group Signature Authentication Scheme for M-Healthcare Emergency

Angolo Shem Mbandu, *Member, IACSIT*, Xu Chunxiang, and Kamenyi Domenic Mutiria

***Abstract*—M-healthcare applications make use of Body Sensor Network nodes to capture health data from a patient, transfer the data via blue tooth to the patient's smartphone, which in turn transmits the information via a 3G network to remote servers at a Healthcare Center.This paper proposes a group signature authentication scheme composed of a medical users group and a medical personnel group to be used by patients and doctors respectively in the event that during an emergency the battery power of the patient under emergency runs low by using opportunistic computing approach. The group signature authentication scheme which is based on an RSA variant ensures that the privacy of the health information is controlled by the user, while a symptom matching scheme is used to control privacy. The scheme ensures user centric privacy of patient's health information. A detailed security analysis shows that the proposed scheme can withstand several kinds of attacks while at the same time achieving user centered privacy access control. In addition, extensive performance evaluations using simulations on real world maps demonstrate the efficiency and effectiveness in terms of providing high reliable PHI processing and transmission while minimizing the privacy disclosure during and m-Healthcare emergency.**

***Index Terms*—M-healthcare, authentication, group signature, opportunistic computing, matchmaking.**

I. Introduction

Group signature schemes first proposed by [1] and improved by many other researchers including [2], [3] have increasingly found wide applications in our day to day lives. In this paper, we use a group signature as an authentication scheme between members of a remote health monitoring system. In remote health monitoring systems, patients who are at home or going about their daily routines have Body Sensor Network (BSN) nodes attached to their bodies. The idea of using BSNs to carry out remote monitoring of patients can be found in a lot of literature [4], [5]. The motivation is that, collection of health information from patients can be cuff-less [6] and automated. In this approach, several BSNs which are specialized in collecting some data such as blood pressure and body temperature from a patient are attached to the patient's body. At certain desired intervals, these BSNs transmit the collected data to a second device which is then used to transmit the data to the desired destination, usually the healthcare provider at a remote location while at the same time ensuring security of this information. It then becomes clear that if the patients are mobile, the devices to be used for this transmission of collected health information are also mobile. Recently, there is more research [7], [8] on the use of smartphones to receive information from the BSNs and transmitting the health information to the healthcare provider via a 3G network. The collection of this data is at regular intervals, say every 5 minutes. However, in the case of an emergency, collection and aggregation of this data is done at much higher intervals which consumes the power of the smartphone faster. It may also happen that the power of the battery of the smartphone may run low at this critical moment. Even though the probability of this event happening is very low, i.e. 0.005, [9], when the number of emergencies increase, the number of these events will become significant, hence the justification for this work. At the occurrence of this event, opportunistic computing comes in by the use of other mobile devices in the vicinity of the medical user in an emergency to receive the Personal Health Information (PHI) from the patient and transmit to the healthcare provider. This will save the smartphone of the patient in an emergency from heavy computation s and hence extend the life of the batter power, while at the same time sending the crucial PHI. However, it is important that smartphones that participate in this scheme belong to patients with similar conditions. That is, they should have similar medical symptoms, since the software for aggregation of the PHI works best of the patients have similar symptoms. To ensure that the smartphone used to offer help in the opportunistic computing scheme has similar symptoms we shall use a privacy-preserving match making protocol proposed by [10]. It is necessary that this information is sent to enable emergency services to arrive at the scene ready with whatever assistance is immediately necessary. In this paper we want to modify the scheme by [9]. We shall do this by introducing a new group of medical personnel as participants in the model. Further, we shall use a privacy-preserving matchmaking protocol for mobile social networks to identify members of the medical users group with similar symptoms. Our model is comprised of four parties as shown in Fig. 1. First is the Membership manager. The membership manager is responsible for issuing membership keys to new members of the group. The second is the Revocation manager whose sole role is to revoke anonymity of members. The third party is the group Medical Users and the forth is the group of Medical Personnel. The Membership Manager is responsible for managing the entire M-Healthcare system. This includes setting up the system and ensuring that the BSN nodes are

Manuscript received August 25, 2014; revised December 10, 2014.

A. S. Mbandu and X. Chunxiang are with the Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, P.R.China (e-mail: asmbandu@gmail.com, chxxu@uestc.edu.cn).

D. M. Kamenyi is with the Office of the Auditor General, Kenya. He is also with University of Electronic Science and Technology of China, Chengdu, P.R.China (e-mail: dkamenyi@yahoo.co.uk).

functional. Each Medical User and Medical Personnel are equipped with smartphones installed with generic Medical User software. In addition, each Medical User is equipped with BSN nodes which collect Personal Health Information at regular intervals and send it to the healthcare center for remote monitoring of management of medications and patient behavior.

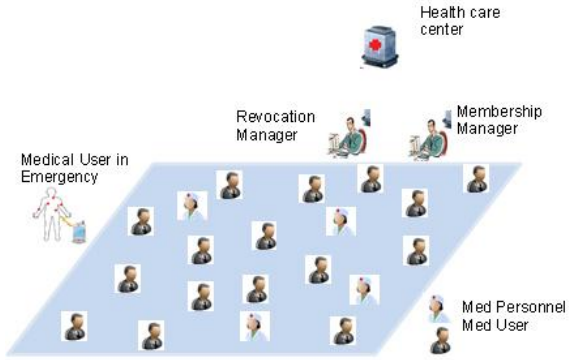

Fig. 1. Proposed model.

Body sensor nodes are dedicated devices. As such, if they are charged every day, the battery power can support the daily task of collecting raw data and transmission to the smartphone via Bluetooth and other low rate wireless personal area network (LR-WPAN) devices specified by IEEE 802.15.4 standard. On the other hand, the smartphone receives PHI data from the different BSN nodes, aggregates it and transmits it via the 3G network to the healthcare monitoring on a regular interval, say every 5 minutes. Since the smartphone is also used for other applications such as calling, messaging and browsing, the battery power may run low depending on usage. Furthermore, in case of an emergency situation, data collection, aggregation and forwarding to the healthcare facility is executed at a much shorter interval, say every 5 seconds for closer monitoring of the patient's condition. Subsequently, battery power or even memory resources may run out at this moment of need. To deal with this situation, opportunistic computing can be used. The concept of opportunistic computing is not new. In a situation where a particular node may not have enough resources to execute a task, the task can be delegated to co-operating nodes which have enough resources to carry out the task and the outcomes aggregated for further processing. In our case, in the event that the smartphone of the Medical User under an emergency goes below a certain pre-determined resource requirement threshold, other Medical Users or Medical Personnel in the vicinity of this patient may allow their smartphone resources to be used to process and transmit the PHI of the emergency case to the healthcare center. As we solve the challenge of limited resources on a Medical User's smartphone, especially in the event of an emergency, we are left with the challenge of ensuring the privacy of the PHI of the Medical User under an emergency.

The rest of the paper is organized as follows. In Section II, we briefly describe the description of SPOC. We present the proposed scheme in Section III, followed by the security analysis in Section IV. In Section V, we present the performance evaluation of the work and finally, we draw our conclusions in Section VI.

II. Related Work

In this section, we shall review SPOC [9] and thereafter present our proposed scheme.

A. Review of SPOC

SPOC proposed an M-Healthcare scheme that uses opportunistic computing. In the SPOC scheme, the system is made up of Medical Users with similar symptoms, a Trusted Authority and a healthcare center. Since privacy of PHI is a major concern [11]-[15], SPOC employs a two-phase privacy access control mechanism. The first phase ensures that non-medical users do not participate in the scheme. In the second phase, only users with symptoms below a certain threshold of similarity, is allowed to help. However, this paper suffers some shortcomings in a number of ways. The first one is that one key is generated and used for the whole day. This exposes the risk of a two time pad attack and replay attacks on the scheme. Also, only medical users participate in the scheme limiting opportunistic computing resources to only transmission of PHI to the remote healthcare center. To improve this scheme, we have made modifications to key management and introduced a new group of Medical Personnel who may also participate in the opportunistic computing model making the system more reliable.

B. Our Contribution

Our work was motivated by the need to improve [9]. Towards this end, we proposed a two-step access control approach to ensure privacy. In particular, we summarize our contributions as follows:-

1) First, we use a group signature scheme [16] to authenticate members of the two groups, namely; Medical Personnel and Medical Users. The user centric privacy access control scheme employed by [9] uses bilinear maps that are computationally expensive. Further, in the event that the identity of the Qualified Helper is needed, it is not possible to know who participated in the help. Moreover, we observe that by increasing the participants of the scheme to include medical personnel, we increase the availability of the help to a Medical User in an emergency situation.
2) Second, we use a matchmaking scheme [10] to select Medical Users with common symptoms to act as helpers.
3) Finally, we give a detailed analysis of the security of the proposed protocol.

III. Proposed Model

A. System Model

The model will only allow two groups of people to participate in the scheme, the Medical Users and the Medical Personnel. When the power resources of a Medical User in an emergency fall below the set threshold then, his smartphone will send a help request to two groups of people, the Medical Personnel and the Medical Users. The message will be signed and as such will only be accessible to the members of the above two groups. If successful contact is made with members of both groups, the Medical User will give preference to the response from the Medical Personnel for further communications. Otherwise, the Medical User will, through a process detailed later, identify a qualified helper,

who will then receive the PHI of the patient under emergency, aggregate it, and forward it to the healthcare center. Our research will not focus on the nature of computations required on the PHI of the user in an emergency, but rather, on the privacy of the PHI. It is obvious that if the Medical User makes contact with a Medical Personnel at the time of emergency, there will be no need to control privacy.

If however, all attempts to contact any of the above group members fail, the Medical User under emergency will send a medical-emergency-call message in plain text to some members listed on the phone book of the smartphone in use as shown in Algorithm 1 and Fig. 2.

Algorithm 1 Emergency Occurrence

```
while Smartphone Battery Power < Threshold Power do
    if Medical Personnel is Present then
        Send raw-PHI;
    else if Medical User is Present then
        if Similar Symptoms ≥ Threshold Symptoms then
            Send encryptedPHI;
        else
            Send Text Message in PlainText;
        end if
    end if
end while
```

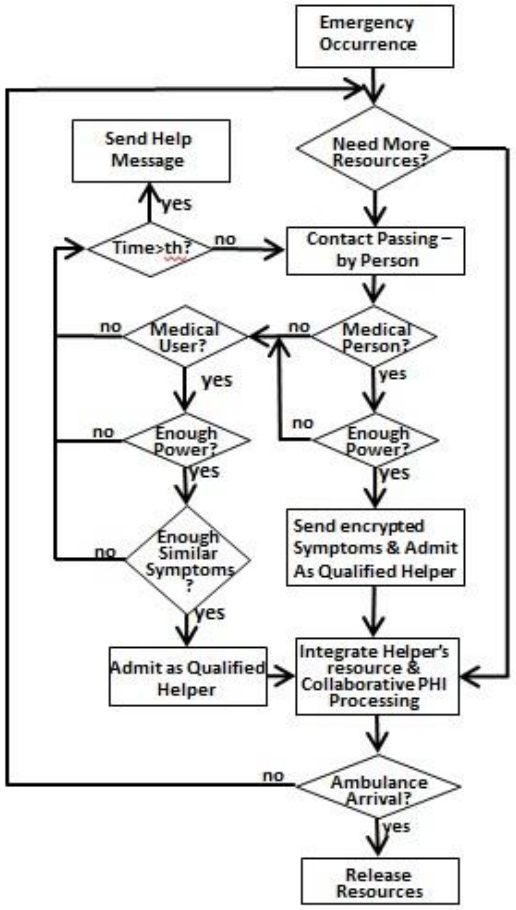

Fig. 2. Emergency response model.

B. Security Model

Opportunistic computing can effectively improve the reliability and availability of remote health monitoring systems especially during emergency cases. Our security model follow that of [9]. During the occurrence of an emergency and there is need for opportunistic computing, the security of the PHI of the medical user in an emergency remains a priority. Since, while transmitting this information there exists a significant risk of privacy violation, our scheme employs a two-stage access control.

Access Control I: During this step, even though a medical user in an emergency may have other smartphone users with enough power nearby, they may not be allowed to participate in the help because, these smartphones may not be having the necessary software to process the medical information to be transmitted. Hence, only registered smartphones may participate in the help. The registered smartphones could be of other medical users or medical personnel. If a Medical Personnel is contacted at this step, help will be rendered immediately, otherwise, the scheme will proceed to Step II Access Control.

Access Control II: This step allows registered smartphones who have similar symptoms as the emergency case to participate. The number of similar symptoms to be used (th) can be varied depending on the privacy level desired. The idea here is that, using similar symptoms minimizes privacy violations and the smartphones of medical users with similar symptoms have the same kind of software for the same kind of PHI.

C. Threat Model

In this section, we describe our threat model. We assume that the users are semi-honest. Semi-honest parties are those that follow the prescribed protocol but to glean more information than allowed from the protocol transcript[16]. Hence our Medical Users will be curious to about learning more information about the PHI of fellow Medical Users than the protocol allows. As such, they may want to get PHI information about Medical Users by launching replay and timing attacks to the protocol. However, they should not be successful even though they can have access to the encrypted PHI from Medical Users.

D. Design Goal

To design an efficient and reliable opportunistic computing scheme capable of processing and transmitting the PHI of a Medical User in an emergency situation while preserving the privacy of the PHI.

E. Description of the Proposed Scheme

System Initialization: The membership manager will be responsible for the initializing the system and he will choose a secure symmetric key algorithm $E()$ such as AES and a collision resistant hash function $H: \{0,1\}^* \rightarrow Z_p^*$. Further, he will choose a random number $a \in Z_p^*$ and compute $b = H(a)$. He will publish $(H, E())$. For a user $MU_i, sk_i = H(MU_i||b)$. User MU_i will then compute $k_i = (sk_i||Cdate)$ and send this to the Body Sensor Nodes (BSNs) as the shared key to be used to communication of $raw - PHI$ between the two entities. After every set interval, the BSN collects $raw - PHI$ and sends to the smartphone the following encryption; $E(k_i, raw - PHI||timestamp)$. Upon receiving this message from the BSN, MU_i accepts $raw - PHI$ from $E(k_i, raw - PHI||timestamp)$ only after confirming the validity of the timestamp. The medical user MU_i then processes the $raw - PHI$ and uses the 3G technology to report the processes PHI to the membership manager in the form of $(MU_i||timestamp||k_i, raw -$

$PHI||timestamp$). When the membership manager receives the message, it will carry out an authenticated integrity check. Regardless of whether the results of the integrity check are positive or negative, it will proceed and use its key b to compute sk_i and further compute k_i. It will decrypt the message and confirm that the two timestamps are same and valid. At this point, if the timestamp was not valid, the membership manager will drop the communication without giving reason to the sender. If the received message is valid, the membership manager will send the resultant PHI to the healthcare center.

Communication Key Setup: There shall be two groups managed by a trusted authority. The purpose of introducing the group is to use a group signature scheme for group member authentication. All medical users and some medical personnel will help to transmit the medical users PHI to the healthcare center. We envisage that medical users are willing to help fellow medial users while it is assumed that doctors likewise will be willing to help medical users in the event of an emergency. Subsequently,, parties involved in the scheme shall be the membership manager, the revocation manager, the Medical user and the medical personnel. One group will have its members as the Medical users and the second group will have its members as the Medical personnel. While setting the Medical users group, the membership manager shall choose a group $G =< g >$ and two random elements, $z_{mu}$and $h_{mu} \in G$ with the same large order. The revocation manager chooses hi secret key x_{mu} and publishes $y_{mu} = g^{x_{mu}} = GTK_{mu}$. The tuple $(z_{mu}, h_{mu}, g) = GPK_{mu}$ is the group public key of the Medical Users. Finally a hash function, $H: \{0,1\}^* \rightarrow \{0,1\}^k$ and security parameters, $\hat{I}, l_1, l_2$and $\in$ are set. To become a group member, a Medical User chooses a random prime $e \in_R \{2^{l_1}, \dots, 2^{l_1} + 2^{l_2} - 1\}$ and $\in_R \{\{2^{\hat{I}_1}, \dots, 2^{\hat{I}_1} + 2^{\hat{I}_2} - 1\}$ such that $e \neq 1(mod\ 8)$[16] and $\neq e(mod\ 8)$, computes $= e$ and $\check{z} = z$ commits to and ž and sends , ž and their commitments to the membership manager. The prospective member has to prove to the membership manager that and ž were chosen correctly. The membership manager computes $u = \check{z}^{1/}$ and sends u to the new member, who checks that $\check{z} = z$ holds. The membership manager stores $(u, \check{z},)$together with the identity of the new member and the commitments to and ž in the group member list. The new member stores $(u, e) = GSK_{i_{mu}}$ as the membership signing key. The same procedure will be followed to generate corresponding keys for the members of the Medical Personnel. Upon completion of the initialization phase, MU_i shall have the following tuple $(GPK_{mu}, GPK_{mp}, GSK_{i_{mu}})$. Likewise, MP_j shall have the following tuple, $(GPK_{mu}, GPK_{mp}, GSK_{j_{mp}})$. A user can authenticate his membership to any other member of wither of the two groups as follows during an emergency situation.

F. Implementation

Access Control-I: This is implemented using the group signature scheme already described. When an emergency happens, and the smartphone of the Medical User runs low on power, the opportunistic computing mechanism will set in as described in Fig. 2 and Algorithm1. The objective of this phase is for the MU_i to make contact with either MP_j or a fellow Medical User MU_j whom we shall refer as Help Contact (HC) in the vicinity of the emergency and establish a session key sk to used by the two parties. MU_iwill choose a random number $x_{mu_i} \in_R G$ and compute $g^{x_{mu_i}}$. He will send out this within its transmission range. If a HC receives this message, he may choose a random number $x_{HC} \in_R G$ and compute $g^{x_{HC}}$. HCwill then send back toMU_i the signature $\sigma_{GSK_{HC}}$. The signature is created as follows:

HC chooses an integer $\omega \in_R \{0,1\}^{l_g}$, computes $a = g^{\omega}, b = uy^{\omega}$ and d a commitment to e.

HC chooses $r_1 \in_R \{0,1\}^{\in(l_2+k)}, r_2 \in_R \{0,1\}^{\in(l_2+l_1+k)}$ and $r_3 \in_R \{0,1\}^{\in(l_g+k)}$and computes equations 1,2 and 3 below.

$$t_1 = b^{r_1}(1/y)^{r_2}, t_2 = a^{r_1}(1/g)^{r_2}, t_3 = g^{r_3}, t_4 = g^{r_1}h^{r_3} \quad (1)$$

$$c = H(g||h||y||z||a||b||d||t_1|||t_2|||t_3|||t_4||g^{x_{mu_i}}||g^{x_{HC}}) \quad (2)$$

$$s_1 = r_1 - c(e - 2^{l_1})(inZ),\ s_2 = r_2 - ce\omega(inZ),$$

$$s_3 = r_3 - ce\omega(inZ) \quad (3)$$

The signature $\sigma_{GSK_{HC}}$ is $(c, s_1,\ s_2, s_3, a, b, d)$. HC will send this signature to MU_i . MU_iwill verify this signature. To ascertain whether HC is a fellow Medical User or a Medical Personnel, MU_i will first use GPK_{mp} to check whether the *Definition 1* holds. If it does not hold, MU_iwill use GPK_{mu}. At this point, the MU_i will be able to know whether HC is a Medical User or a Medical Personnel.

Definition 1: Let $\varepsilon, l_1$and $l_2$be security parameters such that $\varepsilon < l, l_2 < l_1 < l_g$ *and* $l_2 < \frac{l_g - 2}{\varepsilon} - k$ holds. A group signature $\sigma = sign((g, h, y, z), m)$ of a message $g^{x_{mu_i}}||g^{x_{HC}} \in \{0,1\}^*$ is a matrix $(c, s_1,\ s_2, s_3, a, b, d) \in \{0,1\}^k \times \{-2^{l_2+K}, \dots, 2^{l_2+k}\} \times \{-2^{l_g+l_1+k}, \dots, 2^{l_g+l_1+k}\} \times \{-2^{l_g+k}, \dots, 2^{l_g+k}\} \times G$ satisfying equation 4.

$$c = H(g||h||y||z||a||b||d||z^c b^{s_1 - c_2^{l_1}}/y^{s_2}||a^{s_1 - c_2^{l_1}}/ g^{s_2}||a^c g^{s_3}||d^c g^{s_1 - c_2^{l_1}}||g^{x_{HC}}||g^{x_{mu_i}}) \quad (4)$$

If the signature is found to be valid, MU_i will compute the session-key $sk = (g^{x_{HC}})^{x_{mu_i}}$. If after a certain pre-defined time MU_i does not get favorable response from any of the group members, it will activate a plaintext message to some designated persons on its phonebook requesting for help.

If the group signature message was received by a Medical Personnel, i.e. HC:=MP_j, MU_i will then send messages of the format $MU_i||\ E(sk, raw - PHI||timestamp)$. The Medical Personnel will check the validity of the timestamp before processing the raw-PHI. According to the processed PHI, the Medical Personnel will giveMU_i emergency help, and at the same time send the message $MP_j||MU_i||timestamp||E(sk_{mp_j}, MP_j||MU_i||timestamp||raw - PHI)$ to the healthcare center. If the group signature message was received by a fellow Medical User, i.e. $HC = MU_j$, the scheme will proceed to the *Access Control-II* as follows.

Access Control-II: Once MU_j passes the *Access Control-I*, MU_i and MU_j will proceed to *Access Control-II* to ascertain if they share the required number of similar symptoms. Suppose, the set $X = \{x_1, x_2, x_3, \dots x_m\}$ is the set of $MU_i's$symptoms and the set $Y = \{y_1, y_2, y_3, \dots y_n\}$ is the set

$MU_j's$ symptoms, this step will used the *Symptom-Match-Making-Protocol* explained next to establish the shared symptoms, $X \cap Y$.

Symptom-Match-Making-Protocol: The Access Control-II is implemented using a symptom matchmaking protocol based on [10]. Out interest at this point is to establish the symptoms that MU_i and MU_j have in common. Consider that MU_i has a symptom set $x_i \forall i \in (0.m]$, assuming MU_i has m symptoms and MU_j has a symptom set $y_i \forall i \in (0.n]$, assuming MU_j has n symptoms. Assuming that they use a session-key sk. Each of these symptoms are hashed using a collision resistant hash function such as SHA 3. The new sets of symptoms are as follows; $H(x_i) = X_i$ and similarly $(y_i) = Y_i$. Subsequently, the new set of symptoms for MU_i and MU_j become $X_i \forall i \in (0.m]$ and $Y_i \forall i \in (0.n]$ respectively. MU_ithen randomly selects a random number ra and computes $X_i^{ra} \forall i \in (0.m]$. Likewise, MU_j computes $Y_i^{rb} \forall i \in (0.n]$.

MU_i will send a message of the form $(MU_i||timestamp_1||X_1^{ra}||X_2^{ra}|| \dots ||X_m^{ra}||$.

$E(sk, H(X_1^{ra}||X_2^{ra}|| \dots ||X_m^{ra}||MU_i||timestamp_1)))$ to MU_j . MU_j will send a message of the form $(MU_j||timestamp_2||X_1^{rarb}\left||X_2^{rarb}\right|| \dots \left||X_3^{rarb}\right||$.

$Y_1^{rb}\left||Y_2^{rb}\right|| \dots ||Y_n^{rb}||E(sk, H(Y_1^{rb}||Y_2^{rb}|| \dots ||Y_m^{rb}||\ MU_i||\ timestamp_2)))$.

Finally, MU_i will send a message of the form $(MU_j||timestamp_3||Y_1^{rbra}$

$$\left||Y_2^{rbra}\right|| \dots ||Y_n^{rbra}||E(sk, H(Y_1^{rbra}||Y_2^{rbra}|| \dots$$

$$||Y_m^{rbra}||\ MU_i||timestamp_3))).$$

At the end of the above communication process, each party will learn of the number of shared symptoms $|X \bigcap Y|$. If the shared number of symptoms is greater than a certain threshold, th, i.e. $|X \bigcap Y| > th$, then $MU_j$is accepted as a Qualified Helper, QH.

Upon qualifying as a QH, MU_i may send to MU_j messages of the following format (MU_i ||*timestamp*||*E(sk, raw-PHI||timestamp))* to MU_j. MU_j will then decrypt this message, process the $raw - PHI$, and then send the resulting PHI to the healthcare center. The healthcare center upon receiving helper messages will be able to distinguish whether the helper messages are coming from the Medical Personnel or Medical Users groups by examining the prefix of the messages. To reveal the signer of a message, the revocation manager first verifies the message and aborts if the signature is not valid. Otherwise, the revocation manager computes $= b/a^x$. He then looks up in the group-member list and will find the corresponding u, the groups member's identity and the commitment to and ž .

IV. Security Analysis

A. Security of the Group Authentication Scheme

The group signature scheme used in this paper is based on the strong RSA assumption and the Diffie-Hellman Decision (DHD) assumption. An analysis of the security of this group signature scheme can be found in [16].

B. Timing and Side Channel Attacks of the Group Signature Authentication Scheme

Another attack that the adversary may attempt on the scheme is the timing attack. Our scheme is secure against this attack. The implementation of the scheme uses two ways to ensure that this king of attack is not possible either directly or as a side channel attack. An adversary may send a message it created or intercepted from another valid user to the membership manager. The membership manager will upon receiving this message, carry our several checks. It the message received fails the test at any point, the membership manager will continue with the checking without stopping to the last point, before it discards the invalid message. This ensures that the adversary watching the reaction of the membership manager will not get any information whatsoever as to the reason of the rejection of the packet. Likewise, if the adversary was listening to the power consumption of the membership manager, it will not be able to know the point at which the check failed and as such the end of the process, it will have no information whatsoever regarding the reason for the rejection. Further, the membership manager never communicates back to the sender the invalid messages.

C. Replay Attacks on the Group Signature Authentication Scheme

An adversary may want to attack the scheme by getting messages between the parties in the scheme and later re-send them at a later time. Since the scheme is designed to send messages within such close intervals, we sue timestamps to prevent replay attacks. A good time constraint can be used to determine optimal performance that can be useful to the scheme without degrading performance.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed scheme using Thomas Brinkhoff Network-based Generator of Moving Objects[17]. The distance between smartphones in the simulation area was calculated using equation 7.

$$Distance, D(i,j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \qquad (5)$$

where $i,\ j = 1,\ 2,\ 3, \dots$. The change in distance $D(i,\ j)$ between smartphones at a time t_j with respect to time t_i was calculated using equation 8.

$$Distance, D(i,\ j) = D_{ti}(i,\ j) - D_{tj}(i,\ j) \qquad (6)$$

where $D_{ti}(i,j), D_{tj}(i,j)$ are distances between two smartphones at two different times $t_i$and t_j.

While carrying out this simulation, we assume that communications between smartphones and the communications between BSNs and smartphones are always workable whey they are within each other's transmission ranges. The performance metric that we used in the evaluation is the Number of Qualified Helpers (NQH), which indicates how many qualified helpers can participate in the

opportunistic computing within a given period of time.

A. Simulation Setup

In the simulations, a total of l users $\mathcal{U} = \{U_1, U_2, \ldots, U_{l-1}\}$ are generated using the road network of San Francisco Bay provided by the simulator. Each user U_i is equipped with personal BSNs and a smartphone with a transmission radius of 20 metres. The users independently move along the road with a velocity $v \in [0.5,1.2]$ m/s. We assume that the symptom character space $n = 16$. Each user is randomly assigned 8 symptom characters. Let the emergency of user U_0take place at time t_0, he sets the threshold th as $\{3,5\}$ and waits for the qualified helpers before the ambulance arrives in say 20 minutes. In the simulation, we assume that all users will stop when they meet $U_0's$ emergency, and only the qualified helpers will participate in the opportunistic computing. We consider that $U_0's$ emergency takes place at three different locations, A, B and C to examine how the factors l and th affect the NQH at different locations. We run simulations with the different parameter settings. For each setting, the simulation lasts for 20 minutes and the average performance results are reported.

B. Simulation Results

In Fig. 3, we compare the average NQHs at locations A, B and C varying with time from 2 to 20 minutes under different user number l and the threshold th.

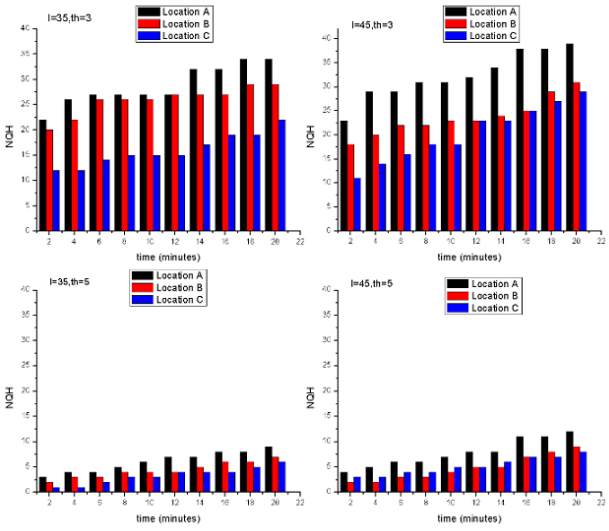

Fig. 3. NQH varying with time under differ l and th.

From Fig. 3, we can see that with the increase of time, the average NQH will also increase. We can see that different locations tend to have different results. For example, location A seem to show good response in the given time period. This is because, by following a natural mobility model as the one used, places with higher traffic register higher user arrival rates compared to places with lower traffic. However, regardless of the amount of traffic, locations register an increase in the arrival of NQHs over a given time period. By further observing the differences of the average NQH under $th = 3$ and $th = 5$, we can see that the average NQH under th=5 is much lower than that under $th = 3$, which indicates that the larger the th the less the NQHs and the less the privacy disclosure and vice versa.

In Fig. 4, we show a performance comparison between our scheme and SPOC. In this comparison, we selected location B, being one of the points at which the simulation was carried out. The two performances seem to show a common trend in the arrival of QH at the scene of the emergency.

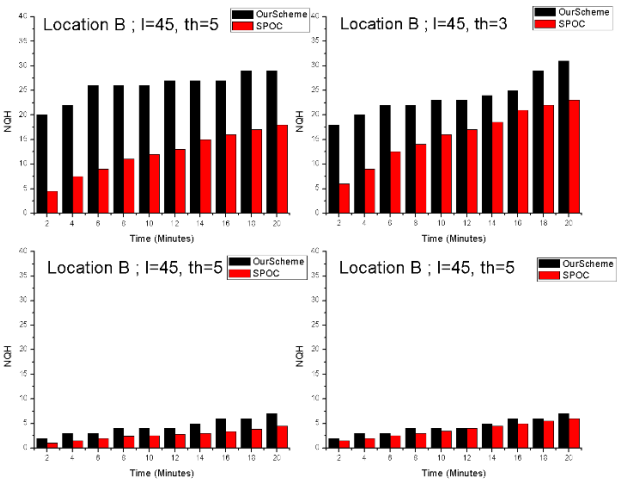

Fig. 4. Performance comparison between our scheme and SPOC at location B.

The trend shows that, when an emergency occurs, the NQH arrival steadily increases with time. We however see that our scheme registers high arrival NQH compared with that of SPOC at almost all levels. This could be attributed to the fact that our scheme using a less resource intensive group signature scheme for authentication results in better performance as opposed to SPOC.

VI. Conclusions

This paper proposes a scheme that can use a group signature algorithm for authentication between members participating in a remote medical health monitoring system. The need for privacy of *PHI* between users is the motivation for this paper. To achieve this objective, we proposed a two level access control scheme based a group signature scheme and a matchmaking scheme both of which are very efficient in implementation. A detailed security analysis shows that our scheme achieves efficient user-centric privacy disclosure control. Further, our performance evaluation, which we performed on a real world map of San Francisco Bay indicated that our proposed scheme preserves privacy as controlled by the user using the parameters of th and l. Comparing the performance of our scheme and SPOC, our scheme performs better. For future work, we intend to implement this scheme on a reputation based medical services scheme.

References

[1] D. Chaum and E. V. Heyst, "Group signatures," in *Proc. Advances in Cryptology—EUROCRYPT'91*, 1991, pp. 257-265.

[2] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in *Proc. Advances in Cryptology—Eurocrypt 2003*, Springer, 2003, pp. 614-629.

[3] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," in *Proc. Topics in Cryptology–CT-RSA 2005*, ed., Springer, 2005, pp. 136-153.

[4] B. P. Lo, S. Thiemjarus, R. King, and G.-Z. Yang, *Body Sensor Network–A Wireless Sensor Platform for Pervasive Healthcare Monitoring*, 2005.
[5] R. Jafari, R. Bajcsy, S. Glaser, B. Gnade, M. Sgroi, and S. Sastry, "Platform design for health-care monitoring applications," in *Proc. HCMDSS-MDPnP. Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability.*, 2007, pp. 88-94.
[6] C. C. Poon, Y. M. Wong, and Y.-T. Zhang, "M-health: The development of cuff-less and wearable blood pressure meters for use in body sensor networks," in *Proc. Life Science Systems and Applications Workshop, IEEE/NLM*, 2006, pp. 1-2.
[7] A. Bourouis, M. Feham, and A. Bouchachia, "Ubiquitous mobile health monitoring system for elderly (UMHMSE)," 2011.
[8] M. Milošević, M. T. Shrove, and E. Jovanov, "Applications of smartphones for ubiquitous health monitoring and wellbeing management," *JITA-Journal of Information Technology and Applications (Banja Luka)-APEIRON*, vol. 1, 2011.
[9] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, pp. 614-624, 2013.
[10] Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in *Proc. 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST)*, 2011, pp. 252-259.
[11] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys (CSUR)*, vol. 45, p. 3, 2012.
[12] J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," *Wireless Communications, IEEE*, vol. 20, 2013.
[13] X. Huang, Y. Jiang, Z. Liu, T. Kanter, and T. Zhang, "Privacy for mHealth presence," *International Journal of Next-Generation Networks (IJNGN)*, vol. 2, pp. 33-44, 2010.
[14] A. M. Helm and D. Georgatos, "Privacy and mhealth: How mobile health "apps" fit into a privacy framework not limited to HIPAA," *Syracuse L. Rev.*, vol. 64, pp. 131-197, 2014.
[15] S. Mare, J. Sorber, M. Shin, C. Cornelius, and D. Kotz, "Adapt-lite: Privacy-aware, secure, and efficient mhealth sensing," in *Proc. the 10th annual ACM Workshop on Privacy in the Electronic Society*, 2011, pp. 137-142.
[16] J. Camenisch and M. Michels, "A group signature scheme with improved efficiency," in *Proc. Advances in Cryptology—ASIACRYPT'98*, 1998, pp. 160-174.
[17] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, pp. 153-180, 2002.

Angolo Shem Mbandu received his bed technology degree from Moi University, Eldoret, Kenya in 1997. He received his MSc information systems degree from University of Nairobi, Nairobi, Kenya in 2009. Currently, he is a PhD candidate in the Department of Computer Science and Engineering at the University of Electronic Science and Technology of China, Chengdu, PRC. He is also a member of IACSIT (membership No. 80337496). His research interests are information security and cryptography its applications.

Chunxiang Xu received her B.Sc., M.Sc. and Ph.D. degrees at Xidian University, in 1985, 1988 and 2004 respectively, P. R. China. She is presently engaged in information security, cloud computing security and cryptography as a professor at University of Electronic Science Technology of China (UESTC).

Kamenyi Domenic Mutiria was born in Kenya on Sep. 4, 1972. He attained a BSc degree in statistical math's and computing of Kenyatta University, Kenya in October 1996; in March 2005, graduated with Msc (information systems) of University of Nairobi, Kenya; and in June, 2014, graduated with PhD degree in computer science and technology of University of Electronic Science and Technology of China (UESTC), Peoples Republic of China.

From July 1997 to date, he has been working in Nairobi Kenya with the Office of the Auditor-General as an assistant manager in charge of ICT Audit. He has four years part-time teaching experience in IT with Kenya Methodist University. Previously, he worked with Teachers Service Commission of Kenya and Group 4 Security, Kenya. He published many papers and attend conferences, such as "Authenticated privacy preserving for continuous query in location based services" in *Journal of Computational Information Systems* by Kamenyi D. M., Yong Wang, Fengli Zhang, Imran Memon and Y. H. Gustav. His current research interest are network security and privacy, location based services privacy, cloud based systems, reputation systems, security protocols.

Dr. Kamenyi is a Certified Information Systems Auditor, CISA in 2008. He also holders of Cisco Certified Network Associates, CCNA and Cisco Certified Network Professional, CCNP Certificates.