Remote Medical Monitoring System in Wireless Sensor Networks

https://doi.org/10.3991/ijoe.v12i11.6239

Zhang Chao
Bozhou University, Anhui, China

***Abstract*—In order to solve the problem of monitoring remote medical care to identify good medical services, a medical service recommendation system based on privacy-preserved reputation scoring is designed. This system enables medical service users to get a reputation score of a Medical Service Provider before engaging in any services. The experiment results show that the proposed scheme is significantly more efficient in batch verification of digital signatures, making it a suitable practical solution to Mobile Health Care applications, while the third solution shows that the system is able to provide reputation scores as well as recommendation while preserving privacy as desired.**

***Index Terms*—remote medical, monitoring system, wireless sensor networks**

I. INTRODUCTION

Advancements in standards of living as well as better medical services have contributed to an increase of the aged population. The net effect is an increase in the number of people seeking medical attention and as such more strain on the medical services available. A novel use of smartphones can help to mitigate this situation.

Smartphones have the ability to receive and transmit data in an automatic manner by the use of apps and other ways and communicating this data with servers in remote locations over the 3G networks. This coupled with data collection devices such as Body Sensor Network (BSN) nodes maybe used to collect health information from patients and transmit this information to medical facilities which maybe some considerable distance from the location of the patients. Moreover, this kind of communication may be secured by using appropriate cryptographic schemes. This new way of collecting Patient Health Information (PHI) in an automated manner is most suitable for patients who are outdoors going about their day to day activities while at the same time require close monitoring of their health conditions.

Similarly, as more and more smartphone apps are used in communication of sensitive information over the insecure wireless channel, a new challenge arises. This is the challenge of more and more digital signatures being generated by these mobile devices which have limited computational and battery power. Conventional digital signature schemes were designed with desktop computers in mind. These desktop computers are devices with relatively high computational resources and do not experience a limitation of power to run the systems. However, the entrance of mobile devices calls for the design of digital signature schemes which consume less power and require less computation resources. Also, the connectivity of all these devices on the Internet has resulted new opportunities that make use of the Internet on the mobile platform such as Ecommerce and other reputation based systems that users can benefit from. Reputation based systems readily find application in M-Healthcare. Medical users can find convenience when they need to identify quality Medical Service Providers (MSPs) by requesting other medical users to avail reputation scores of several MSPs and finally engage the services of the best MSP.

The Wireless Sensor Networks (WSN) have become the evolution trend and hot research spot in sensor and control field. Great attention has been paid by the military, industry and academe field all over the world. Many researchers gave abundant findings about wireless sensor from both fundamental theory and application. At the same time, WSN is being widely applied in many fields like military, industry, agriculture, environment monitoring, smart traffic, smart home etc. Among these wireless sensor networks application systems, the resource of low-cost wireless sensor node is constrained, i.e., capacity of computing, storage, wireless communication distance and energy is very limited, and also the wireless sensor nodes are easily affected by noise, interference and surrounding environment. So during the wireless transmission, the sensor data missing often occurs, and this phenomena is worse in some special environments. This problem has become a big challenge for data processing methods. And the sensor data estimation is effective way to solve this problem. Also it is a powerful tool to support data inquiry, data aggregating, energy-saving transmission and early warning mechanism.

For the estimation of missing sensor data in wireless sensor networks, many researchers home and abroad have been doing a lot of research works and getting certain research results. But there still exist some important problems needed to be resolved. For example, the characteristics of the sensor data are not fully investigated and made use to estimate the sensor data, which lead to high computing complexity; The estimation accuracy is very low with high complexity; The estimation problem of the uncertain sensor data in a local field is not considered; The dynamic data module of sensor data stream is not fully considered.

In such cases, a collection of mobile ad-hoc with wireless network interfaces could form a momentary network without the assistance of any established network infrastructure or centralized administration. The mobile ad-hoc network (MANET) group which is formed within Internet Engineering Task Force (IETF) is mainly focusing on to develop evolving M.ANET specifications and introduces them to the track of an Internet standard. Their goal is to support mobile ad-hoc networks. The goal is to support mobile ad-hoc networks by hundreds of ad-hoc routers and solve a challenge that facing this kind of network.

II. OVERVIEW

A lot of research in M-Health is currently uncoordinated. However, recently, some of the M-Health research has been centered on answering some of the following questions

1. How do we deal with a situation where power on a mobile device run low during an emergency situation on a patient? Collection and transmission of PHI runs continuously as the patient goes about their day to day daily activities, with PHI collection and transmission taking place say every 5 minutes. However, when a life threatening condition happens, the frequency of collecting and aggregating this information increases. What happens if the information transmitting device runs out of battery power during this crucial time?

Application: Smartphone resources such as computing power and data transmission can be gathered opportunistically. In particular, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for delegation of computing tasks. Thus, when the residual power of smartphone of a patient runs low during a medical emergency, other smartphones in close proximity may be used to process the PHI and transmit it to the remote healthcare center.

2. The proliferation of mobile devices connected on the Internet has suddenly increased the number of data sources. With the increase of these data sources, how do we optimize on the digital signature signing and verification process?

A lot of research has gone into designing short, resource efficient digital signatures and their batch verification scheme versions[1-2]. Also, a lot of research has gone towards implementation of cryptographic schemes on groups structures such as elliptic curve schemes as well as lattices. Elliptic curve cryptography has helped implement lighter cryptosystems, making it appealing to mobile devices.

Application: Efficient cryptosystems on computing resources and battery power are very readily applicable to mobile devices. With the number of mobile devices ever increasing, soon the number of mobile devices connected to the Internet maybe more than that of Personal Computers. This offers the motivation to design digital signatures that are fast and efficient while not compromising on security.

3. How do we get to identify the best medical services available in a particular locality? Is it enough to just look at the yellow pages and pick out the best medical service provider for a specific medical condition? Are there ways in which we can determine the most reputable medical service provider?

Application: Since cases of medical negligence cause a lot of concern to patients, it is important that patients get medical services from reputable medical service providers. A medical service provider with a good reputation will most likely be the one with the best services and least cases of unethical medical behavior or negligence. Likewise, a scheme that provides patients with a way to determine the best medical service provider is most welcome.

According to [3]， recent trends in healthcare, focusing on accessing patients data anytime and anywhere, encourage moving the healthcare towards the cloud. Despite the fact that the cloud offers many benefits, it also presents threats to the data in terms of privacy and security. The concept of privacy preservation is more than just ensuring confidentiality. [4] argues that the threats to the data in the cloud include spoofing identity, repudiation, tampering and information disclosure. In spoofing attack, the attacker pretends to be a valid user whereas tempering involves unauthorized alterations and modifications of the data. Repudiations are concerned with users who deny responsibility of performing after performing an activity related to the data. Information disclosure on the other hand is the exposure of information to the entities having no right to access information. Ideally, the cloud service providers should completely recognize and deal with security concerns in the cloud to enhance trust level of the patients as well as healthcare organizations that hire these services. In the United States of America for example, use and disclosure of Protected Health Information should be in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA requires the maintaining of confidentiality of health data is not an option, but rather an obligation.

M-Healthcare can only flourish with the development of electronic health records managed by healthcare providers. This has resulted in a new way of managing health records known as e-Health, which necessitated the restructuring and digitization of healthcare infrastructure. The new paradigm shift for provision of ubiquitous health services that are affordable has been adopted in countries such as USA, Canada, Korea [5] and European Union. Indeed, many healthcare providers today use one form of electronic medical record system or the other. On the other hand, a patient may have several healthcare service providers such as primary care physicians, specialists and therapists. In addition, a patient may purchase insurance policies from several health insurance companies. The requirement for storage and continuous availability of electronic health data has necessitated the emergence of cloud computing services [6-8]. Cloud computing can shift the computing resources to third-party service providers. These third-party service providers are responsible for the management of hardware and software resources eventually leading to cost reductions [9-11].

As more and more healthcare organizations migrate their data to the cloud, it still remains apparent that security challenges still abound that will take a long time to despite a lot of research that is ongoing in the area of cloud computing. [9] posits that it is necessary to understand cloud computing vulnerabilities even as organizations rush in to embrace the technology in bid to exploit the many benefits that it is claimed to offer. Some of the vulnerabilities of cloud computing such as unauthorized access to management interface, Internet protocol vulnerabilities, data recovery vulnerability and billing evasion are real challenges the research should endeavor to solve in order to make cloud computing more robust as the technology of the future of data healthcare and data management.

III. METHOD AND ALGORITHM

Personal health data collection especially in an automated manner can greatly improve the quality of healthcare services for patients in a way that will not hinder them from going about their day to day activities. The greatest benefit is the freedom from confinement at hospitals, hospices, home cares and assisted living homes etc. since it will be possible to monitor their health status on the fly. This ensures that the patients are productive thus contributing to the economy. Moreover, during an emergency such as that due to cardiac-diseases, much may be done to stop a heart attack, or even resuscitate a patient from sudden cardiac death. For example, the first 60 minutes (the golden hour) are the most critical regarding the long-term patient of a cardiac arrest.

With continuous remote monitoring of patients there may be enough information available for pre-hospital treatment making it very timely and effective at handling such emergency cases emergency cases. Moreover, continuous data collection and a method of signaling to the patient an impending heart attack can be very beneficial to the patient. In addition, the benefits of pre-hospital-transmitted ECG (electrocardiogram) a reduction of hospital delays, better triage, continuous monitoring, ECG data accessibility for comparison, computer-aided analysis and decision making can be beneficial to the patient. The preceding discussion is a clear evidence of the benefits of M-Healthcare. According to [9]， a lot of research has been conducted in the area of M-Health data generation and transmission. However, most of the work cited does not make mention of the security of the health data collected and transmitted. In an attempt to solve the problem of privacy of M-Health data, SPOC proposed an M-Healthcare that not only ensures an end to end security scheme, but also one that attempts to solve the problem of low power using opportunistic computing. In the SPOC scheme, the system is made up of Medical Users, a Trusted Authority and a healthcare center. Since privacy of PHI is a major concern, 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 are allowed to help.

SPOC is an opportunistic computing framework for m-Healthcare emergency. The framework is made up of medical users, a trusted authority TA and a healthcare center. The TA is a trustable and powerful entity located at the healthcare center and is responsible for the management of the whole m-Healthcare system. Each medical user is equipped with personal BSN and a smartphone, which can periodically collect PHI and report them to the healthcare facility. In order to guarantee high reliability of BSN and smartphone, the batteries of smartphone and BSN should be charged every day; BSN can deal with not only the normal situations but also the emergency cases in m-Healthcare. However, since the smartphone could be used for other purposes such as receiving or making calls, browsing when an emergency occurs, the residual power of the smartphone maybe insufficient. To address this scenario, SPOC presents a two phase access control system for their opportunistic computing framework. The first access control phase ensures that the medical user under emergency makes contact only with fellow medical users.

To achieve this, they propose the use bilinear pairings to get in touch with other medical users in case opportunistic computing services are required. The second access control mechanism identifies helpers with a certain level of similarities of symptoms between the medical user and the helper. This level of similarities is set by the user, thus making the user have control of privacy desired. To compute the level of similarities, SPOC uses Privacy Preserving Scalar Product Computation which they claim is efficient.

SPOC suffers from two drawbacks. The first is that, it is vulnerable to replay attacks, between the medical user and the TA. Since medical users use that same key for 24 hours, an active adversary can intercept the first packet of the day and replay it for the next 24 hours without ever the TA realizing that they are receiving bogus information. The second drawback is that the helpers cannot be identified. In some cases, the identity of the helpers may be necessary.

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. In this approach, several BSNs which are specialized in collecting some data such as blood pressure, body temperature, breathing rate, Electrocardiogram (ECG), blood sugar level and peripheral oxygen saturation 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 on the use of smartphones to receive information from the BSNs and transmitting the health information to the healthcare provider via a 3G network as depicted in Figure 1. The collection of this data is at regular intervals, say every 5 minutes.

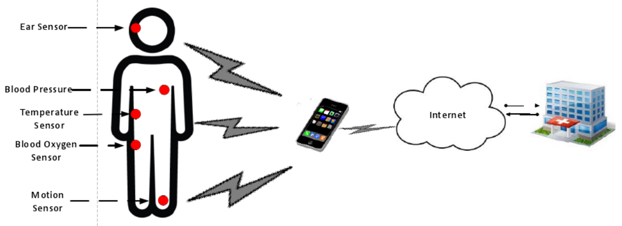

Figure 1. Magnetization as a function of applied field. Note how the caption is centered in the column

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 computations and hence extend the fife of the battery 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. The benefits of prompt pre-hospital care during medical emergencies are well documented. It is thus crucial that during an emergency, the emergency crew arrive at the scene of the emergency with information regarding the condition of the patient to enable them to offer the best possible pre-hospital first-aid. In this chapter we modify the scheme by [8-9]. We do this by using a more efficient group signature authentication scheme, 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 Figure 2. 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 fourth 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 functional. Each Medical User (MU) and Medical Personnel (MP) is equipped with smartphones installed with generic MU software.

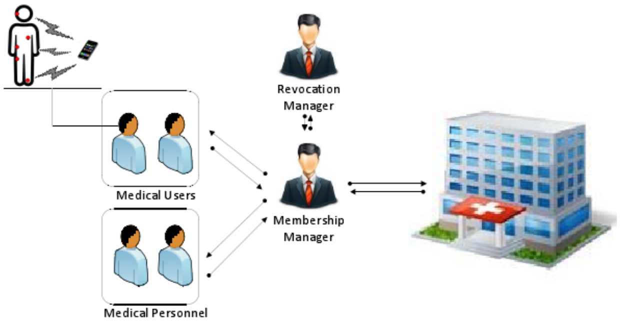

Figure 2. M-Healthcare System Model

In addition, each MU is equipped with BSN nodes which collect PHI at regular intervals and send it to the healthcare center for remote monitoring and management of medications and patient behavior. BSN 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 system on a regular interval, say every 5 minutes. Since the smartphone is also used for other applications such as calling, messaging, chatting 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 requiring even more resources.

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 MU under an emergency goes below a certain pre-determined resource requirement threshold, other MUs or MP 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 MU'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.

IV. EXPERIMENT RESULT

Opportunistic computing can effectively improve the reliability and availability of remote health monitoring systems especially during emergency cases. Our security model follows that of [10]. 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 exist a significant risk of privacy violation, our scheme employs a two-stage access control.

1) Access Control I: During this step, even though a MU 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. If however, all attempts to contact any of the above group members fail, the MU 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 and Figure 3. These particular contacts in the phone book of the MU will have been pre-selected. Hence, only registered smartphones may participate in the help. The registered smartphones could be of other MUs or MP. If a MP is contacted at this step, help will be rendered immediately; otherwise, the scheme will proceed to Step II Access Control.

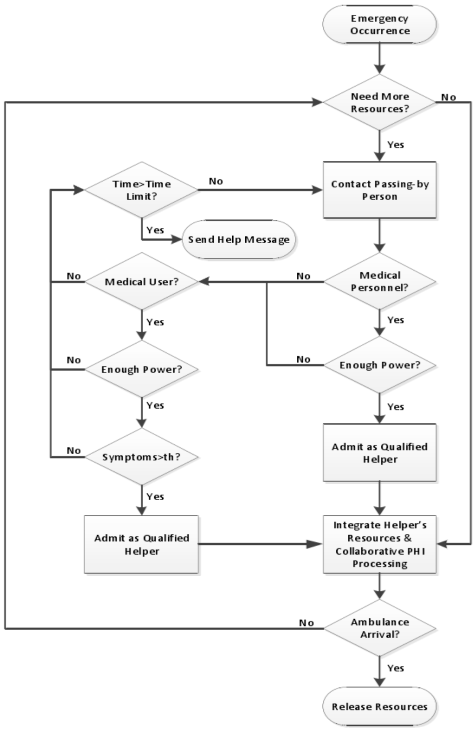

Figure 3. Emergency response model

2) Access Control II: This step allows registered smartphones who have similar symptoms as the emergency case to participate. The threshold of similar symptoms to be used can be varied depending on the privacy level desired. The idea here is that, using similar symptoms minimizes privacy violations. Also, the smartphones of MU with similar symptoms have the same kind of software for the same kind of PHI, hence making it easy to aggregate the raw PHI.

The equation of basic function is as equation (1) as follows:

$$\partial_j(C_{ijkl}\partial_k u_l + e_{kij}\partial_k\varphi) - \rho\ddot{u}_i = 0 \quad (1)$$

Under the linear relationship, basic equation is shown in equation (2):

$$\partial_j(e_{ijkl}\partial_k u_l - \eta_{kij}\partial_k\varphi) = 0 \quad (2)$$

The linear differential equation can be expressed into the following simplified forms:

$$L(\nabla,\omega)f(x,\omega) = 0,$$

$$L(\nabla,\omega) = T(\nabla) + \omega^2\rho\mathrm{J} \quad (3)$$

In which,

$$T(\nabla) = \left\| \begin{matrix} T_{ik}(\nabla) & t_i(\nabla) \\ t_k^T(\nabla) & -\tau(\nabla) \end{matrix} \right\|, \quad \mathrm{J} = \left\| \begin{matrix} \delta_{ik} & 0 \\ 0 & 0 \end{matrix} \right\|,$$

$$f(x,\omega) = \left\| \begin{matrix} u_k(x,\omega) \\ \varphi(x,\omega) \end{matrix} \right\| \quad (4)$$

$$T_{ik}(\nabla) = \partial_j C_{ijkl}\partial_l, \quad t_i(\nabla) = \partial_j e_{ijk}\partial_k,$$

$$\tau(\nabla) = \partial_i \eta_{ik}\partial_k$$

Consider an infinite situation, we have the equation (5) in the following:

$$L^0 = \left\| \begin{matrix} C^0_{ijkl} & e^0_{kij} \\ e^{0T}_{ikl} & -\eta^0_{ik} \end{matrix} \right\| \quad (5)$$

In Figure 4-7, 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.

V. DISCUSSION

The value l refers to the number of MUs while th refers to the number of shared medical symptoms. By using different values for both, we are able to investigate the performance of the proposed design under different scenarios. From Figure4-7, 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 while location C seem to register a lower response rate of MUs. 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. It is also clear that the higher the threshold values, the more the number of helpers become available. Setting a threshold that is so high will reveal a lot more information regarding a MU's PHI.

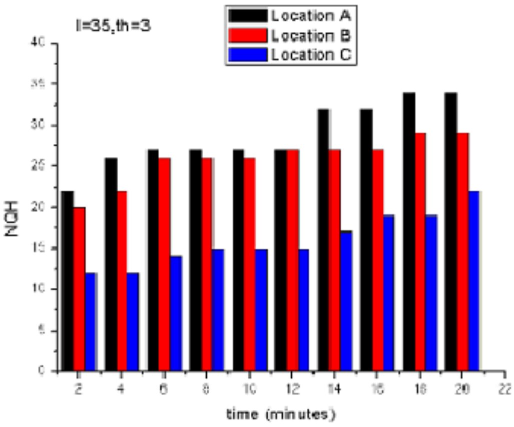

Figure 4. NQH varying with time under l=35,th=3

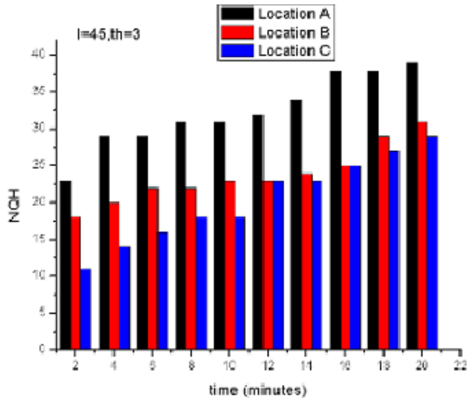

Figure 5. NQH varying with time under l=45,th=3

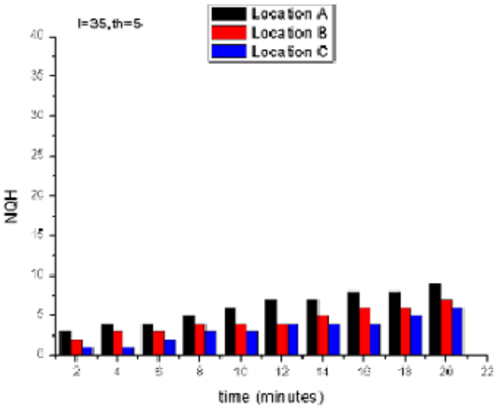

Figure 6. NQH varying with time under l=35,th=5

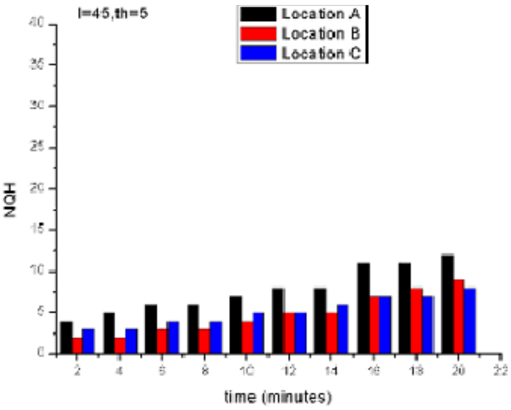

Figure 7. NQH varying with time under l=45,th=5

VI. CONCLUSION

The challenge of limited resources of mobile devices in the application to M-Healthcare, especially during the times of medical emergency has put a constraint into the use of smartphones in M-Healthcare emergencies. This chapter has addressed this challenge by using 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 of primary concern while addressing this problem. A detailed security analysis shows that our scheme achieves efficient user-centric privacy disclosure control. This system enables Medical Users to get a reputation score of a Medical Service Provider before engaging in any services. 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.

The experiment results show that our scheme is significantly more efficient in batch verification of digital signatures, making it a suitable practical solution to Mobile Health Care applications, while the third solution shows that our system is able to provide reputation scores as well as recommendation while preserving privacy as desired.

REFERENCES

[1] H. Jing, “Node deployment algorithm based on perception model of wireless sensor network,” *International Journal of Automation Technology*,vol.9, no.3, pp. 210-215, April 2015. https://doi.org/10.20965/ijat.2015.p0210

[2] H. Jing, “Routing optimization algorithm based on nodes density and energy consumption of wireless sensor network,” *Journal of Computational Information Systems*, vol. 11, no.14, pp. 5047-5054, July 2015.

[3] Y. Jiao, “Electronic Commerce Logistics Network Optimization Based on Swarm Intelligent Algorithm,” *Journal of Networks,* pp. 89-98, 2013.

[4] Y. Xu, X. Xie, and H. Zhang, “Modeling and Analysis of Electronic Commerce Protocols Using Colored Petri Nets,” *Journal of Software,* pp. 67-79, 2011.

[5] X. Zhang, et al., "Rotation-based privacy-preserving data aggregation in wireless sensor networks," *ICC 2014 - 2014 IEEE International Conference on Communications,* pp. 4184-4189, 2014.

[6] J. Zheng, et al., "Auction-based adaptive sensor activation algorithm for target tracking in wireless sensor networks," *Future Generation Computer Systems,* vol. 39, no. 1, pp.88-99, 2014. https://doi.org/10.1016/j.future.2013.12.014

[7] Chifu Huang, Yuchee Tseng, and Liuchu Lo, "The coverage problem in three-dimensional wireless sensor networks," *Journal of Interconnection Networks,* vol. 08, no. 03, pp. 3182-3186, 2015.

[8] H. Yang, et al., "Toward resilient security in wireless sensor networks," *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing ACM,* pp.34-45, 2015.

[9] Y. Hu, and X. Zhang, "Aggregation Tree Based Data Aggregation Algorithm in Wireless Sensor Networks," *International Journal of Online Engineering*, vol. 12, no 06, pp. 10-15, June 2016. https://doi.org/10.3991/ijoe.v12i06.5408

[10] J. Yang, et al., “Analysis of Camera Arrays Applicable to the Internet of Things,” *Sensors,* vol. 16, no.3,March 2016. https://doi.org/10.3390/s16030421

[11] Y. Li, et al., "Improved Compact Polarimetric SAR Quad-Pol Reconstruction Algorithm for Oil Spill Detection," *IEEE Geoscience & Remote Sensing Letters,* vol. 7, no.1, pp. 1139-1142, 2014. https://doi.org/10.1109/LGRS.2013.2288336

AUTHOR

ZHANG Chao is with the Electronic and Information Engineering Department of Bozhou University, Anhui, China (zhangchao@chinauniedu.com).

The paper is supported by Computer Application Technology Major’s Comprehensive Reform Pilot in Anhui Province of 2015(No.2015zy078), Master Studio in Anhui Province of 2014(No.2014 msgzs170), and University-enterprise Cooperation Base in Bozhou University, 2016-Software Engineering Innovation Practice Base. Submitted 09 September 2016. Published as resubmitted by the author 10 October 2016.