# A Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency

**Supriya Mishra**[1], **Sohit Shukla**[2]

*Assistant Professor Rajkiya Engineering College, Ambedkar Nagar, U.P.*[1]
*Assistant Professor B.N. College of Engineering & Technology, Lucknow, U.P.*[2]
supriya.mishra24@gmail.com[1]
Sohit009@gmail.com[2]

**Abstract- Nowadays the quality of healthcare has been improved gradually. However, the time consuming pre-hospital emergency process could sometimes cause many regrets. Therefore, the minimization of time required for providing primary care and consultation to patients is one of the crucial factors when trying to improve the healthcare delivery in emergency situations. If the Emergency Medical Technician (EMT) can hold on signs of life of patients immediately when accidents happened, higher quality of healthcare could be achieved. Mobile healthcare is a new paradigm that combines the evolution of emerging wireless communications and network technologies to connect healthcare anytime and anywhere. The purpose of the study is to develop a Mobile Emergency Healthcare Information System (MEHIS). A Standard Operation Procedure of Emergency Healthcare (SOPEH) is first planned. Then, the system is developed for EMT or families of patients to communicate with physicians in hospitals. Users can use their 3G mobile phone to transfer symptoms and information of the situation to JSP server which then quickly delivers information while providing proper emergency care at the prime time. Meanwhile, MEHIS can shorten emergency healthcare time and therefore enhance quality of emergency healthcare**.

**Keywords - Mobile-Healthcare emergency, opportunistic computing, user-centric privacy access control, PPSPC**

## 1. INTRODUCTION

In our aging society, mobile Healthcare (m-Healthcare) system has been envisioned as an important application of pervasive computing to improve health care quality and save lives, where miniaturized wearable and implantable body sensor nodes and smartphones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart disease. Specifically, in an m-Healthcare system, medical users are no longer needed to be monitored within home or hospital environments. Instead, after being equipped with smartphone and wireless body sensor network (BSN) formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. For example, as shown in Fig. 1, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by BSN, and then aggregated by smartphone via bluetooth. Finally, they are further transmitted to the remote healthcare center via 3G networks. Based on these collected PHI data, medical professionals at healthcare center can continuously monitor medical users' health conditions and as well quickly react to users' lifethreatening situations and save their lives by dispatching ambulance and medical personnel to an emergency location in a timely fashion.

Although m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the flourish of m-Healthcare system still hinges upon how we fully understand and manage the challenges facing in m-Healthcare system, especially during a medical emergency. To clearly illustrate the challenges in m-Healthcare emergency, we consider the following scenario. In general, a medical user's PHI should be reported to the healthcare centre every 5 minutes for normal remote monitoring [6]. However, when he has an emergency medical condition, for example, heart attack, his BSN becomes busy reading a variety of medical measures, such as heart rate, blood pressure, and as a result, a large amount of PHI data will be generated in a very short period of time, and they further should be reported every 10 seconds for high-intensive monitoring before ambulance and medical personnel's arrival. However, since smart phone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smart phone's energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, i.e., 0.005, for a medical emergency, when we take into 10,000 emergency cases into consideration, the average event number will reach 50, which is not negligible and explicitly indicates the reliability of m-Healthcare system is still challenging in emergency. Recently, opportunistic computing, as a new pervasive computing paradigm, has received much attention. Essentially, opportunistic computing is characterized by exploiting all available computing resources in an opportunistic environment to provide a platform for the distributed execution of a computing-intensive task. For example, once the execution of a task exceeds the energy and computing power available on a single node, other opportunistically contacted nodes can contribute to the execution of the original task by running a subset of task, so that the original task can be reliably performed . Obviously, opportunistic computing paradigm can be applied in mHealthcare emergency to resolve the challenging reliability issue in PHI process. However, PHI are personal information and very sensitive to medical users, once the raw PHI data are processed in opportunistic computing, the privacy of PHI would be disclosed. Therefore, how to balance the high reliability of PHI process while minimizing the PHI privacy disclosure during the opportunistic computing becomes a challenging issue in m-Healthcare emergency.

## 2. PROPOSED WORK

In this paper, we propose a new secure and privacy-preserving opportunistic computing framework, called SPOC, to address this challenge. With the proposed SPOC framework, each medical user in emergency can achieve the user-centric privacy access control to allow only those qualified helpers to participate in the opportunistic computing to balance the high-reliability of PHI process and minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, the main contributions of this paper are threefold. • First, we propose SPOC, a secure and privacy-preserving opportunistic computing framework for m-Healthcare emergency. With SPOC, the resources available on other opportunistically contacted medical users' smartphones can be gathered together to deal with the computingintensive PHI process in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure, SPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.

Second, to achieve user-centric privacy access control in opportunistic computing, we present an efficient attributebased access control and a novel non-homomorphic encryption based privacypreserving scalar product computation (PPSPC) protocol, where the attributed-based access control can help a medical user in emergency to identify other medical users, and PPSPC protocol can further control only those medical users who have similar symptoms to participate in the opportunistic computing while without directly revealing users' symptoms. Note that, although PPSPC protocols have been well studied in privacy-preserving data mining, yet most of them are relying on time consuming homomorphism encryption technique. To the best of our knowledge, our novel non-homomorphism encryption based PPSPC protocol is the most efficient one in terms of computational and communication overheads.

Third, to validate the effectiveness of the proposed SPOC framework in m-Healthcare emergency, we also develop a custom simulator built in Java. Extensive simulation results show that the proposed SPOC framework can help medical users to balance the high-reliability of PHI process and minimizing the PHI privacy disclosure in mHealthcare emergency.

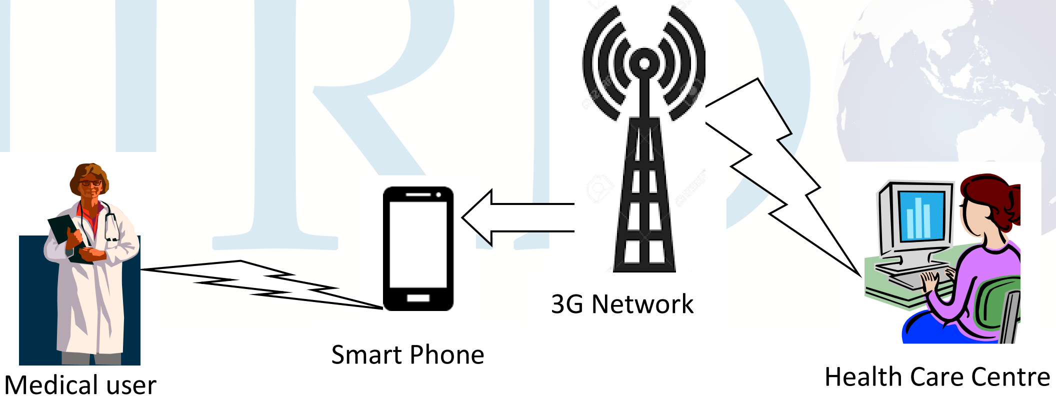
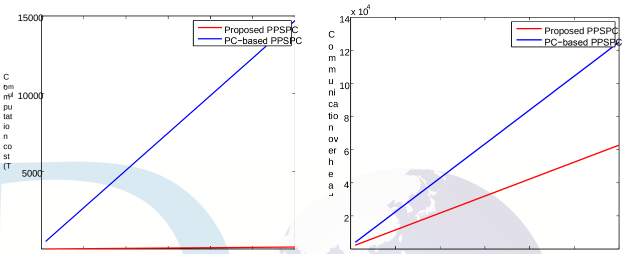


Fig.1. Pervasive health monitoring in m-Healthcare system

## 3. RELATED WORKS

Opportunistic computing: The study of opportunistic computing has gained the great interest from the research community recently, and we briefly review some of them related to our work. In, Avvenuti et al. introduce the opportunistic computing paradigm in wireless sensor network to solve the problem of storing and executing an application that exceeds the memory resources available on a single sensor node. Especially, their solution is based on the idea of partitioning the application code into a number of opportunistically cooperating modules, and each node contributes to the execution of the original application by running a subset of the application tasks and providing service to the neighboring nodes. In Passarella et al. evaluate the performance of service execution in opportunistic computing. Specifically, they first abstract resources in pervasive computing as services that are opportunistically contributed by providers and invoked by seekers. Then, they present a complete analytical model to depict the service invocation process between seekers and providers, and derive the optimal number of replicas to be spawned on encountered nodes, in order to minimize the execution time and optimize the computational and bandwidth resources used. Although these are important for understanding how the opportunistic computing paradigm work when resources available on different nodes can be opportunistically gathered together to provide richer functionality, they have not considered the potential security and privacy issues existing in the opportunistic computing paradigm . Different from the above works, our proposed SPOC framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in mHealthcare emergency. Privacy-preserving scalar product computation: Research on privacy-preservingscalar product computation (PPSPC) has been conducted for privacy-preserving data mining  and as well for secure friend discovery in mobile social networks quite recently . Initially, PPSPC protocol was designed by involving a semi-trusted party . Later, to remove the semitrusted party, many PPSPC protocols without a third party were proposed. However, they are relying on time-consuming “homomorphic encryption” and/or “add vector protocol”, and are not quite efficient2. In our proposed SPOC framework, we present a new PPSPC protocol, which does not use any “homomorphic encryption”, but is very efficient in terms of computational and communication costs, i.e., the computational cost only takes 2n multiplications (mul), and the communication cost is only (n + 1) · 1024 + 256 bits. Let Tmul, Texp denote the time needed to execute a modulus multiplication and a modulus exponentiation, respectively. When we roughly estimate Texp ≈ 240Tmul [33], we use Fig. 8 to compare the computation and communication costs of the proposed PPSPC protocol and the popular Paillier Cryptosystem (PC)-based PPSPC protocol described in Fig. 9. From Fig. 8, we can obviously observe that our proposed PPSPC protocol is much efficient, especially in computation costs. To the best of our knowledge, our proposed PPSPC is the most efficient privacy preserving scalar product computation protocol till now.



00 10 20 30 40 50 60

00 10 20 30 40 50

60 n n

(a) Computation comparison (b) Communication comparison

Fig.8. Computation and communication comparisons between the proposed PPSPC and the PC-based PPSPC varying with n

## 4. CONCLUSIONS

In this paper, we have proposed a secure and privacy preserving opportunistic computing (SPOC) framework for mHealthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed SPOC framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in mHealthcare emergency. In our future work, we intend to carry on Smartphone based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers 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] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network,” in Proc. BodyNets’10, Corfu Island, Greece, 2010.

[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, “Monitoring patients via a secure and mobile healthcare system,” IEEE Wireless Communications, vol. 17, pp. 59–65, 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, “A secure handshake scheme with symptoms-matching for mhealthcare social network,” MONET, vol. 16, no. 6, pp. 683–694, 2011.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed System, to appear.

[6] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, “Wireless body sensor network using medical implant band,” Journal of Medical Systems, vol. 31, no. 6, pp. 467–474, 2007.