IJDCST @Sep-Oct, Issue- V-2, I-8, SW-26
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Sophisticated Mobile-Healthcare Emergency Based On Opportunistic Computing Framework Incorporating Secure and Privacy Preserving Mechanism

Potteti Sandhya Rani, S. Rama Krishna,
M-tech Student Scholar, Department of Computer Science Engineering,VRS & YRN College of Engineering & Technology, Chirala;Prakasam (Dt); Andhra Pradesh, India.
Assistant Professor &H.O.D, Department of Computer Science Engineering, VRS & YRN College of Engineering &Technology, Chirala; Prakasam (Dt), Andhra Pradesh, India.

Abstract — With the pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation. In this paper, we propose a secure and privacy-preserving opportunistic computing framework, called SPOC, for m-Healthcare emergency. With SPOC, smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. In specific, to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, we introduce an efficient user-centric privacy access control in SPOC framework, which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in term of providing high reliable PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

The enhancement for this project aims to increase the security of the existing remote patient monitoring system. It is necessary to protect the user data from being mishandled by unauthorized users. In this scenario, we incorporate a novel approach of protecting the medical information captured from the patient while transferring it over the network using a secret key. The health care provider has to undergo an additional authentication mechanism in order to be able to view the remote patient's data. By implementing the above approach, we are able to transfer the data of the remote patient securely to the authorized doctors.

Index Terms— Mobile-Healthcare emergency; opportunistic computing; user-centric privacy access control; PPSPC

I. 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 [1], [2], [3], [4], [5]. 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. 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' life-threatening 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 center 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 smartphone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smartphone'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 [7], [8], [9], [10]. 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 [10]. 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 [7]. Obviously, opportunistic computing paradigm can be applied in m-Healthcare 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. In this paper, we propose a new secure and privacypreserving 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 privacydisclosure 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 privacy-preserving 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 [11], [12], [13], yet most of them are relying on time-consuming homomorphic encryption technique [14], [15]. To the best of our knowledge, our novel non-homomorphic 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 m-Healthcare emergency.[16]

In the existing remote patient monitoring system, the patient's crucial heath parameters such as BP, heartbeat, Blood sugar etc are monitored continuously by the doctor in a remote location. Various health parameters of the patient are transferred to the base station using sensors and the doctor can get a report of the patient condition from a report location and suggest appropriate medication. In the existing system, there is a chance that the data transferred over the network to the doctor might be mishandled as the user name and password might not be a completely secure solution to protect the patient data. Hence we have incorporated an additional level of authentication in order to be able to view the remote patient's data. The doctor must produce the secret key given to him before viewing the reports of the patient. This enhances the security of the system and protects the data from falling into wrong hands.

II. RELATED WORK

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 [7], [8], [9], [10]. In [7], 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 [8], 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 [7] and [8] 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 [9], [10]. 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 m-Healthcare emergency.

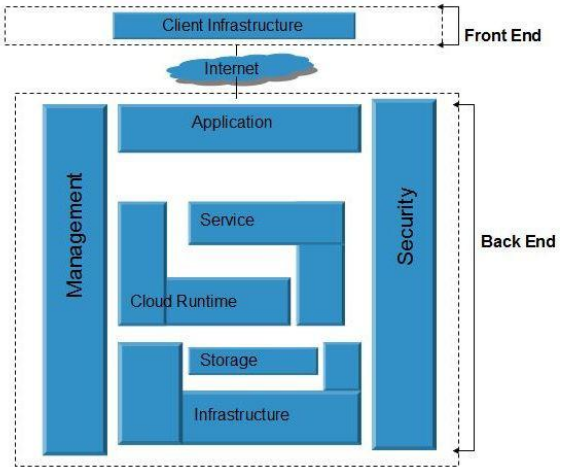
The Cloud Computing architecture

The Cloud Computing architecture comprises of many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

- Front End

- Back End

Each of the ends are connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:



FRONT END

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.

BACK END

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

IMPORTANT POINTS

It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.

The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.

Cloud based delivery

Software as a service (SaaS)

The software-as-a-service (SaaS) service-model involves the cloud provider installing and maintaining software in the cloud and users running the software from their cloud clients over the Internet (or Intranet). The users' client machines require no installation of any application-specific software - cloud applications run on the server (in the cloud). SaaS is scalable, and system administration may load the applications on several servers. In the past, each customer would purchase and load their own copy of the application to each of their own servers, but with the SaaS the customer can access the application without installing the software locally. SaaS typically involves a monthly or annual fee

Software as a service provides the equivalent of installed applications in the traditional (non-cloud computing) delivery of applications.

Software as a service has four common approaches:

1. single instance
2. multi instance
3. multi-tenant
4. flex tenancy

Development as a service (DaaS)

Development as a service is web based, community shared development tools. This is the equivalent to locally installed development tools in the traditional (non-cloud computing) delivery of development tools.

Platform as a service (PaaS)

Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional (non-cloud computing) delivery of application platforms and databases.

Infrastructure as a service (IaaS)

Infrastructure as a service is taking the physical hardware and going completely virtual (e.g. all servers, networks, storage, and system management all existing in the cloud). This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. In other words, businesses pay a fee (monthly or

annually) to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

III. EXISTING SYSTEM

In Existing System, According to the sensex over the age of 65 is expected to hit 70 million by 2030, having doubled since 2000. Health care expenditures projected to rise to 15.9% by 2010. The cost of health care for the nation's aging population has become a national concern 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.

IV. PROPOSED SYSTEM

In our proposed SPOC framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency. In the existing remote patient monitoring system, the patient's crucial heath parameters such as BP, heartbeat, Blood sugar etc are monitored continuously by the doctor in a remote location. Various health parameters of the patient are transferred to the base station using sensors and the doctor can get a report of the patient condition from a report location and suggest appropriate medication. In the existing system, there is a chance that the data transferred over the network to the doctor might be mishandled as the user name and password might not be a completely secure solution to protect the patient data. Hence we have incorporated an additional level of authentication in order to be able to view the remote patient's data. The doctor must produce the secret key given to him before viewing the reports of the patient. This enhances the security of the system and protects the data from falling into wrong hands.

Advantages:

- Shift from a clinic-oriented, centralized healthcare system to a patient-oriented, distributed healthcare system
- Reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions

Challenges:

- Performance, Reliability, Scalability, QoS, Privacy, Security…
- More prone to failures, caused by power exhaustion, software and hardware faults, natural disasters, malicious attacks, and human errors etc.

V. CONCLUSION

In this paper, we have proposed a secure and privacypreserving opportunistic computing (SPOC) framework for m-Healthcare 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 m-Healthcare 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. By implementing the above discussed security mechanim, we are able to transfer the data of

the remote patient securely to the authorized doctors.

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.

[7] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, "Opportunistic computing for wireless sensor networks," in IEEE Proc. of MASS'07, pp. 1–6.

[8] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance evaluation of service execution in opportunistic computing," in Proc. of ACM MSWIM '10, 2010, pp. 291–298.

[9] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," IEEE Communications Magazine, vol. 48, pp. 126–139, September 2010.

[10] M. Conti and M. Kumar, "Opportunities in opportunistic computing," IEEE Computer, vol. 43, no. 1, pp. 42–50, 2010.

[11] W. Du and M. Atallah, "Privacy-preserving cooperative statistical analysis," in Proc. of ACSAC '01, 2001, pp. 102–111.

[12] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in Proc. of ACM KDD'02, pp. 639–644.

[13] A. Amirbekyan and V. Estivill-Castro, "A new efficient privacypreserving scalar product protocol," in Proc. of AusDM '07, pp. 209–214.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. of EUROCRYPT'99, 1999, pp. 223–238.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Transactions on Parallel Distributed and Systems, to appear.

[16] SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency, IEEE Transactions on parallel and distributed systems, 2012

AUTHOR'S PROFILE

POTTETI SANDHYA RANI, received B.Tech degree from Rao & Naidu College of Engineering &Technology, Ongole, Prakasam, Andhra Pradesh. and currently pursuing M.Tech in Computer Science Engineering at VRS & YRN College of Engineering &Technology, Chirala; Prakasam (Dt), Andhra Pradesh. Her areas of interest area include Cloud Computing.

MR. S. RAMA KRISHNA is presently working as Associate professor and Head of CSE Department in VRS & YRN College of Engineering & Technology, Chirala, AP, India. He completed his B.Tech degree in Computer Science and Engineering from JNTUH, Hyderabad. And then completed his M.Tech. in Computer Science and Engineering as his specialization from JNTUH, Hyderabad. Now he is pursuing his Ph.D Degree in Computer Science and Engineering from JNTUH, Hyderabad. His research areas include Cloud Computing and Security. He has a teaching experience of 10 years. He published papers in 3 International Journals and 1 National Conference.