ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

User Centric Privacy Access control For M-Healthcare Emergency in Opportunistic Computing

M.Anandhajothi[1], S.Hasan Hussain[2]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India
1, 2

ABSTRACT: 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. We propose a secure and privacy-preserving opportunistic computing framework. Here an efficient user-centric privacy access control is introduced in which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique..

KEYWORDS-Usercentric, M-Healthcare, Opurtunistic computing

I. INTRODUCTION

In mobile 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 Smart phones are utilized to provide remote healthcare monitoring to people who have chronic medical conditions such as diabetes and heart . 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 formed by body sensor nodes, medical users can walk outside and receive the high-quality healthcare monitoring from medical professionals anytime and anywhere. For 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. 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. To propose a new secure and privacy preserving opportunistic computing framework to address this challenge. With the proposed 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.

To propose a secure and privacy preserving opportunistic computing framework for m-Healthcare emergency. With this project, the resources available on other opportunistically contacted medical users' smart phones can be gathered together to deal with the computing-intensive PHI process in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure, It introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing. To achieve user-centric privacy access control in opportunistic computing, we present an efficient attribute-based 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 yet most of them are relying on time-consuming homomorphic encryption technique. 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.

II. RELATED WORKS

The m-Healthcare social network (MHSN) built upon wireless body sensor network (WBSN) and mobile communications provides a promising platform for the seniors who have the same symptom to exchange their experiences, give mutual support and inspiration to each other, and help forwarding their health information wirelessly to a related e-Health center. However, there exist many challenging security issues in MHSN such as how to securely identify a senior who has the same symptom, how to prevent others who don't have the symptom from knowing someone's symptom. To tackle these challenging security issues, propose a secure same-symptom-based handshake (SSH) scheme, and apply the provable security technique to demonstrate its security in the random oracle model. In addition, we discuss a promising application – social-based patient health information (PHI) collaborative reporting in MHSN, and conduct extensive simulations to evaluate its efficiency in terms of PHI reporting delay. In m-Healthcare system, patient's PHI is always considered being reported to the e-Health center directly, and the primary security issue is to keep the patient's PHI secret, and only the related medical professionals at e-Health center can read them. However, due to patient's mobility, patients can often contact with each other in m-Healthcare system. If two patients have the same symptom, it is possible for them to share their health condition and experiences, provide mutual support and inspiration to each other to eliminate loneliness. We call such kind of social contact as m-Healthcare social network (MHSN). In our aging society, MHSN is promising and can be accepted by the sensors[1]. The transactions are distributed across sources of each site holds some attributes of each transaction, and the sites wish to collaborate to identify globally valid association rules. However, the sites must not reveal individual transaction data. We present a two-party algorithm for efficiently discovering frequent item sets with minimum support levels, without either site revealing individual transaction values. Secure computation of scalar product is the key to our protocol. Scalar product protocols have been proposed in the Secure Multiparty Computation, however these cryptographic solutions do not scale well to this data mining problem. We give an algebraic solution that hides true values by placing them in equations masked with random values. The knowledge disclosed by these equations only allows computation of private values if one side learns a substantial number of the private values from an outside source[2]. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, to focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. That scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments[3], under the multi owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains (PSDs). In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence. Wireless body sensor network hardware has been designed and implemented based on MICS (Medical Implant Communication Service) band. The MICS band offers the advantage of miniaturized electronic devices that can either be used as an implanted node or as an external node. In this work, the prototype system uses temperature and pulse rate sensors on nodes.To build a Wireless Body Sensor Network (WBSN) that is based on the newly available 402–405 MHz MICS band. As mentioned above, this band was particularly chosen to provide small size, low-power, faster data transfer and longer communication range. The MICS band is located at an optimum frequency range that promises high-level of integration with the advanced radio frequency IC (RFIC) technology. This results in miniaturization and low-power consumption. While higher frequency causes higher penetration loss, high-level integration becomes difficult at low frequencies. In addition, there exists relatively insignificant penetration loss at these frequencies (10 dB with 10 mm tissue penetration). Moreover, a small antenna design is also difficult at lower frequencies. The antennas for this project are designed as a loop printed around the prototyping boards. Combining all these features with the availability of the 402–405 MHZ band internationally offers an attractive frequency choice for the targeted WBSN application[4]. Opportunistic computing has emerged as a new paradigm in computing, leveraging the advances in pervasive computing and opportunistic networking. Nodes in an opportunistic network avail of each other's connectivity and mobility to overcome network partitions. In opportunistic computing, this concept is generalized, as nodes avail of any resource available in the environment. To focus on computational resources, assuming mobile nodes opportunistically invoke services on each other. Specifically, resources are abstracted as services contributed by providers and invoked by seekers. To present an analytical model that depicts the service invocation process between seekers and providers. Specifically, we 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[5].

III. PROPOSED WORK

To propose a new secure and privacy preserving opportunistic computing framework to address this challenge. With the proposed 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 propose a secure and privacy preserving opportunistic computing framework for m-Healthcare emergency. With the resources available on other opportunistically contacted medical users' smart phones can be gathered together to deal with the computing-intensive PHI process in emergency situation. Since the PHI will be disclosed during the process in opportunistic computing, to minimize the PHI privacy disclosure.

It 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 attribute-based access control and a novel nonhomomorphic 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 yet most of them are relying on time-consuming homomorphic encryption technique. To the best of our knowledge, our novel nonhomomorphic encryption-based PPSPC protocol is the most efficient one in terms of computational and communication overheads.

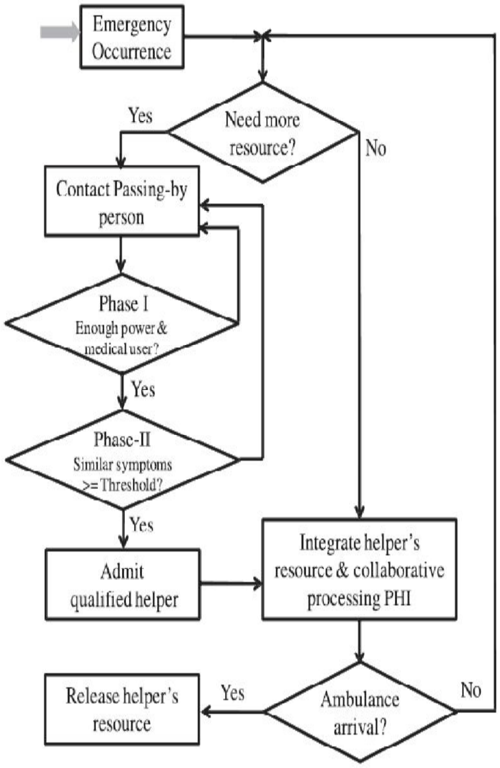
Emergency Occurrence
Need more resource?
Yes
No
Contact Passing-by person
Phase I
Enough power & medical user?
Yes
Phase-II
Similar symptoms >=Threshold?
Yes
Admit qualified helper
Integrate helper's resource & collaborative processing PHI
Release helper's resource
Yes
Ambulance arrival?
No

Fig.1: Opurtunistic computing with two phase user centric access control for M-Healthcare

Opportunistic computing can enhance the reliability for high-intensive PHI process and transmission in m-Healthcare emergency. However, since PHI is very sensitive, a medical user, even in emergency, will not expect to disclose his PHI to all passing-by medical users. Instead, he may only disclose his PHI to those medical users who have some similar symptoms with him. In this case, the emergency situation can be handled by opportunistic computing with minimal privacy disclosure. Specifically, in our security model, we essentially define two-phase privacy access control in opportunistic computing, which are required for achieving high-reliable PHI process and transmission in m-Healthcare emergency, as shown in Fig.1.

Phase-I access control. Phase-I access control indicates that

although a passing-by person has a smart phone with enough power, as a nonmedical user, he is not welcomed to participate in opportunistic computing.1 Since the opportunistic computing requires smart phones that are installed with the same medical software's to cooperatively process the PHI, if a passing-by person is not a medical user, the lack of necessary software's does not make him as an ideal helper. Therefore, the phase-I privacy access control is prerequisite.

Phase-II access control. Phase-II access control only allows those medical users who have some similar symptoms to participate in the opportunistic computing. The reason is that those medical users, due to with the similar symptoms, are kind of skilled to process the same type PHI. Note that, the threshold th is a user self-control parameter. When the emergency takes place at a location with high traffic, the threshold th will be set high to minimize the privacy disclosure. However, if the location has low traffic, the threshold th should be low so that the high-reliable PHI process and transmission can be first guaranteed. Shift from a clinic-oriented, centralized healthcare system to a patient oriented resources and earlier detection of medical conditions Challenges: Performance, Reliability, Scalability, Quos, Privacy.

Security. Distributed healthcare system :Reduce healthcare expenses through more efficient use of clinical This framework can medical users to balance the high reliability of PHI process and minimizing the PHI privacy disclosure in m-Healthcare emergency. The resources available on opportunistically contacted medical users' smart phones can be gathered together to deal with the computing-intensive PHI process in emergency situation. To minimize the PHI privacy disclosure.The attributed-based access control can help a medical user in emergency to identify other medical users.

IV MODULAR DESCRIBTION

There are 5 types of modules in this project.

*A.system initialization:*For a single-authority m-Healthcare system under consideration, we assume a trusted authority located at the healthcare center will bootstrap the whole system. Specifically, given the security parameter, TA first generates the bilinear parameters by running, and chooses a secure symmetric encryption algorithm AES, and two secure cryptographic hash functions. In addition, TA chooses two random numbers as the master key, two random elements, and computes. Finally, TA keeps the master secretly, and publishes the system parameter. Assume there are total n symptom characters considered in m-Healthcare system, and each medical user's symptoms can be represented through his personal health profile, a binary vector in the n-dimensional symptom character space, where indicates a symptom character, i.e., if the medical user has the corresponding symptom character, and otherwise. Therefore, for each medical user Ui 2 UU, when he registers himself in the healthcare center, the medical professionals at healthcare centre first make medical examination for Ui, and generate Ui's personal health profile. Afterward, the following steps will be performed by TA. Based on Ui's personal health profile, TA first chooses the proper body sensor nodes to establish Ui's personal BSN, and installs the necessary medical software in Ui's Smartphone.To equipped with the personal BSN and key materials can securely report his PHI to healthcare center for achieving better healthcare monitoring.Every five minutes, BSN collects the raw PHI data rPHI and reports the encrypted value to the Smartphone with Bluetooth technology.

*B.User-centric privacy access control for m-healthcare emergency:*When an emergency takes place in m-Healthcare U0 suddenly falls down outside, the healthcare center will monitor the emergency, and immediately dispatch an ambulance and medical personnel to the emergency location. Generally, the ambulance will arrive at the scene around 20 minutes. During the 20 minutes, the medical personnel needs high-intensive PHI to real-time monitor U0. However, the power of U0's Smartphone may be not sufficient to support the high-intensive PHI process and transmission.

Phase-I access control:The goal of phase-I access control is to identify other medical users in emergency. To achieve the phase-I access control, Smartphone first chooses a random number. When user U0 receives Auth||timestamp at time timestamp 0, he first checks the validity of the time interval between timestamp0 and timestamp in order to resist the replaying attack. If j timestamp 0 time stamp j, where T denotes the expected valid time interval for transmission delay, U0 accepts and processes Auth||timestamp, and rejects otherwise. Once Auth||timestamp is accepted, U0 uses the stored to compute, and checks whether Auth. If it does hold, Uj is authenticated as a medical user, and passes the phase-I access control.

Phase-II access control:Once Uj passes the phase-I access control, U0 and Uj continue to perform the phase-II access control to check whether they have some similar symptoms. Suppose the personal health profiles of medical users U0, Uj are respectively. U0 first defines an expected threshold th for the number of common symptom characters. Then, in order to compute a privacy-preserving way, U0 and Uj invoke our newly designed PPSPC protocol in Algorithm. Since the

PPSPC protocol ensures neither U0 nor Uj will disclose their personal healthcare profiles to each other during the computation , it can efficiently achieve privacy preserving access control. However, if the returned value, Uj is not a qualified helper to participate in opportunistic computing. Note that the threshold th is not fixed, if the residual power of U0's Smartphone can last a little long time, can be set relatively high to minimize the PHI privacy disclosure. However, if the residual power is little, can be set low so as to first guarantee the reliability of high-intensive PHI process and transmission.

*C.Analysis of opportunistic computing in m-healthcare emergency:*Consider the ambulance will arrive at the emergency location in the time period t. To gauge the benefits brought by opportunistic computing in m-Healthcare emergency, we analyze how many qualified helpers can participate in opportunistic computing within the time period t, and how many resources can the opportunities computing provide.For a given threshold th, respectively, denoted as the number of qualified helpers (NQHs) and the number of nonqualified helpers. For any arriving user at time, the probability that the user is a qualified helper.

Theorem 1: The expected number of the qualified helpers participating in opportunistic computing within time.

Theorem 2:The expected resources that can be provided by opportunistic computing.

*D. Security Analysis:*To analyze the security properties of the proposed SPOC framework. In specific, following the security requirements discussed earlier, analyses will focus on how the proposed SPOC framework can achieve the user-centric privacy access control for opportunistic computing in m-Healthcare emergency.The proposed SPOC framework can achieve the phase-I access control. In the phase-I access control, the single attribute encryption technique is employed.The proposed SPOC framework can achieve the session key's forward and backward secrecy.

*E.Simulation setup:*The communications between Smartphone and the communications between BSNs and Smartphone are always workable when they are within each other's transmission ranges. The performance metrics used in the evaluation are 1) the average number of qualified helpers, which indicates how many qualified helpers can participate in the opportunistic computing within a given time period, and 2) the average resource consumption ratio (RCR), which is defined as the fraction of the resources consumed by the medical user in emergency to the total resources consumed in opportunistic computing for PHI process within a given time period. Both NGH and RCR can be used to examine the effectiveness of the proposed SPOC framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

In this module, the performance metrics used in the evaluation are :

1) The average number of qualified helpers (NQH), which indicates how many qualified helpers can participate in the opportunistic computing within a given time period, and

2) The average resource consumption ratio (RCR), which is defined as the fraction of the resources consumed by the medical user in emergency to the total resources consumed in opportunistic computing for PHI process within a given time period.

In this Module, the simulator implements the application layer under the assumptions that the communications between smart phones and the communications between BSNs and smart phones are always workable when they are within each other's transmission ranges.

V CONCLUSION

The secure and privacy preserving opportunistic computing 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.

To intend carry on Smartphone-based experiments to further verify the effectiveness of the proposed 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 Comm., vol. 16, no. 3, pp. 24-32, June 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," Proc. Fifth Int'l Conf. Body Area Networks (BodyNets '10), 2010.

[3] Y. Ren, R.W.N. Pazzi, and A. Boukerche, "Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Comm., vol. 17, no. 1, pp. 59-65, Feb. 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, "A Secure Handshake Scheme with Symptoms-Matching for mHealthcare Social Network," Mobile Networks and Applications—special issue on wireless and personal comm., 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 Trans. Parallel and Distributed System, to be published.

[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," J. 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," Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '07), pp. 1-6, 2007.

[8] A. Passarella, M. Conti, E. Borgia, and M. Kumar, "Performance Evaluation of Service Execution in Opportunistic Computing," Proc. 13th ACM Int'l Conf. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM '10), pp. 291-298, 2010.

[9] M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," IEEE Comm. Magazine, vol. 48, no. 9, pp. 126-139, Sept. 2010.

[10] M. Conti and M. Kumar, "Opportunities in Opportunistic Computing," IEEE Computer, vol. 43, no. 1, pp. 42-50, Jan. 2010.