IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

P. Swetha[1*], P. Srividhya[2]

[1,2]M.Sc Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India

Corresponding Author:swetha892@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**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. In this proposal 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, it leverages attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we 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 multiauthority ABE. This technique also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

***Keywords*—** Attribute, Encryption, Health Record, Cloud, Trusted Server.

I. INTRODUCTION

The 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 smart phones 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 smart phone 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, 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. 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, It 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 smart phone 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. 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 m-Healthcare emergency to resolve the challenging reliability issue in PHI process.

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.

II. METHODOLOGY

This proposed technique is a new secure and privacy preserving opportunistic computing framework, called MASPOC, to address this challenge. With the proposed MASPOC 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 system have been developed with multiple attributes.

This technique is to leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, it introduce an efficient user-centric privacy access control in MASPOC framework, which is based on an attribute-based access control and a new OTP based 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 MASPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency. In addition, performance evaluations via extensive simulations demonstrate the MASPOC's effectiveness in term of providing high-reliable-PHI process and transmission while minimizing the privacy disclosure during m-Healthcare emergency.

Advantages

- This system monitors health care emergency systems are works with both passive and active data stored in the centralized data servers.
- Opportunistic computing with maximum true user's information leads to effective and efficient data collection during the time of emergency situations.
- Since smart phones are 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 proposed system handles the kind of unexpected event may happen with very high probability, i.e., 60.2%, for a medical emergency, take into 10,000 emergency cases into consideration, the average event number will reach 500, which is not negligible and explicitly indicates the reliability of m-Healthcare system is still challenging in emergency.
- This system can be extended into active directory based data separation options given for each smart phone users.
- Location based privacy protection modules can be added for better data preservation for individual user's perspective.
- PHI data can be serve as per the emergency situation by sending the OTP mechanism can also added to get the fast authentification from the donor.

The proposed system has been divided into several modules to achieve the MASPOC data extraction with formulation of optimized results.

III. MODULES

1. **HEALTH Cloud SERVER**
2. **USER DATA PHI METRIC**
3. **HEALTH EMERGENCY REQUEST PROCESSOR**
4. **SERVICE PROVIDER**
5. **OTC Privacy Tracker**
6. **RESULTS**

HEALTH Cloud SERVER

In this module new secure and privacy preserving opportunistic computing health server has been installed, to address the m-user data storing and retrieval on a secured process. With the proposed SPOC framework, each medical user in emergency can achieve the user-centric privacy access control to allow entering into the system only qualified m-users to participate in the opportunistic

computing to balance the high reliability of PHI process in m-Healthcare emergency server.

MOBILE USER DATA PHI METRIC

This module mainly deals with the process of registering the m-user PHI data into the mobile health care server and provides the login credentials for further authentication process, it shows the secure and privacy preserving opportunistic computing framework for m-Healthcare emergency. With MASPOC, the resources available on other opportunistically contacted medical users' 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, MASPOC introduces a user-centric two-phase privacy access control to only allow those medical users who have similar symptoms to participate in opportunistic computing.

M-HEALTH EMERGENCY REQUEST PROCESSOR

The major process of the system is to provide the PHI data to the particular emergency user by validate the user's request on the basis of timestamp, location based user search ,status of the donors and active directory user search implemented attributed based access control can help the emergency user in emergency 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.

SERVICE PROVIDER

The PHI data has send to the particular emergency m-user by the sending the OTP(one time password) code to the donors list after confirm the code the complete PHI m-user list has send to the emergency requester for further communication has been made directly.

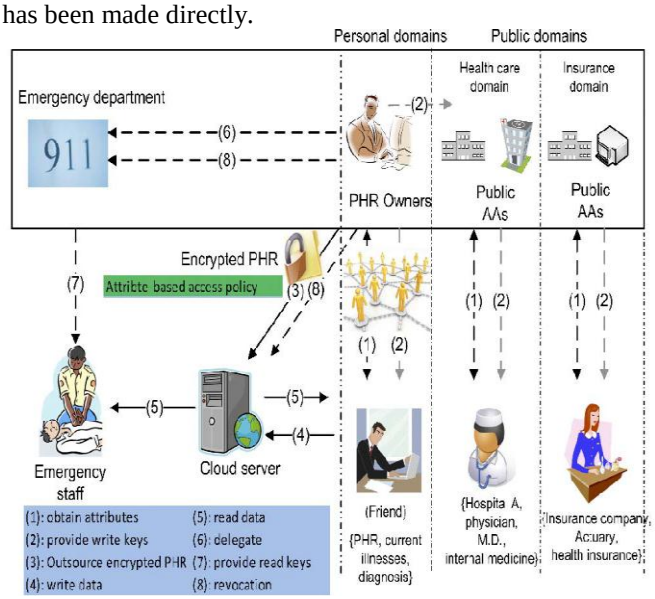

Figure 1: System architecture

IV. RESULTS AND DISCUSSION

In this section, evaluate the performance of the proposed SPOC framework using a custom simulator built in Java. 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. 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 MASPOC framework with user-centric privacy access control of opportunistic computing in m-Healthcare emergency.

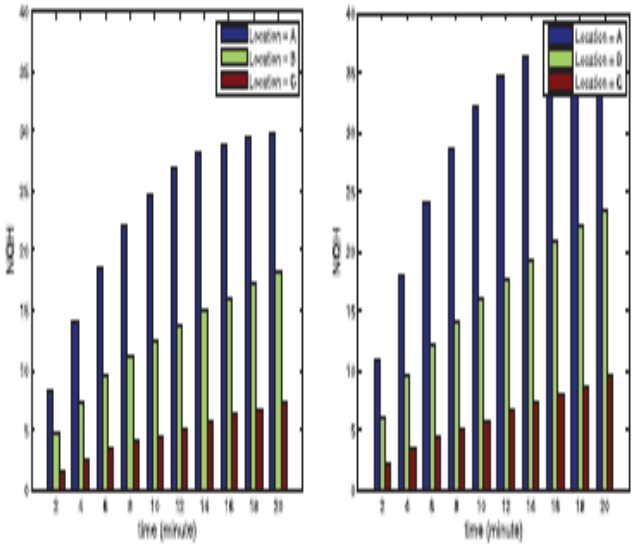

Figure 2: Results

Note that, in the simulations, consider all users will stop when they meet U0's emergency, and only the qualified helpers will participate in the opportunistic computing. To eliminate the influence of initial system state, a warm-up period of first 10 minutes is used. In addition, the system consider U0's emergency takes place at three locations, A, B, and C, in the map to examine how the factors l, th affect the NGH and RCR at different locations. The detailed parameter settings are summarized in Table 1.

TABLE 1
Simulation Settings

Parameter	Setting
Simulation area	500 m × 500 m
Simulation warm-up, duration	10 minutes, 20 minutes
Number, velocity of users	$l = \{40, 60\}$, $v = 0.5 - 1.2$ m/s
Similarity threshold	$th = \{3, 5\}$
Transmission of smartphone, BSN	20 m, 20 m
Raw PHI data generation interval	every 10 seconds
Emergency location	A, B, and C

In the following the simulations with different parameter settings. For each setting, the simulation lasts for 20 minutes (excluding the warm-up time), and the average performance results over 10,000 runs are reported. the system compare the average NQHs at locations A, B and C varying with time from 2 to 20 minutes under different user number l and threshold th. From the figure, the system can see, with the increase of time, the average NQH will also increase, especially for the location A. The reason is that, when all users move in the simulation area by following the same mobility model, location A will have higher traffic than locations B and C. In addition, when the user number l in the simulation area increases, the user arrival rate at locations A, B, and C also increase. Then, the average NQH increases as well. By further observing the differences of the average NQH under thresholds th = 3 and th = 5, the system can see the average NQH under th = 5 is much lower than that under th = 3, which indicates that, in order to minimize the privacy disclosure in opportunistic computing, the larger threshold should be chosen. However, since the high reliability of PHI process is expected in m-Healthcare emergency, minimizing the privacy disclosure in opportunistic computing is not always the first priority.

V. CONCLUSION

This proposed model SPOC a 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, this demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency.

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 andpersonal 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.

[11] W. Du and M. Atallah, "Privacy-Preserving Cooperative Statistical Analysis," Proc. 17th Ann. Computer Security Applications Conf. (ACSAC '01), pp. 102-111, 2001,

[12] J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data," Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '02), pp. 639-644, 2002.

[13] A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," Proc. Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), pp. 209- 214, 2007.

[14] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Proc. 17th Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT '99), pp. 223-238, 1999.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Comm.," IEEE Trans. Parallel Distributed and Systems, to be published.

[16] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A Strong Privacy-Preserving Scheme against Global Eavesdropping for Ehealth Systems," IEEE J. Selected Areas in Comm., vol. 27, no. 4, pp. 365-378, May 2009.

[17] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm., vol. 17, no. 1, pp. 51-58, Feb. 2010.

[18] J. Sun and Y. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," IEEE Trans. Parallel Distributed and Systems, vol. 21, no. 6, pp. 754-764, June 2010.

[19] "Exercise and Walking is Great for the Alzheimer's and Dementia Patient's Physical and Emotional Health," http://freealzheimers-support.com/wordpress/2010/06/exercise-andwalking/, June 2010.
[20] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications," IEEE Comm. Magazine, vol. 49, no. 4, pp. 28-35, Apr. 2011.
[21] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Ann. Int'l Conf. Cryptology Organized (CRYPTO '01), pp. 213-229, 2001.
[22] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for vehicular communications," IEEE Trans.Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.
[23] R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 6,pp. 2772-2785, July 2010.
[24] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets," IEEE Trans. Vehicular Technology, vol. 61,
pp. 86-96, 2012.
[25] http://www.uaproperty.com/articles/In-Ukraine-ambulancecome-patient-10-minute s.html, 2012.
[26] S. Ross, Introduction to Probability Models, Ninth Ed., 2007.
[27] X. Lin, R. Lu, X. Liang, and X. Shen, "STAP: A Social-Tier-Assisted Packet Forwarding Protocol for Achieving Receiver-Location Privacy Preservation in Vanets," Proc. of INFOCOM '11, pp. 2147-2155, 2011.
[28] W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," Proc. of CRPIT '14, ser. CRPIT '14, pp. 1-8, 2002.
[29] I. Ioannidis, A. Grama, and M. Atallah, "A Secure Protocol for Computing Dot-Products in Clustered and Distributed Environments,"Proc. of ICPP '02, pp. 379-384, 2002.
[30] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure Friend Discovery in Mobile Social Networks," Prof. of INFOCOM '11,pp. 1647-1655, 2011.
[31] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-Grained Private Matching for Proximity-Based Mobile Social Networking," Prof. of INFOCOM '12, pp. 1-9, 2012.
[32] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-Preserving Personal Profile Matching in Mobile Social Networks," Proc. INFOCOM, pp. 2435-2443, 2011.
[33] K.-H. Huang, Y.-F.Chung, C.-H.Liu, F. Lai, and T.-S. Chen, "Efficient Migration for Mobile Computing in Distributed Networks,"Computer Standards and Interfaces, vol. 31, no. 1, pp. 40-47,2009.

