Personalized and Self Control Privacy Preserving Of the Data in the Cloud

Mr.S.RamanaReddy, Mr.N.SaiKrishna

ABSTRACT:

Distributed m-healthcare cloud computing system significantly facilitates efficient patient treatment for medical consultation by sharing personal health information among healthcare providers. However, it brings about the challenge of keeping both the data confidentiality and patients' identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem, in this paper, a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.

INTRODUCTION

Distributed m-healthcare systems have been increasingly adopted by the European Commission activities, the US Health Insurance Portability and Accountability Act (HIPAA) and many other governments for efficient and high-quality treat- ment [1-3]. The personal health information is always shared among the patients suffering from the same disease, between the patients and physicians as equivalent counterparts or even across distributed healthcare providers for medical consultant [28], [29]. This kind of personal health information sharing allows each collaborating healthcare provider to process it locally with higher efficiency and scalability, greatly enhances the treatment quality, significantly alleviates the complexity at the patient side and therefore becomes the preliminary component of a distributed m-healthcare system. However, it also brings about a series of challenges, es- pecially how to ensure the security and privacy of the patients' personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering [5], [26].

As to the security facet, we mean the access control of personal health information, namely it is only the autho- rized physicians or institutions that can recover the patients' personal health information during the data sharing in the distributed m-healthcare system. In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. For example, the patients' insurance application may be rejected once the insurance company has the knowledge of the serious health condition of its consumers. Therefore, in distributed m-healthcare systems, which part of the patients' personal health information should be shared and which part of physicians should their personal health information be shared with have increasingly become two intractable problems demanding urgent solutions. There has emerged various research [8- 11, 15, 16, 18, 19] focusing on it such as a fine-grained distributed data access control scheme [9] using the technique of attribute based encryption and a rendezvous-based access control method [10] providing access if and only if the patient and the physician meet in the physical world. Unfortunately, the problem of simultaneously protecting patients' privacy was left unsolved.

II. RELATED WORK

Besides the constructions for authorized access control of patients' personal health information [8-11, 15, 16, 18, 19] we mentioned above, there exist anonymous identification schemes by pseudonyms and other privacy-preserving tech- niques [4, 10-14, 17, 20, 23, 25]. Lin et. al. proposed SAGE achieving not only the content oriented privacy but also the contextual privacy against a strong global adversary [12]. Sun et. al. proposed a solution to privacy and emergency responses based on anonymous credential, pseudorandom number gen- erator and proof of knowledge [11, 13]. Lu et. al. proposed a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof [14]. However, the heavy computational overhead of Zero-Knowledge Proof makes it cannot be directly applied to the distributed m- healthcare systems where the computational resource for both patients and physicians is limited. Riedl et. al. presented a new architecture pseudonymiaztion of information for privacy in E- health (PIPE) [25]. Slamanig et. al. integrated pseudonymiza- tion of medical data, identity management, obfuscation of metadata with anonymous authentication to prevent disclo- sure attacks and statistical analysis in [26] and suggested a secure mechanism guaranteeing anonymity and privacy in both the personal health information transferring and storage at a healthcare provider [7]. Schechter et. al. proposed an anonymous authentication of membership in dynamic groups [6]. However, since the anonymous authentication mentioned above [6], [7] are established based on public key infrastructure (PKI), the need of an online certificate authority (CA) and one unique public key encryption for each symmetric key *k* for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level is dependent on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

In this paper, our proposed authorized accessible privacy model (AAPM) and the patient self-controllable privacy-preserving authentication scheme (PSCPA) are proposed by extending the traditional designated verifier signature to an attribute based counterpart. The security and anonymity level is significantly enhanced by associating it to GBDH problem and the number of patients' attributes to deal with the privacy leakage in patient sparsely distributed scenarios in [6, 7]. Meanwhile, our construction cost is linear to the number of attributes rather than the physicians in healthcare providers. Therefore, it better adapts to the distributed m-healthcare systems where the number of physicians is great and the patients need the timely responses from the healthcare providers.

Last but not least, it is noticed that our construction essen- tially differs from the trivial combination of attribute based encryption [22] and designated verifier signature [21]. As the simulation results shows, we achieve the functionalities of both access control for personal health information and anonymous authentication for patients simultaneously with the efficiency significantly less than the trivial combination of the two building blocks above. Therefore, our PSCPA far outperforms the previous schemes [21, 22] in access control for patients' personal health information and [6, 7] in realizing privacy-preserving cooperative authentication in distributed m- healthcare systems.

III. NETWORK MODEL

The basic e-healthcare system consists of three components: BANs, wireless transmission networks and the healthcare providers [1], [2]. Body sensor networks consist of vari- ous kinds of sensors monitoring and collecting all personal health information to the patient hand-held mobile device. The wireless transmit ssion networks transfer personal health information to the physicians in healthcare providers. The healthcare provider consists of physicians and the patient infor- mation database (PIDs) [26]. Authorized physicians can access their corresponding patients' personal health information and authenticates their identities.

CONCLUSIONS

In this paper, a novel authorized accessible privacy model (AAPM) and a patient self-controllable privacy-preserving cooperative authentication scheme (PSCPA) realizing three levels of security and privacy requirement in the distributed m-healthcare system are proposed, followed by the formal se- curity proof and efficiency evaluations. Patients can authorize the physicians by setting an access tree supporting flexible threshold predicates. The directly authorized physicians, the indirectly authorized physicians and the unauthorized physi- cians would know both the patient's identity and the per- sonal health information, only the personal health information and nothing respectively. Finally, simulation results show our PSCPA far outperforms previous schemes in terms of storage, computational and communication overhead.

REFERENCES

[1] L.Gatzoulis and I. Iakovidis, *Wearable and Portable E-health Systems*,
IEEE Eng. Med. Biol. Mag., 26(5):51-56, 2007.

[2] I. Iakovidis, *Towards Personal Health Record: Current Situation, Ob-*

stacles and Trends in Inplementation of Electronic Healthcare Records in Europe, International Journal of Medical Informatics, 52(1):105-115, 1998.

[3] E. Villalba, M.T. Arredondo, S. Guillen and E. Hoyo-Barbolla, *A New Solution for A Heart Failure Monitoring System based on Wearable and Information Technologies*, In International Workshop on Wearable and Implantable Body Sensor Networks 2006-BSN 2006, April, 2006.

[4] R. Lu and Z. Cao, *Efficient Remote User Authentication Scheme Using Smart Card*, Computer Networks, 49(4):535-540, 2005.

[5] M.D.N. Huda, N. Sonehara and S. Yamada, *A Privacy Management Architecture for Patient-controlled Personal Health Record System*, Journal of Engineering Science and Technology, 4(2):154-170, 2009.

[6] S. Schechter, T. Parnell and A. Hartemink, *Anonymous Authentication of Membership in Dynamic Groups*, in Proceedings of the Third International Conference on Financial Cryptography, 1999.

[7] D. Slamanig, C. Stingl, C. Menard, M. Heiligenbrunner and J. Thierry, *Anonymity and Application Privacy in Context of Mobile Computing in eHealth*, Mobile Response, LNCS 5424, pp. 148-157, 2009.

[8] M. Li, S. Yu, W. Lou and K. Ren, *Group Device Paring based Secure Sensor Association and Key Management for Body Area Networks*, In IEEE Infocom 2010.

[9] S. Yu, K. Ren and W. Lou, *FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks*, In IEEE Infocom 2009.

[10] F.W. Dillema and S. Lupetti, *Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment*, In HealthNet 2007.

[11] J. Sun, Y. Fang and X. Zhu, *Privacy and Emergency Response in E-healthcare Leveraging Wireless Body Sensor Networks*, IEEE Wireless Communications, pp. 66-73, February, 2010.

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, *SAGE: A Strong Privacy-preserving Scheme against Global Eavesdropping for E-health*

Systems, IEEE Journal on Selected Areas in Communications, 27(4):365-378, May, 2009.

[13] J. Sun, X. Zhu, C. Zhang and Y. Fang, *HCPP: Cryptography Based Secure EHR System for Patient Privacy and Emergency Healthcare*, ICDCS'11.

[14] L. Lu, J. Han, Y. Liu, L. Hu, J. Huai, L.M. Ni and J. Ma, *Pseudo Trust: Zero-Knowledge Authentication in Anonymous P2Ps*, IEEE Transactions on Parallel and Distributed Systems, vol. 19, No. 10, October, 2008.

[15] J. Zhou and M. He, *An Improved Distributed key Management Scheme in Wireless Sensor Networks*, In 9th. International Workshop of Information Security Applications 2008-WISA 2008, September, 2008.

[16] M. Li, S. Yu, N. Cao and W. Lou, *Authorized Private Keyword Search over Encrypted Data in Cloud Computing*, ICDCS'11.

[17] M. Chase and S.S. Chow, *Improving Privacy and Security in Multi-authority Attribute-based Encryption*, In ACM CCS 2009, pp. 121-130, 2009.

[18] J. Bethencourt, A. Sahai, and B. Waters, *Ciphertext-Plicy Attribte-Based Encryption*, In IEEE Symposium on Security and Privacy, 2007.

[19] N. Cao, Z. Yang, C. Wang, K. Ren and W. Lou, *Privacy-preserving Query over Encrypted Graph-structured Data in Cloud Computing*, ICDCS'11.

[20] F. Cao and Z. Cao, *A Secure Identity-based Multi-proxy Signature Scheme*, Computers and Electrical Engineering, vol. 35, pp. 86-95, 2009.

[21] X. Huang, W. Susilo, Y. Mu and F. Zhang, *Short Designated Verifier*

Author's profile:

Mr.S.Ramana Reddy received M.Tech(CSE) Degree from School of Information Technology, Autonomous, and Affiliated to JNTUH, Hyderabad. He is currently working as Assistant Professor in the Department of Computer Science and Engineering in Nalgonda Institute of Technology and Science, Nalgonda, Telangana, India. His interests includes Object Oriented Programming, Operating System, Database Management System, Computer Networking, Cloud Computing and Software Quality Assurance.

Mr. N.Sai Krishna received B.Tech Degree from Nalgonda Institute of Technology & Science in Nalgonda. He is currently pursuing M.tech Degree in Computer Science and Engineering specialization in Nalgonda Instituite of Technology & Science in Nalgonda, Telangana, India.

Signature Scheme and Its Identity-based Variant, International Journal of Network Security, 6(1):82-93, January, 2008.

[22] V. Goyal, O. Pandey, A. Sahai and B. Waters, *Attribute-based Encryption for Fine-grained Access Control of Encrypted Data*, In ACM CCS'06, 2006.

[23] J. Li, M.H. Au, W. Susilo, D. Xie and K. Ren, *Attribute-based Signature and its Applications*, In ASIACCS'10, 2010.

[24] PBC Library, *http://crypto.stanford.edu/pbc/times.html*.

[25] B. Riedl, V. Grascher and T. Neubauer, *A Secure E-health Architecture based on the Appliance of Pseudonymization*, Journal of Software, 3(2):23-32, February, 2008