IEEE COMSOC MMTC E-Letter

Privacy-preserving Wireless Data Transmission for e-Healthcare Applications

Xiaohui Liang, University of Waterloo, Canada
Mrinmoy Barua, University of Waterloo, Canada
Rongxing Lu, University of Waterloo, Canada
Xuemin (Sherman) Shen, University of Waterloo, Canada
{x27liang, mbarua, rxlu, xshen}@bbcr.uwaterloo.ca

1. Introduction

Recent advances in body sensors and wireless communications have revealed the possibility of providing remote healthcare monitoring and fast emergency services to patients via a smart e-healthcare system. The e-healthcare system pervasively adopts electronic and portable devices, such as smart phones, to monitor, transmit, and store patient medical records, and shifts healthcare tasks from a traditional clinical environment to a pervasive patient-centered setting. Such system has been widely regarded as a potential solution to reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions. However, the e-healthcare system leads to more challenging privacy issues especially when wireless data transmission from patients to healthcare service providers is employed. To increase public acceptability from privacy-sensitive patients, it is critical to investigate their privacy requirements for various e-healthcare applications and maximally preserve patient privacy based on these requirements.

2. Patient Privacy for e-Healthcare

Patient privacy for healthcare applications has been extensively explored among government officers, research scholars and industrial investors in the past years. Government legislations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), introduce penalty rules towards the privacy violations by healthcare service providers and prompt these providers to find privacy enhancing technologies to protect medical records. However, privacy policies are often dynamic and should be defined according to system and environmental changes [1]. The current legislations are disconnected to the ever-increasing patient privacy requirements and cannot fit the emerging e-healthcare applications. For example, healthcare monitoring devices become smaller, light-weighted and smarter such that they can be easily deployed around, on or in human body. Patients are able to read their medical records directly from the devices and they require to primarily controlling the access to their privacy-sensitive records. Patient self-controllable privacy preservation has been proposed in [2,3,4], aiming to grant any healthcare service providers an access to patient medical records following patient access policies. Meanwhile, certain privacy requirements in the traditional wireless communication design also need to be extended for e-healthcare applications. These privacy requirements can be the protection of identity information, location information, and transmitted data etc. In the following, we categorize the privacy issues for e-healthcare applications into two types: data privacy and communication privacy, and present some state-of-art solutions [5,6,7,8].

3. Data Privacy

The e-healthcare applications require fine-grained access control for privacy-sensitive data (i.e., medical records). The access control must be patient-centric, since patients are able to monitor, store and transmit the data using portable devices for most cases. In other words, patients must be able to select the access policy for their own personal information and apply distinct access policies to their medical records in different situations. For example, in a normal situation they may only send their data to a remote trusted authority; whereas, in a life-threatening scenario they may want to disseminate the data around to find a helper while disclosing minimal personal information to the public. The trade-off between safety, privacy, and access control in different contextual cases is shown in Figure 1(a). The research efforts [5,6] have been devoted to attribute-based encryption (ABE) schemes for fine-grained access control without lengthy user authorization process. Such schemes encrypt a patient's medical record with an access tree, where each leaf node represents an attribute (or access role) and each non-leaf node represents a threshold value shown in Figure 1(b). An access tree can be semantically transformed to a Boolean function. If the

healthcare service provider has an attribute set that satisfies the Boolean function, he/she is able to decrypt the patient's medical record. In this way, the access to patient medical records can be controlled by patients themselves. Patients are able to choose appropriate access policies for different e-healthcare applications and only allow other users they trust to access their privacy-sensitive medical records.

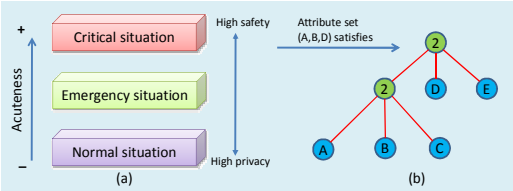


Figure 1. Trade-off and access policy

4. Communication Privacy

The communication privacy for e-healthcare is to protect multiple types of information related to communication entities, e.g., patients and healthcare service providers. Patient identity and location information are most critical and they must be protected from unauthorized entities by default unless patients allow the disclosure for special purposes. In [7], the multiple pseudonym technique is adopted to attain identity privacy preservation and location privacy preservation. The basic idea is to require patients to frequently change the pseudonyms that are used for authentication. Since other users cannot link the pseudonyms to the real identities of patients, patient' identities cannot be retrieved from the communications. Moreover, as the pseudonyms are generated independently, the transactions from one patient are not linkable and any other users cannot trace the patient's behaviors.

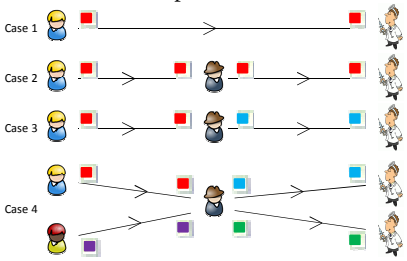


Figure 2. Several contextual privacy cases

Another contextual privacy [8] has also been addressed for the wireless data transmission of e-healthcare applications. To preserve contextual privacy, the communication protocols must resist an attack which aims to link the source and the destination of a transaction. If an adversary is able to do so, the relations between patients and healthcare service providers will be exposed and the patient medical conditions might be revealed. In [8], a mix technique is utilized to resolve this problem. The main idea is to cut off the relation between the input and the output. As shown in Figure 2, the contextual privacy of Cases 1 and 2 is easily violated since an adversary can link the patient with the healthcare services provider by simply comparing the contents in the transactions. For Case 3, a relay user re-randomizes the transaction but it cannot preserve contextual privacy since the input number and the output number are both one, and an adversary can still link them. The contextual privacy is successfully preserved in Case 4, where 2 patients and 2 healthcare service providers connect to the same relay user. The probability that the adversary has a correct observation is only 1/2. Therefore, the above mix technique can be used to preserve contextual privacy if at least a relay user has m inputs and n outputs. The parameters (m,n) should be as large as possible. Otherwise, the contextual privacy level will decrease quickly.

5. Conclusion

E-healthcare systems are very promising and attractive to both healthcare service providers and patients since they can provide long-term, real-time monitoring and fast emergency services anywhere at any time. As the transmitted data in such system is often privacy-sensitive to patients, patient privacy concerns must be well addressed. In this article, we have presented the privacy issues specifically for wireless data transmission in e-healthcare systems, and provided potential solutions to resolve these problems.

Reference

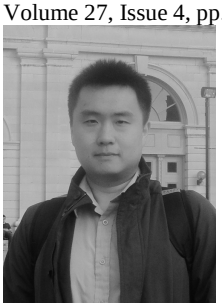
[1] A. AL Faresi, D. Wijesekera, and K. Moidu, "A Comprehensive Privacy-aware Authorization Framework Founded on HIPAA Privacy Rules," IHI'10, Arlington, Virginia, pp. 637-646, 2010.

[2] N. Huda, N. Sonehara, and S. Yamada, "A Privacy Management Architecture for Patient-controlled Personal Health Record System," Journal of Engineering Science and Technology, Vol. 4, No. 2, pp. 154-170, 2009.

[3] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Communications Magazine, Vol. 17, Issue 1, pp. 51-58, 2010.

[4] J. Sun, Y. Fang, and X. Zhu, "Privacy and Emergency Response in E-Healthcare Leveraging Wireless Body Sensor Networks," IEEE Wireless Communications Magazine, Vol. 17, Issue 1, pp. 66-73, 2010.

[5] X. Liang, R. Lu, X. Lin, and X. Shen, "Patient Self-controllable Access Policy on PHI in eHealthcare Systems", AHIC 2010, Kitchener, Ontario, Canada, 2010.
[6] M. Barua, X. Liang, R. Lu, and X. Shen, "PEACE: An Efficeint and Secure Patient-centric Access Control Scheme for eHealth Care System," IEEE Infocom Workshop on Security in Computers, Networking and Communications, pp. 970-975, Shanghai, China, 2011.
[7] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, "PEC: A Privacy-preserving Emergency Call Scheme for Mobile Healthcare Social Networks", Journal of Communications and Networks, Vol. 13, No.2, pp. 102-112, 2011 .
[8] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," IEEE Journal on Selected Areas in Communications, Volume 27, Issue 4, pp. 365-378, 2009.



Xiaohui Liang [S'10] is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include network security and privacy, applied cryptography, and e-healthcare system.

Mrinmoy Barua is now pursuing the Ph.D. degree in Electrical and Computer Engineering at the University of Waterloo, Canada. His research interests include applied cryptography, wireless network security, and security and privacy in eHealth and cloud computing.

Rongxing Lu [S'09, M'11] is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He served as an Area Editor for IEEE Transactions on Wireless Communications and Editor-in- Chief for Peer-to- Peer Networks and Applications. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society and Vehicular Technology Society.