JES
Journal of Engineering Sciences

Vol 10, Issue 12, DEC/2019
ISSN NO:0377-9254

SECURE IDENTITY-BASED DATA SHARING AND PROFILE MATCHING FOR MOBILE HEALTHCARE SOCIAL NETWORKS IN CLOUD COMPUTING: A REVIEW

[1]Mohammed Seid Yimam [2]Dr. K Suresh Babu

[1]M.Tech (SE), School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India.

[2]Associate Professor of CSE, School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Telangana, India

ABSTRACT-Profile matching, a challenging task in mobile social networks, is getting more attention in recent years.Online social networks (OSNs) have become popular around the world due to its openness. Although cryptographic techniques can provide privacy protection for users in OSNs. Cloud computing and social networks are change the way of healthcare by providing real-time data sharing in a cost-effective manner. However, data security issue is one of the major goals to the extensive application of mobile healthcare social networks (MHSN), since health information is considered to be extremely sensitive.In this paper, a secure data sharing and profile matching scheme introduced for the MHSN in cloud computing. The patients can outsource their encrypted health records to cloud storage with an identity-based broadcast encryption technique, and share them with a group of doctors in a secure and efficient manner.And then presented an attribute-based conditional data re-encryption construction, which permits the doctors to convert a cipher-text into a new cipher-text of an identity-based encryption scheme for specialist without leaking any sensitive information.

1. INTRODUCTION

Discovering and interacting with people within a certain distance according to personal preferences is a crucial service provided by mobile social networks (MSN), which is helping us to stay connected better than ever. Let us imagine the following two scenarios. (1) At the airport, a passenger wants to discover and connect with the nearby passengers who come from the same university. (2) In the hospital, a patient wants to find similar patients according to their disease symptoms and medications for physical or mental support. In MSN, all such requirements can be satisfied by user profile matching very quickly and accurately. Generally speaking, user profile is a set of attributes generated by users to describe themselves for special friending purpose when they join social networks. For example, in the first scenario, the user profile of a passenger may include his/her age, sex, university from which he/ she graduated, company in which he/she is working and his/her destination, etc. In the second scenario, the user profile of a patient may include his/her disease symptoms, medications being taken and his/her doctor, etc. The meaning of "matching" can be defined from different perspectives.

Personal health records (PHRs) are the electronic records containing health and medical information of patients, which involves privacy information that patients are unwilling to disclose. Thus, the security and protection of PHR have been of great concern and a subject of research over the years. Mobile healthcare is an innovative combination of mobile devices and mobile communication technologies, for it can provide required health information, usual care improvements, potential infectious disease prevention, health interventions, etc. It is getting more and more widely to apply the emerging cloud

computing technology into the fields of mobile healthcare. By using mobile healthcare system, the electronic health record (EHR) can be transmitted through the network to the cloud service provider (CSP) for remote storage.

Moreover, the healthcare providers can read it from an end device or access it remotely using a mobile device to provide real-time medical treatment [1]. Meanwhile, people tend to distribute and disseminate the healthcare information via social networks, since social media is an extension of the healthcare professional and patient relationship. Consequently, mobile healthcare social networks (MHSN) are created for connecting patients so that they could distribute healthcare information using their mobile devices, and also connecting doctors and specialists for better healthcare. For example, people in MHSN can communicate and interact with each other before making healthcare decision.

However, data security issues are the major obstacles to the application of MHSN [2]. As we all know, health information such as treatment and drug information is considered to be highly sensitive. If these data are outsourced to the CSP, the patients cannot directly control the software or hardware platform for storing data. Without careful consideration, patients may suffer serious medical information leakage from the cloud. For example, millions of EHRs have beencompromised in recent years. Hence, it is significant that the EHRs should be stored in an encrypted form. Even if the CSP is untrusted or compromised, the data maintains security and privacy. Simultaneously, the encrypted records should be shared and accessed in a reasonable way.

By using identity-based PRE (IBPRE), the specialist in MHSN can access the EHRs without the CSP getting any useful information. The MHSN also provides strong social interconnection functions since the patients can communicate with others. Specially, patients can find similar patients with the profile matching mechanism and communicate their illness symptoms and medications. However, the patients may disclose their sensitive health information to other users, including the users being matched with. Therefore, it is essential to protect the patients' personal information during the match process, otherwise malicious users may easily collect and use this information. Recently, many researchers have applied the equality test technique to achieve profile matching in cloud and social networks. However, there might be keywords guessing attack, especially in the medical system with limited keywords. Therefore, the attack is more likely to be successful in MHSN and may cause serious privacy leakage.

2. RELATEDWORK

PAAS: A Privacy-Preserving Attribute-based Authentication System for eHealth Networks [1]

Recently, eHealth systems have replaced paper based medical system due to its prominent features of convenience and accuracy. Also, since the medical data can be stored on any kind of digital devices, people can easily obtain medical services at any time and any place. However, privacy concern over patient medical data draws an increasing attention. In the current eHealth networks, patients are assigned multiple attributes which directly reflect their symptoms, undergoing treatments, etc. Those life-threatened attributes need to be verified by an authorized medical facilities, such as hospitals and clinics. When there is a need for medical services, patients have to be authenticated by showing their identities and the corresponding attributes in order to take appropriate healthcare actions. However, directly disclosing those attributes for verification may expose real identities. Therefore, existing eHealth systems fail to preserve patients' private attribute information while maintaining original functionalities of medical services. To solve this dilemma, they proposed a framework called PAAS which leverages users' verifiable attributes to authenticate users in eHealth systems while preserving their privacy issues. In their system, instead of letting centralized infrastructures take care of authentication, our scheme only involves two end users. they also offer authentication strategies with progressive privacy requirements among patients or between patients and physicians. Based on the security and efficiency analysis, they showed their framework is better than existing eHealth systems in terms of privacy preservation and practicality.

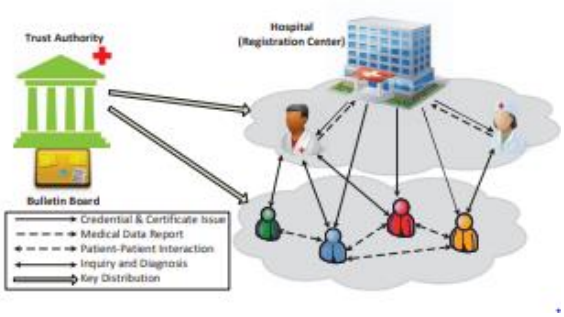

Fig.1: Distinct Patients in eHealth Networks in a Distributed Manner

In this paper, they proposed a framework of privacy-preserving attribute-based authentication system in eHealth networks. Our framework applies the non-interactive proof system as the basic building block, in which they given formal definitions of four progressive privacy levels. The attribute-based authentication schemes designed for higher privacy levels preserve the more privacy on attributes and attribute values, but cost more computation and communication resources. Based on the security analysis, we show that our scheme satisfies both the verifiability and privacy of attributes and attribute values. According to experimental results, the efficiency of different privacy levels is acceptable for laptops.

Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys [3]

This paper describes the first identity-based broadcast encryption scheme (IBBE) with constant size ciphertexts and private keys. In their scheme, the public key is of size linear in the maximal size m of the set of receivers, which is smaller than the number of possible users (identities) in the system. Compared with a recent broadcast encryption system introduced by Boneh, Gentry and Waters (BGW), their system has comparable properties, but with a better efficiency: the public key is shorter than in BGW. Moreover, the total number of possible users in the system does not have to be fixed in the setup.

They introduced the first identity-based broadcast encryption (IBBE) scheme with constant size ciphertexts and private keys. One interesting open problem would be to construct an IBBE system with constant size ciphertexts and private keys that is secure under a more standard assumption, or which achieves a stronger security notion, equivalent to full security in IBE schemes.

ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing[7]

They consider the problem of patient self-controlled access privilege to highly sensitive Personal Health Information (PHI), where PHI is expected to be securely stored in cloud storage for uninterrupted anytime, anywhere remote access. In order to assure the privacy of PHI, we propose Efficient and Secure Patient-centric Access Control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles, and then assigns different attribute sets to them. Extensive security and performance analyses demonstrate that the ESPAC scheme is able to achieve desired security requirements with acceptable communication delay.

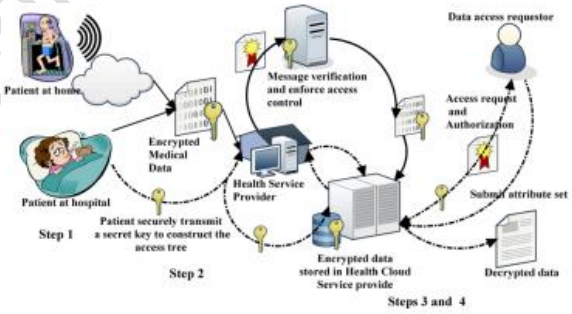

Fig.2: Major steps of the ESPAC scheme

In this paper, they have proposed a scheme, ESPAC, to achieve patient-centric access control with security and privacy by exploiting attribute-based encryption. Moreover ESPAC enables the eHealth care service provider to reduce the overall maintaining cost by moving data to a centralized storage or cloud storage for further processing and long-term storage. Moreover, storing PHIs in the cloud storage provides anytime, anywhere access to stored patient's health information. The proposed scheme also preserves user privacy with data integrity. Through detailed security and performance analyses, it has been demonstrated that the proposed scheme is highly efficient to resist various possible attacks and malicious behaviour. In our future work, they will

extend the proposed scheme to support encrypted keyword search in cloud computing.

Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing [8]

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when finegrained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in finegrained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

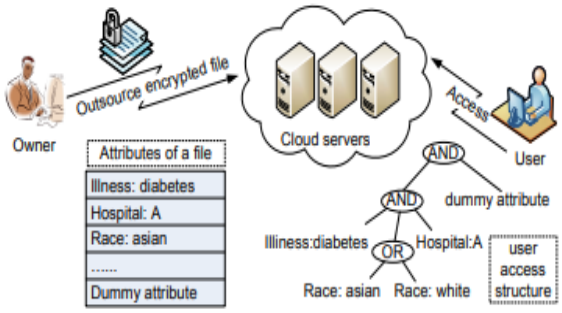

Fig.3: An exemplary case in the healthcare scenario

This paper aims at fine-grained data access control in cloud computing. One challenge in this context is to achieve finegrainedness, data confidentiality, and scalability simultaneously, which is not provided by current work. In this paper we propose a scheme to achieve this goal by exploiting KPABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption. Moreover, our proposed scheme can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved. Formal security proofs show that our proposed scheme is secure under standard cryptographic models.

3.FRAMEWORK

Many encryption schemes were proposed to protect data security in mobile healthcare system. Li et al. [6] presented an access control framework through EHRs that utilizes ABE to encrypt each patient's data. Barua et al. [7] proposed ESPAC which also utilizes ABE to achieve patient-centric access control. Yu et al. [8] exploited key-policy ABE (KP-ABE) technique to protect the EHRs in cloud computing. Although ABE can encrypt the data and achieve fine-grained access control over the cipher-text, it suffers from the inconvenience of heavy computation cost in encryption and decryption phases.In order to protect data confidentiality and availability, and also preserve the patients' privacy in MHSN, encryption techniques must be adopted. In this study, a secure and efficient data sharing and profile matching scheme for MHSN in cloud computing is introduced.

A secure identity-based data sharing scheme for MHSN is proposed, which allows patients to outsource their encrypted health records to CSP with IBBE technique, and share them with a group of doctors in a secure and efficient manner. And also presented an attribute-based conditional data re-encryption construction, which permits doctors who satisfy the pre-defined conditions in the ciphertext to authorize the CSP to re-encrypt the ciphertext for specialist, without leaking any sensitive information. It provide an efficient profile matching mechanism in MHSN based on IBE with equality test (IBEET) that helps patients to find friends in a privacy-preserving manner.

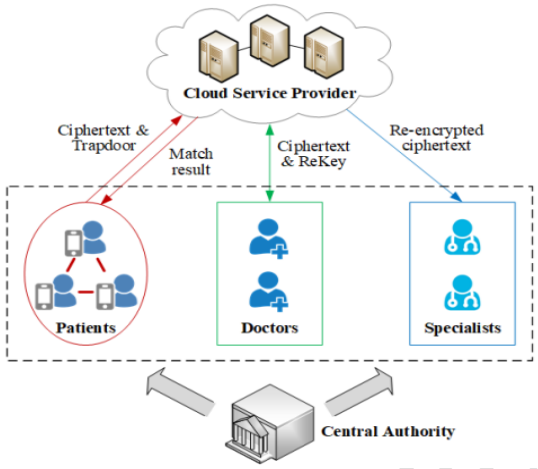

Fig.4: Framework

Here proposed secure identity-based data sharing and profile matching model for MHSN in cloud computing is shown in Fig. 4, including five entities: central authority, CSP, patient, doctor and specialist.

(1) Central authority: The central authority is trusted for initializing the system and generating attribute keys and secret keys for participating users.

(2) CSP: The CSP is responsible for data storage and can be acted as a proxy as it is semi-trusted. Besides, the CSP performs the profile matching for patients.

(3) Patient: The patients register the system to obtain their secret keys with their identities. They encrypt the EHRs using IBBE algorithm and outsource the ciphertexts to CSP, hence only authorized doctors could decrypt them. Simultaneously, patients with the same symptom can generate trapdoors and form social relationships according to their wills.

(4) Doctor: The authorized doctors can decrypt the patients' ciphertext that stored in the CSP. When encountering a problem that needs to negotiate with a specialist, the doctor can generate a re-encryption request, thus the CSP converts the ciphertext into an IBE-encrypted data for specialist if the doctor satisfies the pre-defined conditions in the ciphertext.

(5) Specialist: The specialist could decrypt the re-encrypted ciphertext with the secret key and then assist doctors for advice.

Algorithm Description:

An IBE scheme consists of the following algorithms.

(1) (MK; PK) ←Setup(1λ). The setup algorithm inputs a security parameter λ, and outputs the master secret key MK and public parameters PK.

(2) SK ←KeyGen(MK, PK, ID). The key generation algorithm inputs the master secret key MK, public parameters PK and an identity ID. It outputs a secret key SK.

(3) CT ←Enc(ID, PK, M). The encryption algorithm inputs an identity ID, public parameters PK and a plaintext M. It outputs a ciphertext CT.

(4) M ←Dec(SK, PK, CT). The decryption algorithm inputs a secret key SK, PK and a ciphertext CT, and outputs M.

4. CONCLUSION

The MHSN has improved the healthcare through its convenient data sharing. For the purpose of guaranteeing data confidentiality and availability in MHSN, here proposedan secure identity-based data sharing and profile matching scheme in cloud computing. First realizedthat the secure data sharing in MHSN with IBBE cryptographic technique, which allows the patients to store EHRs to cloud securely and share them with a group of doctors efficiently. Then presented an attribute-based CPRE mechanism in MHSN, which allows doctors who satisfy the pre-defined conditions to authorize the cloud to convert a

stored cipher-text into a new cipher-text under IBE for the specialist, without leaking any sensitive information.

5. FUTURE WORK

In this review further provides a profile matching mechanism based on IBEET, which can achieve flexible authorization on encrypted EHRs and help patients to find friends in a privacy-preserving and efficient way. The analysis and results show that the computation cost on patient side is reduced.

REFERENCES

[1] L. Guo, C. Zhang, J. Sun, and Y. Fang, ‘‘PAAS: A privacy-preserving attribute-based authentication system for eHealth networks,’’ in Proc. 32nd Int. Conf. Distrib. Comput. Syst., Macau, China, Jun. 2012, pp. 224–233.

[2] A. Abbas and S. U. Khan, ‘‘A review on the state-of-the-art privacypreserving approaches in the e-health clouds,’’ IEEE J. Biomed. Health Informat., vol. 18, no. 4, pp. 1431–1441, Apr. 2014.

[3] C. DelerablØe, ‘‘Identity-based broadcast encryption with constant size ciphertexts and private keys,’’ in Proc. 13th Int. Conf. Theory Appl. Cryptol. Inf. Secur., Kuching, Malaysia, 2007, pp. 200–215.

[4] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2007, pp. 321–334.

[5] M. Green and G. Ateniese, ‘‘Identity-based proxy re-encryption,’’ in Proc. 5th Int. Conf. Appl. Cryptogr. Netw. Secur., Zhuhai, China, 2007, pp. 288–306.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[7] M. Barua, X. Liang, R. Lu, and X. Shen, ‘‘ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing,’’ Int. J. Secur. Netw., vol. 6, nos. 2–3, pp. 67–76, 2011.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in Proc. IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[9] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, ‘‘Secure and fine-grained access control on e-healthcare records in mobile cloud computing,’’ Future Gener. Comput. Syst., vol. 78, pp. 1020–1026, Jan. 2017.

[10] Y. Yang, X. Liu, R. H. Deng, and Y. Li, ‘‘Lightweight sharable and traceable secure mobile health system,’’ IEEE Trans. Dependable Secure Comput., to be published, doi: 10.1109/TDSC.2017.2729556.

[11] Y. Yang, X. Liu, and R. H. Deng, ‘‘Lightweight break-glass access control system for healthcare Internet-of-Things,’’ IEEE Trans. Ind. Inform., to be published, doi: 10. 1109/TII.2017.2751640.

[12] G.-C. Li, C.-L. Chen, H. C. Chen, F. Lin, and C. Gu, ‘‘Design of a secure and effective medical cyber-physical system for ubiquitous telemonitoring pregnancy,’’ Concurrency Comput. Pract. Exper., vol. 30, no. 2, p. e4236, 2018.

[13] C. C. Tan, H. Wang, S. Zhong, and Q. Li, ‘‘IBE-lite: A lightweight identitybased cryptography for body sensor networks,’’ Trans. Inf. Technol. Biomed., vol. 13, no. 6, pp. 926–932, Jun. 2009, doi: 10.1109/titb.2033055.

[14] X. An Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, ‘‘Cost-effective secure E-health cloud system using identity based cryptographic techniques,’’ Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.

[15] M. Blaze, G. Bleumer, and M. Strauss, ‘‘Divertible protocols and atomic proxy cryptography,’’ in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., Espoo, Finland, 1998, pp. 127–144.