IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

A Mobile Health Care Social Networks In Cloud Computing Based On Secure Identity Based Data Sharing and Profile Matching

A. Apoorva[1*], K.Amoolya[2], K. Anil[3], M.Guruprasad[4], Vinodh H N[5]

[1,2,3,4,5]Dept. of Computer Science, East West Institute of technology, Vishveswaraya Technological University, Bangalore, India

DOI: https://doi.org/10.26438/ijcse/v7si15.5458 | Available online at: www.ijcseonline.org

***Abstract*—**Cloud computing and social networks are providing real time data sharing by changing the way of healthcare in a cost-effective manner. However, data security issue is one of the main obstacles of mobile healthcare social networks (MHSN), since health information is considered to be highly sensitive and securable. In this paper, we introduce a mobile health care social networks in cloud computing based on profile matching and data sharing. The patients can outsource their encrypted health records to cloud storage with identity-based broadcast encryption (IBBE) technique, and share them with a group of doctors in a secure and efficient manner with domains and sub domains.

***Keywords*—**conditional proxy re-encryption, data security, encryption, health information management, profile matching.

I. INTRODUCTION

MOBILE healthcare is an innovative combination of mobile devices, servers and mobile communication technologies, for it can provide necessary health information, routine care improvements, hospital information, doctor specialization and health interventions, etc. It is getting more and more widely to apply the emerging cloud computing technology into the fields of mobile healthcare and to share the data within the cloud to patients and doctors. The electronic health record (EHR) can be transmitted over the network to the cloud service provider (CSP) for remote storage by using mobile healthcare system. Moreover, the healthcare providers can read it and share it from an end device or access it remotely using a mobile device to provide real-time medical treatment and consult doctors. Data security issues are the major problems to the application of MHSN. Highly sensitive data is health information such as treatment and drug information. The patients cannot directly control the software or hardware platform for storing the data, if these data are outsourced to the CSP. Without careful consideration of data security, patients may suffer serious medical information leakage from the cloud and results insecurity in patients to share their data in future. Currently, there have been many techniques utilized to protect data security in MHSN, such as public-key encryption (PKE), identity-based encryption (IBE), identity-based broadcast encryption (IBBE) and attribute-based encryption (ABE). Recently, equality test technique is used in many researchers to achieve profile matching in cloud and social networks. However, keywords guessing attack especially in the medical system with limited keywords is the possible attack on the data. Therefore, the attack is more likely to be successful in MHSN and may cause serious privacy leakage and insecuity. In order to protect data confidentiality, security and availability, and also preserve the patients' privacy in MHSN, techniques should be adopted for the encryption. In this study, a mobile health care social networks in cloud computing for secure and efficient data sharing and profile matching scheme is introduced. The contributions are summed up as follows.

(1) 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 and hospitals in a secure and efficient manner.

(2)An attribute-based conditional data re-encryption construction is presented which permits doctors who satisfy the pre-defined conditions in the ciphertext to authorize the Cloud Service Provider to re-encrypt the ciphertext for specialist, without leaking any sensitive information.

(3) An efficient profile matching mechanism in MHSN based on IBE with equality test (IBEET) is provided, that helps patients to share data in a privacy-preserving manner, and achieve flexible authorization on the encrypted health records with resisting the attacks on data.

II. RELATED WORK

A. Health Records Encryption

EHRs should be encrypted to guarantee data confidentiality is a fundamental security requirement of MHSN. Many encryption schemes were proposed to protect data security and confidentiality in mobile healthcare system. An access control framework over EHRs is presented by Li et al. [1], that utilizes ABE to encryptioneach patient's data. ESPAC which also utilizes ABE to achieve patient-centric access control is proposed by Barua et al. [2]. Key-policy ABE (KP-ABE) technique to protect the EHRs in cloud computing is exploited by Yu et al. [3]. Although ABE can encrypt the data and achieve fine-grained access control over the ciphertext, heavy computation cost in encryption and decryption phases suffers from the inconvenience. With the case of resource-limited healthcare devices, such as wearable devices and mobile terminals it becomes even worse. An outsourced EHR access control scheme which allows data owner to complete most of encryption computation in advance introduced by Liu et al[4]. and then generate the ciphertext with very low computation cost. Similar with this scheme, the recent ABE-based schemes [5,6] also outsourced most of the expensive cryptographic computations to the CSP to reduce computational overhead of user-side.

B. Identity-Based Proxy Re-encryption

Blaze et al.proposed the cryptographic algorithm PRE for secure data dissemination[7]. Especially, IBPRE allows a proxy to transform a delegator's ciphertext into a delegate's ciphertext. Green and Ateniese[8]established The first IBPRE in which is proved to be chosen ciphertext attack (CCA) secure. a new PRE systems was proposed by Matsuo[9] which can convert a ciphertext encrypted using a traditional PKE scheme to a ciphertext encrypted by IBE scheme. An IBPRE construction was proposed by Zhou et al[10]. which allows the proxy to convert a ciphertext of an IBBE scheme into a ciphertext of an IBE scheme. Recently, Wang et al.[11]showed how to integrate IBPRE into healthcare system in cloud computing, in which the doctors can delegate a key to the CSP so that the stored ciphertext can be transformed into a new one for the planned specialist. However, the above mentioned PRE-based schemes could not control the process of data re-encryption and secure it. The first conditional PRE (CPRE) construction[12] was proposed by Weng et al. that encrypts data with a key condition, and re-encrypts the ciphertext only if the key meets this defined condition. A conditional identity-based broadcast PRE scheme in cloud computing was proposed by Xu et al.[13], which can transform an IBBE ciphertext into another IBBE cipher text if the condition is satisfied.

C. *Profile Matching in Cloud and Social Networks*

Profile matching is an efficient method of comparing different users' personal profiles in cloud and social networks and this can be used with respect to patient profile comparison and giving out results. However, the user's profile may contain sensitive information, so attention should be paid to security and ensure that private information is not leaked. Two mainstreams of ways were proposed. The first way considers the user portfolio as a set of attributes. It uses private set intersection to achieve attribute matching based on secret sharing and homomorphic encryption and generates encrypted result. In order to exchange the minimal private data information of participating users in system, Li et al [14] utilized secret sharing technique to help the user to find friend whose profile best matches with her from a group of users or any other entity. The second way measures the social presence by taking the user profile as a vector. A private matching protocol in mobile social networks is proposed by Zhang et al.[15], which allows subtle difference between users and supports a wide range of matching schemes for matching metrics. A new privacy-preserving configuration profile matching mechanism is proposed by Zhang et al. [15] based on symmetric encryption without any trusted third party.

METHODOLOGY

A. System Model

The proposed secure identity-based data sharing and profile matching model for MHSN in cloud computing is shown in Fig. 1, including five bodies: central authority, CSP, patient, doctor and specialist.

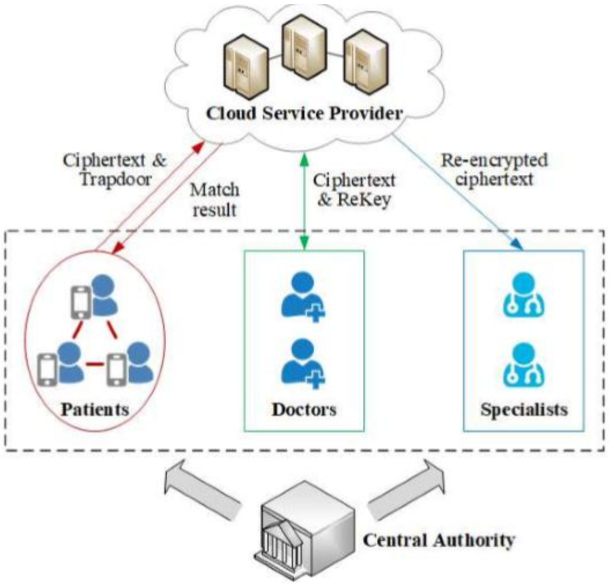

Fig 1: System model

(1) **Central authority.** The central authority is trusted for initializing the system and generating attribute keys and secret keys for participating patients and doctors. It plays an significant role in implementation and operations of keys.

(2) **CSP.** The CSP is responsible for data storage and can be acted as a proxy as it is semi-trusted, it is represented by itself. Besides, the CSP performs the profile matching for patients to match with respective patient. They offer network services, business and infrastructure in cloud. They

are hosted in data center so that different sectors can access them.

(3) **Patient.** The patients register with the system to obtain their secret keys with their identities. The secret keys are being sent to the respective email id patient is registered with. They encrypt the EHRs using IBBE algorithm and externalizing 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 and retrieve data. They can only be authorized by central authority. 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. They are divided by sub domains.

B. Flexible Authorization

In order to control the various attacks on data like keywords guessing attack and strengthen the privacy protection and give full security, flexible authorization is considered in our scheme. Authorization can be described in three possible ways ,they are:

(1) User to user authorization. A and B generate trapdoors on their all ciphertexts respectively.They will consider security as priority.

(2) User to cipher text authorization. A generates a trapdoor on her all cipher text, while B generates a trapdoor on his specific cipher text. Similar symptoms are considered to use as trapdoors by both A and B and sent to CSP.

(3) Ciphertext to ciphertext authorization. A and B may have more than one symptom. They generate a trapdoor on one of their ciphertexts according to their inclinations.

III. SECURITY ANAYLSIS

Theorem 1. We build an algorithm B which interacts with A to break the selective CCA-security of IBBE scheme, if an adversary A breaks our scheme
Proof. The adversary β can question the re-encryption for the chosen identity sets. In order to respond to the ReKeyGen questions of β, to get the requested re-encryption keys algorithm B needs to call the key generation oracle of IBBE scheme and then run the ReKeyGen algorithm with the output keys. With the proof in and the security of ABE, B cannot respond by giving the questioned key if it is queried by β to generate a re-encryption key for the challenge identity. In our scheme, if β has an advantage in breaking the CCA-security, B can break the security of IBBE with this advantage.

Theorem 2. To provide security, our scheme is collusion-resistant against colluding doctors based on the security of ABE.
Proof. To re-encrypt the ciphertext stored in CSP, the authorized doctor must recover (e g h)$^{\alpha t}$. If a patient has enough attribute and, if an attacker does not hold enough attributes, he may run DecryptNode algorithm with some colluding patient's re-encryption key RK. However, the RK is generated by using random and unique α defined by trusted central authority. Hence, the attacker cannot produce the correct C_2^1 and the re-encrypted ciphertext by collusion attack.

Theorem 3.To provide security, our scheme is one-way chosen-ciphertext secure against a chosen identity attack (OW-ID-CCA).
Proof. As proved, if βis an OW-ID-CCA dispute that has advantage against our scheme, then there is a one-way chosen-ciphertext security (OW-CCA) dispute B that has advantage against PKE scheme. Hence,on PKE scheme the OW-ID-CCA attack on our scheme can be converted to an OW-CCA attack. However,under bilinear Diffie-Hellman assumption, the PKE scheme is OW-CCA secure, thus our scheme is OW-ID-CCA secure, which guarantees that during the test processthe ciphertexts cannot be decrypted by CSP during the test process.

IV. PERFORMANCE ANALYSIS

To evaluate the performance, we implement the proposed system with java pairing-based cryptography library.
With Intel Core CPU @ 2.70 GHz, 8 GB memory the experiments are conducted on a Windows platform. Since the encryption computation time is mainly related to N_a and N_u, we evaluate the impact of these two factors on the computation cost respectively by setting one of the factors as a fixed value. The results are shown in Fig. 2, and confirm the fact that the Enc algorithm of our scheme performs linear computations with the Na and Nu. The computation cost with 5 doctors and 20 attributes is about 960 ms, while the computation cost with 5 attributes and 20 doctors is about 670 ms, which is realistic and should be enough to meet the complex requirement of data access control in MHSN. The experimental result of re-encryption phase is showed in Fig. 3, fig 3 shows the computational time of ReEnc varies linearly with N_a and N_u in the CT.

Obviously, the computation time grows at a faster pace with the increasing of N_a than with the increasing of N_u. It is reasonable because more pairing operations will be required in the re-encryption phase, as $N_a$increases.

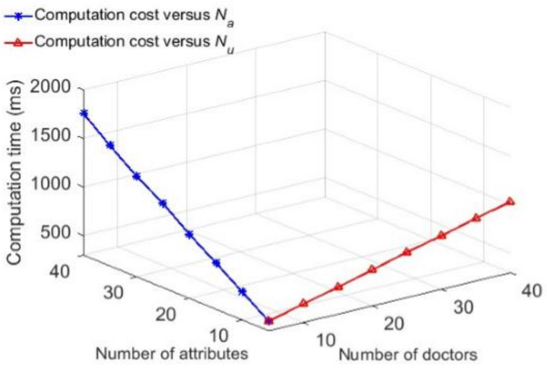

Fig 2. Computation cost of encryption

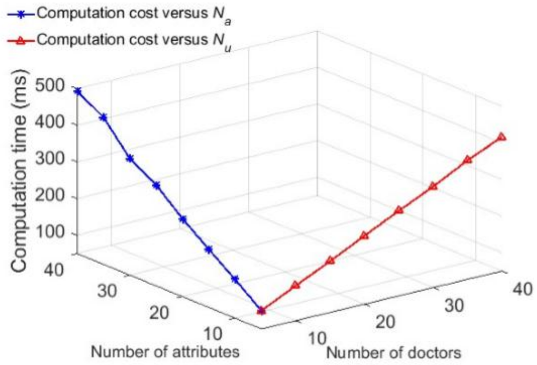

Fig. 3. Computation cost of re-encryption

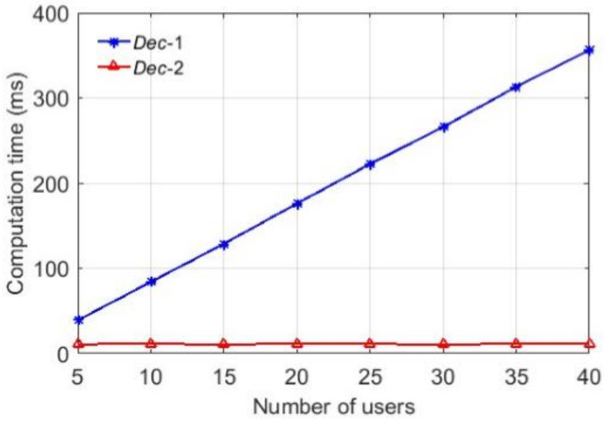

Fig. 4. Computation cost of decryption

Fig. 4 explains the computation time on the user side by decrypting the initial ciphertext and re-encrypted ciphertext. It is obvious thatthe computation time to decrypt the re-encrypted ciphertext is almost constant, which takes about 11 ms, and the computation time to decrypt the initial ciphertext is increasing with N_u.

VI. CONCLUSION AND FUTURE SCOPE

The MHSN has helped to improve the healthcare and life of patient through its convenient data sharing. We propose a secure identity-based data sharing and profile matching scheme in cloud computing for the purpose of guaranteeing data confidentiality and availability in MHSN, we first realize secure data sharing in MHSN with IBBE cryptographic technique is more secure, which allows the patients to store their EHRs to cloud securely and share them with a group of doctors efficiently. Then an attribute-based CPRE mechanism in MHSN is presented, which allows doctors who satisfy the pre-defined conditions to authorize the cloud to convert a stored ciphertext into a new ciphertext under IBE for the specialist, without disclosing any sensitive information. Further, we provide a profile matching mechanism to match the patient identity based on IBEET, which can achieve flexible authorization on encrypted EHRs and help patients to find friends and relatives in a privacy-preserving and efficient way. Using MHSN, the analysis and results show that the computation cost on patient side is reduced and is more convenient.

REFERENCES

[1] 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 on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013.

[2] M. Barua X. Liang, R. Lu and X. Shen, “ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing,” International Journal of Security and Networks, vol. 6, no. 2/3, pp. 67-76, Nov. 2011

[3] S. Yu, C. Wang, K. Ren and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. 29th Conference on Information Communications, San Diego, CA, USA, 2010, pp. 534-542

[4] Y. Liu, Y. Zhang, J. Ling and Z. Liu, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing,” Future Generat.Comput. Syst., vol. 78, pp. 1020-1026, Jan. 2017.

[5] Y. Yang, X. Liu, R. Deng and Y. Li, “Lightweight sharable and traceable secure mobile health system,” IEEE Trans. Depend. Sec Comput., Jul. 2017. [Online]. Available: https://doi.org/10.1109/TDSC.2017.2729556

[6] Y. Yang, X. Liu and R. Deng, “Lightweight break-glass access control system for healthcare internet-of-things,” IEEE Transactions on Industrial Informatics, Sept. 2017.[Online]. Available: https://doi.org/10. 1109/TII.2017.2751640

[7] M. Blaze, G. Bleumer and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Advances in Cryptology - EUROCRYPT' 98, Espoo, Finland, 1998, pp. 127-144.
[8] M. Green, G. Ateniese, “Identity-based proxy re-encryption,” in Proc. the 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, 2007, pp. 288-306.
[9] T. Matsuo, “Proxy re-encryption systems for identity-based encryption,” in Proc. 1st International Conference on Pairing-Based Cryptography, Tokyo, Japan, 2007, pp. 247-267.
[10] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu and Y. Ding, “Identity-based proxy re-encryption version 2: Making mobile access easy in cloud,” Future Generat. Comput. Syst., vol. 62, pp. 128-139, Sept. 2016.
[11] X. Wang, J. Ma, F. Xhafa, M. Zhang and X. Luo, “Cost-effective secure E-health cloud system using identity based cryptographic techniques,” Future Generat.Comput. Syst., vol. 67, pp. 242-254, Feb. 2017.
[12]J. Weng, R. Deng, X. Ding, C. Chu and J. Lai, “Conditional proxy re-encryption secure against chosen-ciphertext attack,” in Proc. 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, 2009, pp. 322-332.
[13] P. Xu, T. Jiao, Q. Wu, W. Wang and H. Jin, “Conditional identity-based broadcast proxy re-encryption and its application to cloud email,” IEEE Transactions on Computers, vol. 65, no. 1, pp. 66-79, Jan. 2016.
[14] R. Zhang, J. Zhang, Y Zhang, J. Sun and G. Yan, “Privacy-preserving profile matching for proximity-based mobile social networking,” IEEE J. Sel. Areas Comm., vol. 31, no. 9, pp. 656-668, Sept. 2013.
[15]L. Zhang, X. Li, K. Liu, T. Jung and Y. Liu, “Message in a sealed bottle: Privacy preserving friending in mobile social networks,” IEEE Trans. Mob. Comput., vol. 14, no. 9, pp. 1888-1902, Sept. 2015.

Authors Profile

Ms. Apoorva A, BE, Department of Computer Science and Engineering, East West Institute of Technology.

Ms.Amoolya , BE, Department of Computer Science and Engineering, East West Institute Of Technology.

Mr.K.Anil , BE, Department of Computer Science and Engineering, East West Institute of Technology.

Mr.Guruprasad M, BE, Department of Computer Science and Engineering, East West Institute of Technology.

Prof.Vinodh H N, BE, MTech, Assistant Professor, Department of Computer Science and Engineering, East West Institute of Technology.