International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

IBBE OVER HEALTHCARE IN SOCIAL NETWORKS

[1]Ms.K.Shanthi,[2] Mr.P.Babu,

[1,2] Assistant Professor,Dept. of CSE,
Malla Reddy Engineering College (Autonomous), Secunderabad, Telangana State

Abstract

Cloud computing and social networks are changing the way of healthcare by providing real-time data sharing in a cost-effective manner. However, data security issue is one of the main obstacles to the wide application of mobile healthcare social networks (MHSN), since health information is considered to be highly sensitive. In this paper, we introduce a secure data sharing and profile matching scheme for MHSN in cloud computing. 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. We then present an attribute-based conditional data re-encryption construction, which permits the doctors who satisfy the pre-defined conditions in the ciphertext to authorize the cloud platform to convert a ciphertext into a new ciphertext of an identity-based encryption scheme for specialist without leaking any sensitive information. Further, we provide a profile matching mechanism in MHSN based on identity-based encryption with equality test that helps patients to find friends in a privacy-preserving way, and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attack. Moreover, this mechanism reduces the computation cost on patient side. The security analysis and experimental evaluation show that our scheme is practical for protecting the data security and privacy in MHSN.

Keywords: - MHSN, Encryption, Cloud Storage

1. INTRODUCTION

Mobile healthcare is an innovative combination of mobile devices and mobile communication technologies, for it can provide necessary health information, routine 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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

record (EHR) can be transmitted over thenetwork 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. Meanwhile, people tend to share 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 share 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.

2. RELATED WORK

Existing System

However, data security issues are the major obstacles to the application of MHSN. 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 been compromised 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.

Proposed System

We propose a secure identity-based data sharing scheme for MHSN, 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. We present 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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

specialist, without leaking any sensitive information. We 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, and achieve flexible authorization on the encrypted health records with resisting the keywords guessing attack.

3. IMPLEMENTATION

Central authority

The central authority is trusted for initializing the system and generating attribute keys and secret keys for participating users.

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.

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.

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.

Specialist

The specialist could decrypt the re-encrypted ciphertext with the secret key and then assist doctors for advice.

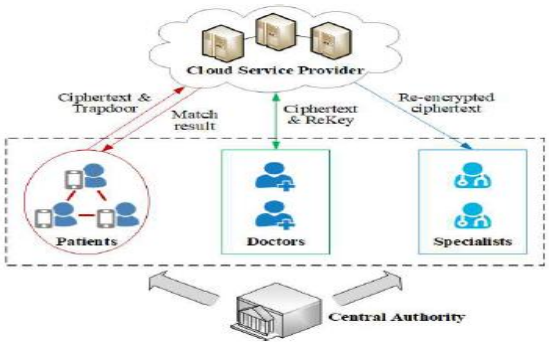

Fig:-1 System architecture

4. EXPERIMENTAL RESULTS

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

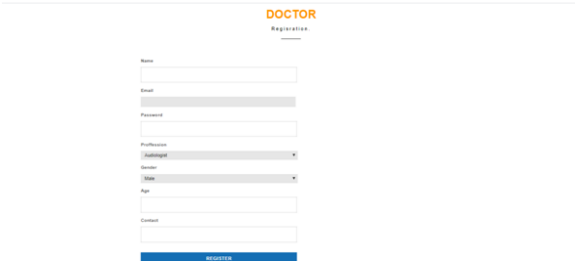

Fig:-2 Data Registration

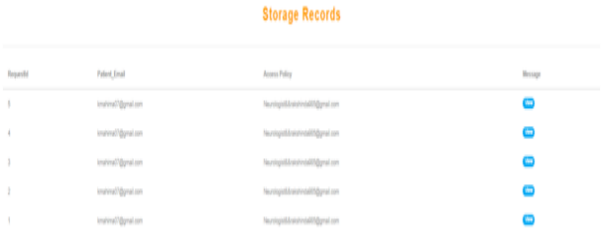

Fig:-3 Data in Cloud

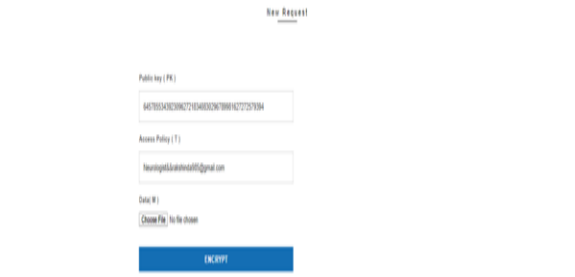

Fig:-4 Key Generation

5. 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 International Conference on Distributed Computing Systems,Macau, China, 2012, pp. 224-233.

[2] A. Abbas and S. Khan, "A Review on the state-of-the-art privacy-preserving approaches in the e-Health clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, Jul. 2014.

[3] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in Proc. 13th International Conference onthe Theory and Application of Cryptology and Information Security,Kuching, Malaysia, 2007, pp. 200-215.

[4] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policyattribute-based encryption," in Proc. 2007 IEEE Symposium on Securityand Privacy, Berkeley, CA, USA, 2007, pp. 321-334.

[5] M. Green, G. Ateniese, "Identity-based proxy re-encryption," in Proc. The5th International Conference on Applied Cryptography and NetworkSecurity, 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 attribute-based encryption," IEEE Trans on Parallel and 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," International Journal of Security and Networks, vol. 6, no. 2/3, pp. 67-76, Nov. 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. 29th Conference on Information Communications, San Diego, CA, USA, 2010, pp. 534-542.

[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 Generat.Comput. Syst., vol. 78, pp. 1020-1026, Jan. 2017.

[10] 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].