International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 6, Nov-Dec-2018, ISSN (Online): 2395-566X

# Identity-based Data Sharing and Profile Identifying For Healthcare Applications in Cloud Storage

**M.Tech.Scholar D.Param Jyothi**
Dept. of CSE
MJR College of Engg. & Tech.
Piler, AP, India

**Asst.Prof. T.Venkataramana**
Dept. of CSE
MJR College of Engg. & Tech.
Piler, AP, India

**Asst.Prof. Karamala Suresh**
Dept. of CSE
MJR College of Engg. & Tech.
Piler, AP, India

***Abstract*** **- 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, 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 allocate 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 to convert a cipher-text into a new cipher-text 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, which helps patients to find friends in a privacy-preserving way, and achieve flexible authorization on the encrypted health. Moreover, this mechanism reduces the computation cost on patient side.**

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

## I. INTRODUCTION

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.

## II. EXISTING SYSTEM

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.

It becomes even worse in the case of resource-limited healthcare devices, such as wearable devices and mobile terminals. Liu et al. [9] introduced an outsourced EHR access control scheme which allows data owner to complete most of encryption computation in advance and then generate the cipher-text with very low computation cost. Similar with this scheme, the recent ABE-based schemes [10,11] also outsourced most of the

expensive cryptographic computations to the CSP to reduce computational overhead of user-side. However, extra communication cost is inevitably brought in these schemes.

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 been compromised in recent years. Hence, it is significant that the EHRs should be stored in an encrypted form. Even if the CSP is un-trusted or compromised, the data maintains security and privacy. Simultaneously, the encrypted records should be shared and accessed in a reasonable way.

Currently, there are many techniques utilized to protect data security in MHSN, such as public-key encryption (PKE), identity-based encryption (IBE), identity-based broadcast encryption (IBBE) [3] and attribute-based encryption (ABE) [4]. In an IBBE system, broadcaster can dynamically select a specific group of users, and then encrypt the message thus only the selected users can decrypt. In an ABE system, secret key and cipher-text are associated with a set of attributes or an access policy. Although there are some schemes which apply ABE to encrypt the EHRs in MHSN, it is not convenient because of the heavy encryption and decryption cost. Let us consider a MHSN system with IBE in cloud computing, Alice may encrypt healthcare information using Doctor Bob's identity and then outsource the cipher-text to the CSP, while Bob can obtain his secret key from the trusted authority (TA) and then access Alice's health data.

In this way, IBE can achieve simple but efficient access control over the sensitive health data. However, when doctor Bob encounters an uncertain problem, he may have a consultation with a specialist for advice or treatment. Since the relevant records stored in the cloud were encrypted, the specialist cannot directly decrypt the cipher-texts. In order to solve this issue, proxy re-encryption (PRE) was employed [5], which can transform a cipher-text under Alice's identity into a cipher-text for Bob. By using identity-based PRE (IBPRE), the specialist in MHSN can access the EHRs without the CSP getting any useful information.

## III. PROPOSED SYSTEM

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.

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. Our contributions are summed up as follows.

- 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 cipher-text to authorize the CSP to re-encrypt the cipher-text for 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.

**1. Health Records Encryption**

A fundamental security requirement of MHSN is that EHRs should be encrypted to guarantee data confidentiality. In order to guarantee both secure EHRs sharing and high comprehensive performance, many IBE-based schemes were proposed in MHSN system, since the IBE mechanism can use any valid string such as unique id as the public key, and reduce the computation cost of patient. Li et al. [12] employed IBE and identity-based signature techniques to protect healthcare data in cloud computing. Tan et al. [13] developed a lightweight IBE scheme suitable for sensors for healthcare monitoring. Wang et al. [14] constructed a new IBE scheme for secure and cost-effective EHRs sharing in mobile healthcare system in cloud computing.

**2. Identity-Based Proxy Re-encryption**

The cryptographic algorithm PRE was proposed by Blaze et al. for secure data dissemination [15].

Especially, IBPRE allows a proxy to transform a delegator's cipher-text into a delegate's cipher-text.

**3. Profile Matching in Cloud and Social Networks**

Profile matching is an efficient method of comparing different users' personal profiles in cloud and social networks. However, the user's profile may contain sensitive information, so attention should be paid to ensure that private information is not leaked. Two mainstreams of ways were proposed. The first way considers the user profile as a set of attributes. It uses private set intersection to achieve attribute matching based on secret sharing and homomorphism encryption.

## IV. SCHEME OVERVIEW

**1. System Model**

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

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

**1.2 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.

**1.3 Patient-** The patients register the system to obtain their secret keys with their identities. They encrypt the EHRs using IBBE algorithm and outsource the cipher-texts 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.

**1.4 Doctor-**The authorized doctors can decrypt the patients' cipher-text 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 cipher-text into an IBE-encrypted data for specialist if the doctor satisfies the pre-defined conditions in the cipher-text.

**1.5 Specialist-** The specialist could decrypt the re-encrypted cipher-text with the secret key and then assist doctors for advice.

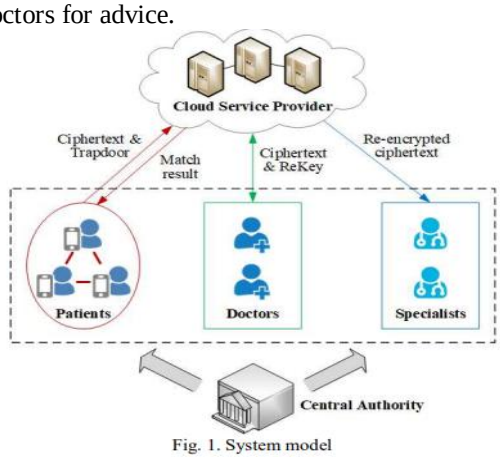


Fig. 1. System model

During the processes of data sharing in MHSN, the patients may want to make friends with others who have the same symptoms through the CSP, and they do not want to leak their private information.

## V. CONCLUSION

The MHSN has improved the healthcare through its convenient data sharing. For the purpose of guaranteeing data confidentiality and availability in MHSN, we propose a secure identity-based data sharing and profile matching scheme in cloud computing. We first realize 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 we present 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. Further, we provide 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 health 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 cipher texts and private keys," in Proc. 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2007, pp. 200-215.

[4]. J. Bethen court, A. Sahai and B. Waters, "Cipher text-policy attribute-based encryption," in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321-334.

[5]. 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.

[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.

**Author's Profile**

**D. Param Jyothi** Pursuing M.Tech at MJR College of Engineering & Technology, Department of CSE, Piler, Chittoor Dist., I Studied my B.Tech, Computer Science & Engineering in Rajiv Gandhi Memorial College of Engineering & Technology, Nandyal.

**T.Venkataramana** Working as a Assistant Professor in MJR College of engineering & technology, Department Of CSE, Piler, Andhra Pradesh.

**Karamala Suresh** Working as a Head of the Department in MJR College Of Engineering And Technology, Department Of Cse, Piler, Chittoor dist. He is having 14 years of teaching experience in engineering colleges, he received B.Tech(CSE) from JNTU Hyderabad in 2002,Received M.E(CSE) from satyabama university Chennai in 2006, and Received M.Tech (CSE) in 2015 from JNTU Anantapuramu, He is interested in Computer Networks.