A STUDY ON SECURITY MANAGEMENT FOR PATIENT HEALTH RECORDS IN HEALTH CLOUD

Dr. P.JOSEPH CHARLES, 1
HEAD, DEPT OF IT
ST. JOSEPH'S COLLEGE
TRICHY, TAMILNADU INDIA

A. PALANIAMMAL, 2
HEAD, DEPT OF BCA
SREE ARUMUGAM ARTS AND SCIENCE COLLEGE
THOLUDUR, TAMILNADU, INDIA

Abstract:

Cloud computing is a rapidly growing model of computation. It is widely used technique for data storage and data sharing on-demand but involves risk such as data security, privacy protection, and access-control and data confidentiality. In order to control access of health related data stored in public Health cloud, efficient authentication mechanism needs to be considered. To ensure high accuracy level, new variant of Hierarchal attribute-based encryption is fused with secret hash key mechanism. In this paper the proposal of HABE extends to Key Policy Attribute-Based Encryption (KP-ABE), for user revocation and user’s secret key updating is carried out by Proxy Re-Encryption (PRE) and Lazy Re-Encryption. The proposed scheme encrypts and stores data in clouds in such a way that only authorized users are able to decrypt the PHR. To reduce computational load during decryption, the decryption process is partially outsourced to a proxy server, who can gain no information about the data.

Keywords: cloud computing, Key Policy Attribute-Based Encryption, Lazy Re-Encryption, Proxy Re-Encryption

1. INTRODUCTION

Data security and Data confidential in cloud server is the major issues of the cloud computing. Most of the application’s stores the data in cloud server but the data security issues are Unsolved in cloud computing. Whenever, user wants to store perceptive information to the cloud server. The issues of Data security and Data confidential must be resolved. The Data security is resolved by using cryptographic techniques. So, that user can be outsourced the perceptive information to the cloud server and the Data confidential is resolved by setting the access privilege for the user want to access the data that stored in the cloud server. The issue of the fine-grained access is solved by setting the access privilege for the data in hierarchical order. The data in cloud server is encrypted by using cryptographic primitive(s), for the authorized user and also these authorized users disclosing decryption keys. If an Unauthorized users requested for the access of data in the cloud server are not able to decrypt since they Does not have the data decryption keys. The authorized user will encrypt the data by using public key components based on their attributes. The secret key for the user access is based on the access structure so that user able to decrypt the cipher text if satisfied the user’s data attributes access structure.

Personal health record is an emerging model which is used to store the personal health information of patients in Cloud. Through PHR, patients referred here as data owners, can share their records with friends, relatives, family members, doctors and other professional users. The doctors can easily get information regarding a patient’s health history and make emergency access if needed. PHR are stored in a third party cloud service providers which is honest but curious means, the cloud servers being honest also tries to gather information illegally. Data security and Data confidential in cloud server is the major issues of the cloud computing. Most of the application’s stores the data in cloud server but the data security issues is unsolved in cloud computing. Whenever, user wants to store perceptive information
to the cloud server. The issues of Data security and Data confidential must be resolved.

The data present in third party servers are not fully controlled by the data owners. This results in serious security and privacy issues. The PHR is divided into two domains namely public domain and private domain to reduce the complexity involved in key management. The system uses attribute based encryption (ABE) techniques to encrypt the personal records and delegate the access to the owners and share the data with users. It uses two types of ABE schemes, Key policy ABE (KPABE) and Cipher text policy ABE (CPABE), one for each domain. In personal domain, the users are related to the data owner personally like friends, family members and caretakers. The data owner directly controls the users in this domain, as they are small in number and can be easily managed. The data owner, themselves decide, which data can be viewed by the users. KPABE is used here. In public domain, the users are professionally related to data owner like doctors, researchers. They are managed by the system, as the users in public domain are huge in number and it would be tough for data owners to manage them. CPABE is used to encrypt data in public domain. In PHR unknown users may access the sensitive data; to overcome this revocation is used which is to revoke users from their access.

The ABE schemes with Central authority to grant control to users. ABE is used as the building block to express flexible access structure. These schemes have several drawbacks. Firstly, with a single central authority it is difficult the manage system with large number of users. Secondly, if the central authority fails or corrupted, the whole system will fail and the privacy and security of the data will be lost. There are lot attacks possible in PHR in

Which collusion attack is a serious cryptographic attack that demolishes the security of the system. Thus the system should ensure that no two users can combine their secret keys to gain access to unauthorized data.

2. RELATED WORKS:

In the Han et al. scheme [1] the first privacy preserving decentralized KPABE encryption algorithm is proposed. In this work, the authorities are not connected through central authority. Hence the authorities can work independently. The Global Identifier, that uniquely identifies the user in this system, is used to connect the keys of the user. Although the system reduces the overhead and other privacy issues involved with central authority, it failed to solve the collusion attack between users. The paper [2] throws light on the security failure of Han et al.’s scheme [1].

In the paper [3], Han proposed a decentralized CPABE scheme, where the users can obtain keys from multiple authorities without any cooperation between them and without central authority. The security analysis of Han’s decentralized KPABE scheme shown in [6] is also applicable to this. Hence this system is also prone to collusion attack.

Attribute-based encryption (ABE) was proposed by Sahai and Waters in [1]. Each user has a set of attributes and the message is encrypted using these attributes. Each user is also given a secret key corresponding to the access policy that it contains. If a receiver possesses a valid access policy, it can decrypt the cipher text using the secret key and obtain the information. This type of ABE is called Key-Policy ABE (KP-ABE). KP-ABE for general
monotonic access structures was studied by Goyal et al. [2]. In Cipher text-policy ABE (CP-ABE) ([6]) the message is encrypted using an access policy. The secret key is constructed using the attributes that a user possesses. If a receiver possesses a matching set of attributes, then it can decrypt the message and Obtain the plaintext. In all these cases, decryption at user’s end is computationally intensive and unsuitable for resource-constrained devices. To get over this problem, Green et al. [7] proposed to outsource the decryption task to a proxy server, which will partially decrypt the ciphertext. The user can then decrypt completely, using the limited resources that it has.

Comparison-Based Encryption (CBE) was introduced by Zhu et al. [8] in 2012. This paper handles ranged attributes and outsources decryption to enable faster decryption at the user end. This makes this scheme very attractive for resource constrained devices. If there are non-temporal attributes, then CBE is inefficient. Also, this scheme does not address user revocation, which is prevalent in large scale cloud applications like social networks, digital health records, where users join and leave often.

Chen [9] presented BestPeer++, a system which delivers elastic data sharing services for corporate network applications in the cloud based on BestPeer – a peer-to-peer (P2P) system based data management platform. This model was deployed in cloud environment as a service that uses bootstrap peers as monitors, normal peer as database engine and access control.

An adaptive query is proposed to switch between a P2P engine for small scale data to leverage fast performance on the local database engine and Map Reduce engine for large scale data in order to exploit the benefits of the Hadoop model. [14] Proposed a hybrid P2P system as a combination of a structured P2P called t-network and an unstructured P2P called s-network.

The t-network plays the role of a core transit network while the s-network stores data in the system and each s-network is attached to a peer in the t-network. The ps parameter is defined to adjust the number of peers in each of the two networks.

Altmann [10] presented a P2P file sharing topology based on social network allowing users to share resources with their friends or family. The number of peers accessing the resources based on their established relationship is, however, limited. [12] Presented a data replication approach to avoid overload of some objects as hotspots by using multiple hash functions. These hotspots are replicated to different nodes dynamically resulting in improvements in access latencies and load balancing.

In [13], authors proposed a model to distribute contents to users in an overlay network as a Constrained Stochastic Graph Process (CSGP). In [12], a secure, scalable and fine grained data access control using techniques like KPABE, proxy and re encryption has been proposed. The data files are associated with a set of attributes and each user has an access policy that is defined over those attributes. Hence KPABE is used here. In order to overcome the computation overhead incurred by the system, proxy and re-encryption techniques are used. The authors [13] proposed a ABE system that provides fine-grained sharing of encrypted data and improves the efficiency in the form of cipher text size and decryption cost i.e. cipher text is added with random hash value without increasing its size and by using verifiable ABE, it reduces the computational cost of user and cloud server, thereby reducing
Overall decryption cost. In multi authority cloud setting, the user’s attribute may be changing dynamically. The users can be assigned to new attributes or the attributes of the users may be revoked. This can be achieved by attribute revocation proposed in [15] which is proved to be secure under random oracle model.

3. METHODOLOGIES:

3.1 KEY POLICY ATTRIBUTE-BASED ENCRYPTION (KPABE)

KP-ABE is a cryptography method of the attribute based encryption (ABE). In KP-ABE, single user can request for the multiple data to cloud server. The data are associated with public key cryptography for which user attributes defined. The set of attribute is associates with encryptor’s message by which encryption is take place with the corresponding public key components. An access structure is assigned for each user’s data attribute is defined as an access tree, i.e., the leaf nodes are associated with attributes and the threshold gates of access tree is interior nodes. The access structure is reflecting in the user secret key. So that the user can able to decrypt the cipher text if it’s satisfied the data attribute access structure.

3.2 PROXY RE-ENCRYPTION (PRE):

These schemes of cryptosystems which allow third-parties (semi-trusted proxy) to alter a cipher text under Alice’s public key into another cipher text that can be opened by Bob’s private key without seeing the original plaintext. This scheme allows the semi trusted proxy, to re-encryption key rka→b, to convert cipher texts under public key pka into cipher texts under public key PKb and vice versa.

• Setup Update attributes: Data owner updates PK to PK+1 by adding each version number to 1.

3.3 LAZY RE-ENCRYPTION (LRE)

The Lazy Re-Encryption (LRE) technique which enable the Cloud Servers to aggregate multiple successive operation such as update secret key and update user attribute for re-encryption operations cloud servers to aggregate multiple operations in computation tasks. Lazy re-encryption operation decided the data to be updates to rekey. Re-encryption of lager part of the data accounts for the cost of key replacement, re-encryption is only performed for the significantly data changes after a user depart. Re-encryption prevent the highly sensitive data and from the user accessing.

Minimum cost is required for rekeying; before user departs the data must be Re-encrypting. However, if a confidential file does not change frequently, lazy re-encryption can allows the intrudes user to copy off information from the file into another file and leave the system as it. Let’s assume that if a key k requires updating, then any objects encrypted with k are available to any user who could derive k. The user u sends the new key k’ until such time as u actually requires k’ to decrypt the data.

3.4 SECURITY MANAGEMENT WITH HABE:

The key idea of the Security Management Infrastructure (SMI) is to divide the system into two domains namely public domain (PUDs) and personal domain (PSDs). The PUDs consists of user who
make access based on their professional roles, such as doctors, nurses and medical researcher. The PSD users are personally associated with a data owner such as family members or close friends and they make access to Personal Health Records based on access rights assigned by the owner. SMI uses a new Decentralized Hash key attribute based Encryption (HABE) with user revocation in Private Domain and Multi Authority Cipher text Policy Attribute Based Encryption (MACPABE) with attribute revocation in Public Domain. In revocation, Lazy revocation concept is used. The System proves to be Collusion Resistance (CR) by employing Tokenization concept in above algorithms.

The work based on the HABE access Control extends to attribute-based encryption (ABE) with Key Policy Attribute-Based Encryption (KP-ABE), Proxy Re-Encryption (PRE) and Lazy Re-Encryption.

The main operations of HABE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

1) System Setup: In this algorithm, the data owner (Patient) sets the security parameter κ and calls it. The output of Setup (k) is PK system public key and MK master key. Then the component of PK is signed by data owner and sends PK along with the data owner signature to Cloud Servers.

2) New File Creation: In this algorithm, the data owner sets the security parameter κ and calls it. The output of Setup (k) is PK system public key and MK master key. Then the component of PK is signed by data owner and sends PK along with the data owner signature to Cloud Servers.

4. PERFORMANCE ANALYSIS:

The proposed system is efficient in key generation and reduces time complexity with the existing algorithms by comparing the results obtained. The performance graphs are shown below.

Comparison of Key Generation time with other Existing Schemes:

![Graph showing comparison of key generation time](image)

The HABE models shown in Fig represent the access of data based on the hierarchical order. The hierarchical system consists of user grant; data file creation, file access, user revocation, and file deletion. The Trusted Authority Grant the access for consent Domain authority for their access. The Domain Authority add user for the access of data.
5. CONCLUSION:

Security Management is one of the essential issues in Healthcare industry. In general access control models and Encryption based techniques fail to protect health care data. A survey of existing Attribute based encryption schemes for specific healthcare industry applications is been carried out.

An innovative HABE for managing Personal Health Record in cloud is proposed. The privacy of both data owners and data users are preserved by hiding their GID from the system through Tokenization concept. From the proposed scheme it is proved system is more efficient than the existing systems in terms of features and key generation time.

REFERENCES:


