A CLOUD BASED HEALTHCARE MANAGEMENT SYSTEM USING ATTRIBUTE BASED ENCRYPTION

K.SAKTHI VIGNESWARI
VELAMMAL COLLEGE OF ENGINEERING
AND TECHNOLOGY,MADURAI.
svsakthi8@gmail.com

T.ARCHANA ,R.SHANMUGAPRIYA
VELAMMAL COLLEGE OF ENGINEERING
AND TECHNOLOGY,MADURAI

Abstract- Nowadays, cloud storages are useful to various users around the world. This motivation becomes very large for all researchers for providing effective file sharing on the cloud environment. Many existing systems are in the under research for effective sharing of files on the cloud environment. Ciphertext-policy attribute-based encryption (CPABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing .In our project, the main motivation is provide effective file sharing among all users. The ciphertext components related to attributes could be shared by the files .Therefore, both ciphertext storage and time cost of encryption are saved. This technique proposes a new effective scheme named efficient file hierarchy attribute-based encryption. Here we store the timing cost of encryption and cipher text. Our experiment is the best secure scheme under the standard assumption and experimental simulation shows proposed scheme is highly effective and more conspicuous under the encryption and decryption when a number of files increase.

Index Terms—Cloud computing, Data sharing, File Hierarchy, Ciphertext-policy, Attribute-based encryption.

Introduction

Cloud Data sharing, also called cloud-based data sharing or online data sharing, is a system in which a user is allotted storage space on a server and reads and writes are carried out over the Internet. Cloud data sharing provides end users with the ability to access datas with any Internet-capable device from any location. Usually, the user has the ability to grant access privileges to other users as they see fit. Although cloud data sharing services are easy to use, the user must rely upon the service provider ability to provide high availability (HA) and backup and recovery in a timely manner. In the enterprise, cloud data sharing can present security risks and compliance concerns if company data is stored on third-party providers without the IT department's knowledge. Popular third-party providers for cloud data sharing include Box, Drop box, Egnyte and Syncplicity.

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice features is, that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

SCOPE AND OBJECTIVE

- Enhance the file sharing in the cloud service
- Improved CP-ABE named efficient file hierarchy based encryption scheme
- Reducing the computation cost for both data owner and user

EXISTING SYSTEM

In existing system, used new versatile cryptosystem referred to as ciphertext-policy hierarchical ABE (CP-HABE). In a CP-HABE scheme, the attributes are organized in a matrix and the users having higher-level attributes can delegate their access rights to the users at a lower level. These features enable a CP-HABE system to host a large number of users from different organizations by delegating keys E.g., enabling efficient data sharing among hierarchically organized large groups. Finally, construct a CP-HABE scheme with short ciphertext.

PROBLEM DEFINITION

Existing CP-ABE schemes are a secret sharing scheme which is employed to realize an access policy associated with a ciphertext. Here each attribute belonging to the access policy obtains a share of the secret. This requires that the same attribute included in the attribute set of the secret key possess a separate key component so that the share can contribute to reconstructing the secret key to be used in decryption. But a delegator's secret key is generated by a key generator; hence, without knowing the secret key of the key generator, the delegator cannot generate a key component for a new attribute.

NEED FOR NEW SYSTEM

To overcome the existing problems, our system supports a new effective file hierarchy attribute-based encryption. Our system allows the process of encryption, decryption, key generation with trusted authority, who involves the data sharing process. Our system provides the best scheme based on encryption in cloud. A new system must solve the complexity that done on encryption phase and decryption phase and it must provide the access structure of every user and it solves the problem of storage cost.

PROPOSED SYSTEM

Our proposed system's main motivation is to provide effective file sharing among all users. This technique proposes a new effective scheme named efficient file hierarchy attribute-based encryption. This data owner has several data which are to be stored and shared on the cloud service. We store the timing cost of encryption and cipher text. Our scope of the project is to reduce the computation time, lowering the cost storage and reducing the complexity for encryption and decryption. Our scheme allows four main processes like encryption, decryption, generating keys and setting facilities of key. Finally we store the data in cloud environment. This specifies the access rights for every person who is all authorized.

CONCLUSION

Our proposed system is effectively performing the file sharing among different users in cloud. Cloud service provider allowed the data store and shared process by using data owner. File hierarchy attribute based encryption method is used for encrypting the plaintext into cipher text. Cloud service provider only allows the authorized person to access the data by using key. Our overall process effectively reduces the computation time, lowering the cost storage and reducing the complexity for both encryption and decryption. Our experimental simulation provides the high efficiency based on encryption and decryption.

References

1. C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Computing, vol. 12, no. 4, pp. 50–57, October-December 2013.

2 A. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-base. 276, pp. 354–362, August 2014.

3. Y. Yang, J. K. Liu, K. Liang, K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," *Computer Security in ESORICS 2015*, vol. 9327, pp. 146–166, September 2015.