International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182 Print ISSN: 2349-5979
www.allsubjectjournal.com
Volume 2; Issue 12; December 2015; Page No. 250-252

Survey on cloud security using attribute based encryption

[1]Soni Kumari, [2]Dr. SB Sonkamble

[1]Department of Computer Engineering JSPM Narhe Technical Campus, Narhe Rajarshi Shahu School of Engineering & Research Pune, Maharashtra

[2](Project Guide) Department of Computer Engineering JSPM Narhe Technical Campus, Narhe Rajarshi Shahu School of Engineering & Research Pune, Maharashtra

Abstract
Cloud computing has become more popular nowadays. It gives many advantages as it provides low cost and makes use of large share storage and processing resources. But with the growth of online system, the cost of storage infrastructure increases. Another concern is security. When storing and processing the data within the same cloud provided by multiple users, it causes effects on security and privacy. However, most of the work focus on the data content privacy and access control, whereas less focus on the privilege control and the identity privacy. So, this paper presents a semi anonymous privilege control and full anonymous privilege control as Anony Contol and Anony Control-F respectively. It ensures not only data privacy, but also prevents the identity leakage that is identity privacy. The second issue is when multiple users provide the data or share files in same cloud, the number of files increases, which leads to less storage space and the duplication of files increases. For this reason, to decrease the duplication of files and to increase security among users for file sharing use to combine data index technique with ABE (Attribute Based Encryption) system, which integrates data de-duplication for remove duplicate file in cloud storage and give storage optimization and provide security for multiple users for accessing the same data.

Keywords: Anonymity, Multi authority, Data Encryption standard, Attribute based Encryption.

Introduction

Cloud storage has been most popular since last few years. It is used as the core technology. Cloud has at least two challenges that must be handled. First is, data confidentiality should be guaranteed. Most of the work focuses on the data content privacy and access control, and there is less focus on the privilege control, so other users might be able to infer sensitive information. Therefore, not only the data content privacy or access, but also the operation should be controlled. The second is, personal information (set of user attribute) is at risk because there is no privacy of the user identity. Nowadays, most people are more concerned about privacy of their identity, so there is a need to protect identity privacy. In previous system only concern was regarded data content privacy as Identity-based encryption (IBE) [2], Fuzzy Identity-Based Encryption [3]. Most work focus on the data content privacy and access control, and less focus on the privilege control and the identity privacy. User's identity with their attributes are revealed to key issuers, and it issue private keys according to their attributes get their private keys. But at present, users are more concerned to keep their identities secret. Therefore, we propose the Anony Control and Anony Control-F [1] with Attribute Based Encryption for cloud servers for users to access data without knowing their identity information.

Attribute-Based-Encryption is a technique for Encryption data by using attributes and keys. Security is main issue in cloud storage system because data is more sensitive so, anyone hack data so used the encryption data with ABE for secure data. Anony Control and Anony Control-F [1] uses to provide access privilege with identity protection.

Literature Survey

The literature survey plays an important role in the research process. A survey gives the idea and developed into concepts. For protecting the data content privacy in cloud computing various techniques have been proposed as Identity Based Encryption(IBE) [2] was first introduced by Shamir [2], in which the encryption and decryption is based on identity. The message sender can specify an identity and message is only decrypted when the receiver with matching identity. It is based on a public key cryptosystem. In which not generating random pair of keys, the user chooses his name and address as his public key, or any combination of name, address, telephone number etc. Few years later, Fuzzy Identity-Based Encryption [3] is proposed. In such encryption scheme, an identity is viewed as a set of descriptive attributes, and in which, if an identity of descriptor has some overlaps with the one specified in the cipher text then decryption is possible. After that, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) [4] and Cipher text Policy Attribute-Based Encryption (CP-ABE) [5], are proposed. In the KP-ABE [4] cipher texts are labeled with sets of attributes, and a private key is associated with an access tree, that provide user's identity. When the access tree is satisfied by the attributes in the cipher text, then the user can decrypt the cipher text. It is mainly based on key generators issue keys with correct structures to correct users. The problem and overhead occur in KP-ABE is resolved by Cipher text-Policy Attribute-Based Encryption (CP-ABE) [5]. In CP-ABE cipher texts are labeled with an access structure, which gives the encryption policy, and private keys are provided by users' attributes. The attributes in the private key satisfy the access

tree, then user can decrypt the cipher text. Due to this, the Encrypter holds the maximum authority about the encryption policy that why solves the problem and overhead occur in KP-ABE. A multi authority system [6] is presented. In which each user has an ID and they can interact with each key generator (authority). More attribute based encryption schemes having multiple authorities have been proposed afterwards [7, 8], but they are only same topic based as either a threshold-based ABE [7], or have a semi-honest central authority [8]. The disadvantage of threshold based ABE is, it cannot tolerate arbitrarily many users' collusion attack [7]. The system proposed by Lewko [9] and Muller [10] are most similar to ours that they also decentralize the central authority in the CP-ABE into multiple ones. But their system not tolerates the compromise attack towards attributes authorities, but our system can tolerate, which is not covered in many existing works.

Problem statement

To develop a system which will store and retrieve data from cloud and provide a secure and scalable solution the user data, where users can provide access to an identity, which can be viewed as a set of descriptive attributes and also provide the user identity privacy and deduplication.

In cloud based file sharing applications when multiple user use service from same cloud service provider than it is responsibility of cloud server providers to prove a secure option for users where they can share and store files among them. The issues with this will be security among users like which all users can access the file and the duplication of the same file. In our project ''Cloud Security uses Attribute Based Encryption" which develops a system where users can have full and only control over their data. They can decide with whom they want to share data. An authorized person can download data, but cannot modify or delete it. Every data should be encrypted before reaching cloud servers.

In this system, we are using unique attribute based encryption technique. The DES encryption will be used for encryption of files and RSA algorithm will be used to encrypt the DES key. In this way the file will have triple layer of security. In our system we have a unique file indexer which will handle the duplicate file issue. This module (indexer) will help to reduce duplication of data in cloud server

Motivation

Nowadays privacy is a major concern for both consumers and enterprises and thus privacy preservation is a challenging problem. Data sharing is an important in cloud storage. The challenging problem is how to effectively share encrypted data with privacy.

Various techniques have been proposed to protect the data contents privacy and encrypt data. Identity-based encryption (IBE) was first introduced by Shamir [2]. Fuzzy Identity-Based Encryption [3] is proposed, however, most technique focuses on the data contents privacy and the access control, but not focus on privilege control and the identity privacy. This motivates us to study how to find an efficient and secure way to share data in cloud storage as well as providing security for storing the data and identity privacy.

Objective

With the advent of tremendous growth in fields related to cloud computing and internet, the amount of personal and sensitive data which are processed, stored and share are rapidly growing. In such situation, privacy of data sharing and identity protection is an important concern. Hence there is a need to design a system to upload and download data from cloud with data privacy and identity protection and to the developed Master Data Inspector for providing scalable and efficient cloud storage solution and use for data deduplication.

Proposed System

We propose Attribute based encryption with identity protection for cloud storage. Also cloud with deduplication, in which the data loaded is first scanned by our master data inspector system which will decide how data should be treated in cloud system. Our Proposed system is contains three main modules.

1. **Server Module**: All requests first go to this module. This module takes request from a client and communicates with other modules to provide the correct response. Server module consists of one application unit which handle uploading and downloading of file from cloud storage. This unit also handles the ABE algorithm.
2. **Master Data Scanner**: When a file upload request came with server module. It first passes request to Master Data Scanner. If the file is already present in cloud than it will not be uploaded twice. The user's ownership of a file will be handling by this module. The even identity of file for a particular user will be private and will not be changed for any upload.
3. **Key Generator**: This Module will provide all types of Key needed to encrypt and decrypt any file. The Key Generator will have all policy stored. It will search in its database and provide the correct key to the correct owner. Also in case of ABE, Key Generator will generate keys from a different set of attribute.

So, all these three modules will help to provide a secure and optimized cloud storage solution to our users.

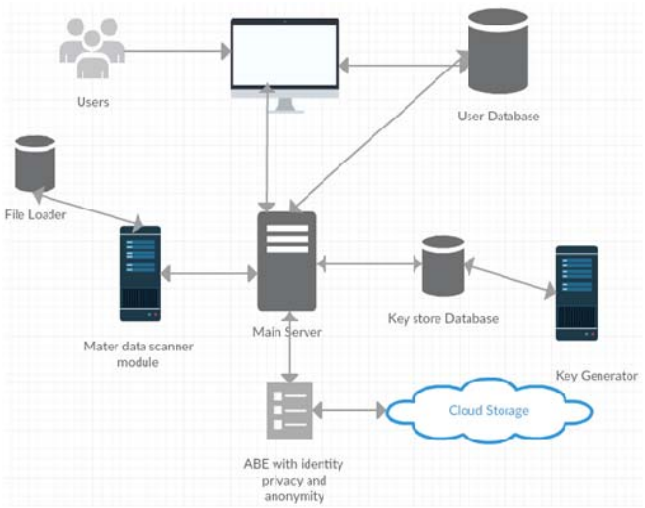

Fig 1: Overview of proposed system

Future Scope

This system can be installed on top of any cloud server by any user. Whenever a company or organization want to use cloud storage for their organization uses than they can install our system as a gateway so that the sharing of data will be secure and also cloud storage will be optimized. This will save cost also. In current scope, we considered only one cloud for reference. But in future we can combine multiple clouds also and use them as an optimized and secure storage system.

Conclusion

To protect user data privacy is a central question of cloud storage. So, we can develop a Secure and scalable file sharing model on the cloud platform using unique Attribute Based Encryption method. The user identity and privacy is much more important and we can share data among users without revealing user identity.

The cloud is very costly. A system must smartly utilize cloud platform while storing data in it. We developed a system where data duplication can be prevented in the cloud.

References

1. Taeho Jung, Xiang-Yang Li, Senior Member, IEEE Zhiguo Wan, Meng Wan, Member IEEE. Control Cloud Data Access Privilege And Anonymity With Fully Anonymous Attribute – Based Encryption IEEE., 2015.
2. Shamir A. Department of Applied Mathematics Identity Based cryptosystems and signature schemes, Springer-Verlag, 1985.
3. Sahai A, Waters B. University of California Fuzzy identity-based encryption, Springer – Verlag, 2005.
4. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data, CCS, 2006.
5. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributebased encryption," IEEE SP, 2007.
6. Chase M. Multi-authority attribute based Encryption" Berlin, Germany: Springer - Verlag, 2007.
7. Lin Z, Cao X. Liang, and J. Shao, Department Of Computer Science and Engineering, Shanghai Jiao Tong University, China "Secure threshold multi authority attribute based encryption without a central authority," Elsevier Inc, 2010.
8. Božovi´c D. Socek Steinwandt R. Villanyi VI. Multi-authority attribute based Encryption with honest-but-curious central Authority, 2012.
9. Lewko A, Waters B. University of Texas Austin, Decentralizing attribute-based Encryption, in Cryptology. Berlin, Springer-Verlag, 2011.
10. Müller S, Katzenbeisser S, Eckert C. On multi-authority ciphertext-policy attribute-based encryption, Math. Soc, 2009.