

An Efficient ABBE for secure data sharing and storage in public and private clouds – A Survey

Jayasudha M¹, *School of computer science, VIT University, Chennai-127, Tamilnadu , India, +91 44 3993 1555, Jayasudha.m@vit.ac.in*

Dr Subbulakshmi T², *School of computer science, VIT University, Chennai-127, Tamilnadu , India, +91 44 3993 1555, subbulakshmi.t@vit.ac.in*

Abstract - Cloud computing, a type of computing paradigm that highly depends on shared data resources rather than local data resources which allow the devices to handle the applications. With the rapid development of cloud data services, the data in cloud was stored and shared across numerous users. Since the shared data can be accessed and modified by multiple users, this new paradigm poses huge challenges in keeping the integrity of the shared data. Several studies about the secure data retrieval focuses heavily on providing strict security for the data stored in the third party domain. However, strict security on third party domain will requires stupendous cost and security issues on cloud service provider which inevitably affects the efficient data retrieval in clouds. In this paper, we propose an effective scheme that supports the efficient retrieval of data stored in clouds. This paper is a survey of specific issues brought by the use of attribute based encryption system in a cloud computing system.

Keywords: Cloud Computing, Data Storage, Data Sharing, Attribute-based Encryption

1. INTRODUCTION

Cloud computing is a promising and emerging computing paradigm in which resources are provided as services and enables users to remotely store their data in a cloud. Since this new computing technology requires users to entrust their important data to cloud providers, there have been growing security and privacy concerns on outsourced data. The idea of cloud computing is based on a very major principal of reusability of IT capabilities. The variation that cloud computing brings compared to traditional computing concepts is to broaden horizons across organizational boundaries. The component of cloud computing includes on-demand self service, broad network access, resource pooling, rapid elasticity and consistent service. On-demand self service means that patrons can request and manage their own computing resources. Broad network access allows

services to be provided over the Internet or private networks. Pooled resources means that patrons draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and patrons are billed accordingly.

Each provider delivers a unique function, giving users higher or lesser control over their cloud depending on the type. While choosing a provider, our need has to be compared with the available cloud services. Cloud needs will vary depending on how we intend to use the space and resources associated with the cloud. There are three types of cloud providers: Software as a Service and Platform as a Service and Infrastructure as a Service. These three types vary in the amount of control that we have over the information, and conversely, how much we can expect the provider to do for us. Software as a Service (SaaS) provider gives subscribers access to

both resources and applications. SaaS makes it unnecessary for us to have a physical copy of software to install on our devices. SaaS also generates it easier to have the same software on all of our devices by accessing it on the cloud. In a SaaS agreement, we have the least control over the cloud. Platform as a Service (PaaS) system goes a level above the Software as a service setup. A PaaS provider enables the subscribers to access the components that they require to develop and operate applications over the internet. Infrastructure as a Service (IaaS) agreement deals primarily with computational infrastructure. In an IaaS agreement, the subscriber totally outsources the storage and resources, such as hardware and software that they need. The cloud provider has lesser control in an IaaS system than with an SaaS agreement.

The information held on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of intimate information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it crucial for us to understand the security measures that your cloud provider has in place, and it is equally critical to take personal precautions to secure your data. The first thing we must look into is the security measures that cloud provider already has in place. These vary from provider to provider and among the various types of clouds. A small business user may have slightly more room to discuss the terms of their contract with the provider and will be able to raise these questions during that time. There are many questions that we can raise, but it is significant to choose a cloud provider that considers the security of our data as a major concern.

Deploying cloud computing can vary depending on requirements, and the following four deployment

models have been classified, each with unique characteristics that support the needs of the services and users of the clouds in peculiar ways. Private Cloud: The cloud infrastructure was deployed, maintained and operated for a specific organization. The action may be in-house or with a third party on the location; Community Cloud: The cloud infrastructure is shared among a number of organizations with similar importance and requirements. This may help reducing the capital expenditure costs for its formulation as the costs are shared among the organizations. The action may be in-house or with a third party on the location; Public Cloud: The cloud infrastructure is available to the public on a monetary basis by a cloud service provider. This empowers a consumer to develop and deploy a service in the cloud with very little financial investment compared to the capital expenditure requirements normally linked with other deployment options; Hybrid Cloud: The cloud infrastructure consists of a number of clouds of any type, but the clouds have the scope through their interfaces to allow data and/or applications to be lifted from one cloud to another. This can be a combo of private and public clouds that support the requirement to preserve some data in an organization, and also the need to offer services in the cloud.

There are some noticeable challenges associated with cloud computing, and some of these may cause a delay when delivering additional services in the cloud, most also can bring opportunities, if resolved with due responsibility and attention in the planning stages. The challenges faced in cloud computing are security and privacy, lack of standards, continuously evolving and compliance concerns. For service developers, making services accessible in the cloud depends on the type of service and the devices being

used to access it. The process may be as simple as a user clicking on the required website, or could associate an application using an API accessing the services in the cloud. Cloud-based communications services enable businesses to enclose communications capabilities into business applications, such as in Enterprise Resource Planning and in Customer Relationship Management systems. For travelling business people, these can be achieved through a smartphone, supporting expanded productivity while moving away from the office. These services are over and above the support of service deployments of VoIP systems, combination systems, and conferencing systems. They can be accessed from any premises and linked into current services to extend their capabilities. In terms of social networking, using cloud-based communications provides click-to-call capacities from social networking sites, access to messaging and video communication systems, improving the interlinking of people within the social circle.

In this paper, we first reviewed the existing schemes using attribute based encryption in cloud computing. Guiyi and Jun [5] proposed an efficient data sharing protocol for the outsourcing of data in cloud and Guojun and Minyi [6] proposed a hierarchical attribute based encryption scheme for achieving fine grained access control and high performance. The existing scheme has two major drawbacks. First, these schemes bring additional decryption and encryption burden to the data owner. The data owner who is required to be online all the time for the secure transfer and retrieval of data's in cloud. Second, if a third party is allowed to fulfill data search task, this requires the party to be fully trusted by providing the secret key of the data owner. The leak of the information disgraces the privacy of the

data owner and this approach is undesirable due to loss of privacy and confidentiality.

The remainder of this paper is organized as follows: Section 2 discussed related works; Section 3 introduces the system model, security model and our design goal; Section 4 provides the details of our proposed scheme; finally Section 5 provides the concluding remarks of the paper

2. RELATED WORK

In this section, we review the concepts of attribute based encryption and provide an abrupt overview of various schemes adopted by existing controls.

2.1 Attribute Based Encryption

In order to improve the compliance of users to share their data in cloud, Sahai and Waters [1] introduced the concept of Attributed-Based Encryption (ABE) in which the user's keys and ciphertexts are defined with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a connection between the attributes of the ciphertext and the user's key. The cryptosystem of sahai and waters permits for decryption when at least k attributes overlapped between a ciphertext and a private key. Goyal [2] proposed a fine grained ABE scheme and defined two complimentary notations: Key Policy ABE and Ciphertext Policy ABE. ABE defines the identity as a set of attributes (key-policy ABE - KP-ABE) or policies defined over a group of attributes (Ciphertext-policy ABE - CP-ABE). The main issue is that decryption of ciphertext is possible only if the person holds a key for matching attributes where user keys are always issued by some trusted party. Bethencourt [3] introduced Ciphertext Policy ABE scheme in which the user's private-key is associated with a set of attributes and a ciphertext determines an access policy over a defined universe

of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Various schemes proposed by researchers in [11 & 17] use CP-ABE with identity-based encryption (IBE) for achieving constant computational cost and constant size cipher texts. In this scheme, there are four algorithms to be executed: Setup, KeyGen, Encrypt and Decrypt.

2.2 Proxy re-encryption

Proxy re-encryption, introduced by Blaze [4] allows a proxy to transfer an encrypted message under A's public key into one more encrypted message under B's public key without viewing the message in plaintext. The proxy does not need the private key of A to encrypt the message and encrypt it under B's public key again. Yang and Jian [9] formed the idea of conditional proxy re-encryption (CPRE) which enables fine grained encryption of cloud data through user revocation. Bharath and Sanjay [8] introduced an efficient and secure data distributed framework using homomorphic encryption and proxy re-encryption schemes that prohibit the leakage of unauthorized data when a revoked user joins the system.

3. PROBLEM STATEMENT

3.1 System model

In the system model as shown in Fig. 1, we assume the cloud computing system mainly composed of the following parties: The data owner; who stores the data in the cloud and depends on the cloud for data maintenance. The authorized user; who accesses the data shared by the data owner, downloads the data and decrypts it using his secret keys. The cloud provider (CP) provides a high quality service using a number of servers with considerable storage space

and computation power. The data should be encrypted before uploading in cloud server. The authorized user accesses the cloud server and receives the encrypted data. After that, the authorized user will submit a request to data owner for authorization and access the data after receiving the credentials from data owner. In addition, the CP has to always be online; whereas, data owners and authorized user can be offline.

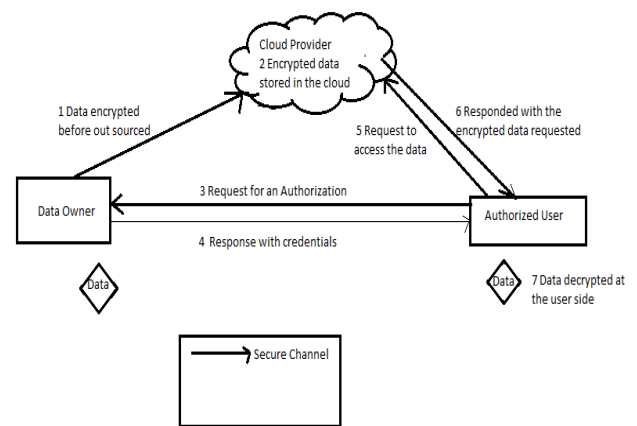


Fig.1 – System Model

3.2 Security model

In the security model, we assume that the cloud provider is untrusted in the manner that it may collude with malignant users to harvest file contents stored in the cloud for its own interest. There are two main attacks under such a circumstance; one is external attacks initiated by unlawful outsiders, and internal attacks initiated by an honest but curious CP as well as malignant end users. The malignant end user needs to access the data that he is ineligible to decrypt. We assume that the CP will not collude with the end users, since the CP is considered to be honest but curious.

3.3 Design goals

The main design goal of our system is to provide a security model with a secure and private policy for data sharing in cloud computing. Especially we want to enable the data owner to share his/her data with the designated authorized sharers such as the shared files, transformed files and re-encryption keys.

4. THE PROPOSED MODEL

In proposed model, attribute based encryption scheme integrates with a secure decentralized code to form a secure shared storage system. The encryption scheme support encoding operations over encrypted messages and forwards the operations over encrypted and encoded messages. The strong integration of encoding, encryption, and forwarding makes the storage system conveniently meet the requirements of data strength, data confidentiality and data forwarding. Accomplishing the assimilation with consideration of a shared structure is challenging. In this scheme, a novel ABE System is proposed that supports keyword private search and encrypted data sharing together. We choose an ABE system with fast decryption as a starting point. The reason of employing ABE is that ABE can provide high articulation for data share and keyword search compared with other encryption systems. To achieve the privacy of keyword search, concrete ABE system was extended into asymmetric pairings. A token related to a keyword to be constructed through an interaction between Private Key Generator and a system user. The construction of the token is similar to that of the secret key of the user and the token will not enable its holder to decrypt the ciphertext associated with same keyword. This is necessary requirement for searchable encryption. The proposed scheme integrates four randomized algorithms: starts

with System initialization, then proceed with Encryption and Key generation, Decryption to achieve secure data sharing in cloud.

5. CONCLUSION

Due to cost efficiency and less hands on management, data owners are very much interested in outsourcing their data in cloud which can access to data as a service. In this paper, we reviewed the schemes and methodologies using attribute based encryption in cloud computing and proposed a novel ABE system for executing data sharing and retrieval simultaneously in cloud. Further work includes the evaluation of our proposal for effective data sharing and retrieval in private and public clouds.

6. REFERENCES

- [1] Sahai A, Waters B. 2005, "Fuzzy identity-based encryption". In: Proceedings of EUROCRYPT. LNCS Vol. 3494; p. 457-73.
- [2] Goyal V, Pandey O, Sahai A, Waters B., 2006, "Attribute-Based encryption for fine-grained access control of encrypted data." In: Proceedings of CCS p. 89-98.
- [3] Bethencourt J, Sahai A, Waters B., "Ciphertext-policy attribute-based encryption." In: Proceedings of ISSP; p. 321-34.
- [4] Matt Blaze, Geritt Bieumer, Martin Strauss, 1998, "Divertible protocols and atomic proxy cryptography," In: Kaisa Nyberg (Ed.), EUROCRYPT, In: Lect. Notes Comput. Sci., vol. 1403, Springer, pp. 127-144.
- [5] Guiyi W, Rongxing L, Jun S. EFADS; 2014, "Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption." In: Journal of Computer and System Sciences 80 (2014); p: 1549-1562.
- [6] Guojun W, Qin L, Jie W, Minyi G., 2011, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers." In: Computers & Security 30 (2011); p. 320-331.

[7] Aws Naser J, Mohamad Fadli Bin Z.,2013,” Use of Cryptography in Cloud Computing.” In: IEEE International Conference on Control System, Computing and Engineering, 29 Nov – 1 Dec 2013, Penang, Malaysia

[8] Bharath K S, Yousef E, Gerry H, Sanjay M.,2015, “A secure data sharing and query processing framework via federation of cloud computing.” In: Information Systems 48(2015); p.196-212.

[9] Yanjiang Y, Haiyan Z, Haibing L, Jian W, Youcheng Z.” Cloud based data sharing with fine-grained proxy re-encryption.” In: ELSEVIER Pervasive and Mobile Computing.

[10] Vijendra Rajendra A, Prabhaker L R.,2014,”Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques.” In: International Journal of Application or Innovation in Engineering & Management (IJAIEEM); Volume 3, Issue 3, March 2014.

[11] Xin D, Jiadi Y, Yuan L, Yingying C, Guangtao X.,2014,” Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing.” In: ELSEVIER Computers & Security 42(2014); p.151-164.

[12] Yuan Zhang et al,2015,”Cryptanalysis of an integrity checking scheme for cloud data sharing”In:ELSEVIER journal of Information security and applications;p.1-6.

[13] Boyang Wang ,Baochun Li , Hui Li , 2015,”Panda: Public Auditing for shared data with efficient user revocation in the cloud”,In:IEEE Transactions on services Computing;p.92-105

[14] Boyang Wang , Baochun Li , Hui Li , 2015,”Oruta:Privacy –Preserving Public Auditing for shared Data in the cloud”, In: IEEE Transaction on cloud computing;p.43-56.

[15] FU Jing-yi, HUANG Qin-long, MA Zhao-feng, YANG Yi-xian,2014,”Secure personal data sharing in cloud computing using attribute –based broadcast encryption”, In: The journal of china universities of Posts and Telecommunications;p.44-77.

[16] D.Thilakanathan , Shiping Chen, Surya Nepal and Rafael A. Calvo,2012,”Secure Data sharing in the cloud”, In: IEEE Conferences on Cloud Computing;p.1-29.

[17] Yinghui Z, Dong Z, Xiaofeng C, Jin L, Hui L. “Efficient attribute-based data sharing in mobile clouds.” In: ELSEVIER Pervasive and Mobile Computing.