Chapter 64
Data Security for Cloud Datasets With Bloom Filters on Ciphertext Policy Attribute Based Encryption

G. Sravan Kumar
Acharya Nagarjuna University, Guntur, India

A. Sri Krishna
RVR & JC College of Engineering, Guntur, India

ABSTRACT

Cloud data storage environments allow the data providers to store and share large amounts of datasets generated from various resources. However, outsourcing private data to a cloud server is insecure without an efficient access control strategy. Thus, it is important to protect the data and privacy of user with a fine-grained access control policy. In this article, a Bloom Filter-based Ciphertext-Policy Attribute-Based Encryption (BF-CP-ABE) technique is presented to provide data security to cloud datasets with a Linear Secret Sharing Structure (LSSS) access policy. This fine-grained access control scheme hides the whole attribute set in the ciphertext, whereas in previous CP-ABE methods, the attributes are partially hidden in the ciphertext which in turn leaks private information about the user. Since the attribute set of the BF-CP-ABE technique is hidden, bloom filters are used to identify the authorized users during data decryption. The BF-CP-ABE technique is designed to be selective secure under an Indistinguishable-Chosen Plaintext attack and the simulation results show that the communication overhead is significantly reduced with the adopted LSSS access policy.

DOI: 10.4018/978-1-7998-7705-9.ch064

1. INTRODUCTION

Conventional computer storage systems are not enough to store enormous amount of data generated from different resources. Whereas cloud computing provides big data storage facilities for the data providers as well as internet users (Lu et al., 2011). The private data stored in cloud computers can be transferred to authorized users when they provide data request to access those data. It is necessary to protect the copyright of original data by not allowing the data users to modify it unless he/she is a trusted user. This could be achieved by implementing an access policy based cryptographic scheme on the data to be transferred via insecure channel. The primary goal of any broadcasting authority is to offer collusion free and privacy preserving data transfer to authorized data users. Many data publishers intend to publish their sensitive data for several purpose including personal need, secret message transmission, online transaction, patients'-health related information storage (Yeh et al., 2018), electronic health record management (Ibraimi et al., 2011) and so on. Thus, privacy of data as well as individuals must be safeguarded from illegal data users on transmission through broadcasting channel (Kaaniche, & Laurent, 2017). In literature, several access policy-based data publishing techniques are introduced to provide data security, and to allow the authorized entity to access the data.

The access control mechanisms will protect the sensitive data from illegal data users by converting the original text into unreadable text format called as ciphertext. Thus, the legal data user is allowed to view and access the original data when the identity information in their decryption key satisfies the access policy embedded in ciphertext (Zhao et al., 2015). The access policies used in most of the cryptographic methods may contain two parts: attribute names and attribute values in which the attribute values are hidden, and the attribute names are not hidden. For example, if age is used as an attribute, then age values are hidden but the attribute name 'age' is not hidden in the ciphertext. This process is followed for easy identification of access policy at decryption device. Besides, the attribute names are also sensitive which in turn leaks private information and influence the anonymity of data publisher. This will remain a security issue in most of the modern applications. Taking these issues into consideration, still there is a need for fine-grained access policy to provide effective control over sensitive information with proven data security (Xu et al., 2019).

Attribute Based Encryption (ABE) schemes are introduced to provide fine-grained access control for efficient data transmission (Huang et al., 2018). In ABE techniques, cloud data is encrypted with piece of user identity information called as attributes (Goyal et al., 2006). These attributes are inserted into the cloud data based on one of the access policy methods like AND and/or OR gates (Yang & Zia, 2013), wildcards (Kumar & Krishna, 2019), hidden AND-gate (Zhong et al., 2018), linear secret sharing structure (Tan, 2019), etc. ABE schemes are categorized into two types such as: Key-Policy Attribute Based Encryption (KP-ABE) (Attrapadung et al., 2011) and Ciphertext-Policy Attribute Based Encryption (CP-ABE) (Bethencourt et al., 2007). In KP-ABE, access policy is encrypted in users' recovery key and the attributes are embedded in the ciphertext. In CP-ABE, access control is encrypted in ciphertext and the attributes are embedded in data recovery key. Of these two techniques, CP-ABE is found to be important to broadcast data with fine-grained access control for providing data anonymity.

In traditional ABE techniques, the cloud server selects the access policy for message encryption and so, the data providers fully rely on them. If the cloud servers make any wrong decision in the access policy, then it is possible that the data may be attacked by unauthorized entities. Furthermore, the access control in certain CP-ABE schemes is embedded in ciphertext as plaintext format (Yang & Jia, 2014; Li et al., 2015; Yang et al., 2016). The main drawback of these techniques is that it leaks sensitive infor-