**An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy**

How to control the access of the huge amount of big data becomes a very challenging issue, especially when big data are stored in the cloud. Ciphertext-Policy Attributebased Encryption (CP-ABE) is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of data consumers and only allows data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the ciphertext in plaintext form, which may also leak some private information about end-users. Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected. In this paper, we propose an efficient and fine-grained big data access control scheme with privacy-preserving policy. Specifically, we hide the whole attribute (rather than only its values) in the access policies. To assist data decryption, we also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy. Security analysis and performance evaluation show that our scheme can preserve the privacy from any LSSS access policy

without employing much overhead.

**Index Terms—Big Data; Access Control; Privacy-preserving Policy; Attribute Bloom Filter; LSSS Access Structure**

**EXISTING SYSTEM:**

In order to enable end-users to control the access of their own data stored on untrusted remote servers (e.g., cloud servers), encryption-based access control is an effective method, where data are encrypted by end-users and only authorized users are given decryption keys. This can also prevent the data security during the transmission over wireless networks which are vulnerable to many threats . However, traditional public key encryption methods are not suitable for data encryption because it may produce multiple copies of ciphertext for the same data when there are many data consumers in the system. In order to cope with this issue, some attribute-based access control schemes are proposed by leveraging attribute-based encryption which only produces one copy of ciphertext for each data and does not need to know how many intended data consumers during the data encryption. Moreover, once the cloud data are encrypted, some searchable encryption algorithms are proposed to support search on encrypted cloud data.

**DISADVANTAGES:**

* Existing methods which only partially hide the attribute values in the access policies
* End-users may worry that the cloud server may make wrong access decision intentionally or unintentionally, and disclose their data to some unauthorized users.
* Attribute-based access control schemes can deal with the attribute revocation problem , they all suffer from one problem: the access policy may leak privacy. This is because the access policy is associated with the encrypted data in plaintext form.

**PROPOSED SYSTEM:**

1. We propose an efficient and fine-gained big data access control scheme with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes.

2) We also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

3) We further give the security proof and performance evaluation of our proposed scheme, which demonstrate that our scheme can preserve the privacy from any LSSS access policy without employing much overhead.

**ADVANTAGES:**

* we have proposed an efficient and fine-grained data access control scheme for big data, where the access policy will not leak any privacy information.
* our method can hide the whole attribute (rather than only its values) in the access policies
* our scheme is selectively secure against chosen plaintext attacks.

**MODULES:**

The system consists of five entities, namely

1. **Cloud Servers**
2. **Attribute Authority**
3. **End-users,**
4. **Data Consumers**

**Cloud Servers** Cloud Servers are employed to store, share and process big data in the system. The cloud servers are managed by cloud service providers, who are not in the same trust domain as end-users. Thus, cloud servers cannot be trusted by end-users to enforce the access policy and make access decisions. We also assume that the cloud server cannot collude with any End-users or Data Consumers.

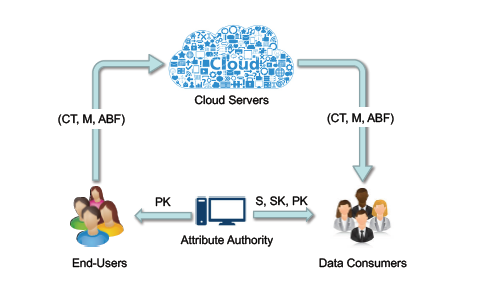
**Attribute Authority** The attribute authority manages all the attributes in the system and assigns attributes chosen from the attribute space to end-users. It is also a key generation center, where the public parameters are generated. It also grants different access privileges to end-users by issuing secret

keys according to their attributes. The attribute authority is assumed to be fully trusted in the system.

**End-user End-users** are the data owners/producers who outsource their data into the cloud. They also would like to control the access of their data by encrypting the data with CP-ABE. End-users are assumed to be honest in the system.

**Data Consumers** Data consumers request the data from cloud servers. Only when their attributes can satisfy the access policies of the data, data consumers can decrypt the data. However, data consumers may try to collude together to access some data that are not accessible individually.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Netbeans 7.2.1
* Database : MYSQL

**REFERENCES**

* C. Dong, L. Chen, and Z. Wen, “When private set intersection meets big data: an efficient and scalable protocol,” in Proc. of CCS’13. ACM, 2013, pp. 789–800.
* K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,” IEEE Trans.
* Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec 2015.
* J. Hur, “Attribute-based secure data sharing with hidden policies in smart grid,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, 2013.