ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

# Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

**Gone Sowjanya**
**Department of Computer Science and Engineering,**
**Vignana Bharathi Institute of Technology,**
**Hyderabad, T.S - 501301, India.**

**Srinivas Rao**
**Department of Computer Science and Engineering,**
**Vignana Bharathi Institute of Technology,**
**Hyderabad, T.S - 501301, India.**

***ABSTRACT:***

***With the development of cloud computing, outsourcing data to cloud server attracts lots of attentions. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a ciphertext-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notbaly, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.***

## INTRODUCTION

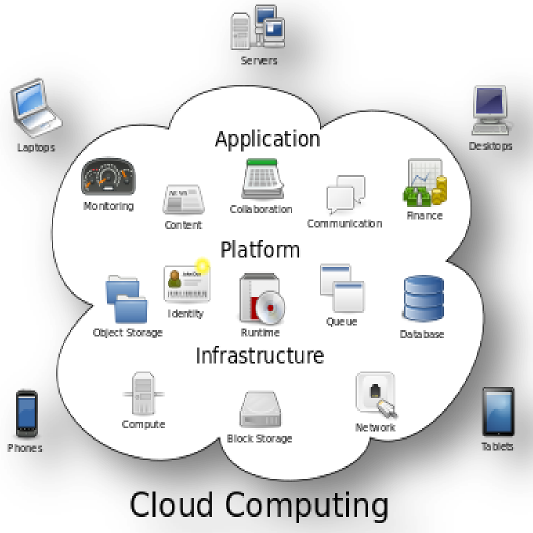
Cloud computing is regarded as a prospective computing paradigm in which resource is supplied as service over the Internet. It has met the increasing needs of computing resources and storage resources for some enterprises due to its advantages of economy, scalability, and accessibility. Recently, several cloud storage services such as Microsoft Azure and Google App Engine were built and can supply users with scalable and dynamic storage. With the increasing of sensitive data outsourced to cloud, cloud storage services are facing many challenges including data security and data access control. To solve those problems, attribute-based encryption (ABE) schemes [1-3] have been applied to cloud storage services. Sahai and Waters [1] first proposed ABE scheme named fuzzy identity-based encryption which is derived from identity-based encryption (IBE) [4]. As a new proposed cryptographic primitive, ABE scheme not only has the advantage of IBE scheme, but also provides the character-istic of "one-to-m any" encryption. Presently, ABE mainly includes two categories called ciphertext -policy ABE (CP-ABE) [2] and key-policy ABE (KP-ABE) [3]. In CP-ABE, ciphertexts are associated with access policies and user's private keys are associated with attribute sets. A user can decrypt the ciphertext if his attributes satisfy the access policy embedded in the ciphertext. It is contrary in KP-ABE. CP-ABE is more suitable for the outsourcing data architecture than KP-ABE because the access policy is defined by the data owners. In this article, we pr esent an efficient CP-ABE with user revocation ability.

### What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes

**Cite this article as:** Gone Sowjanya & Srinivas Rao, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 8, 2018, Page 42-49.

from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

### How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

### Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

### On-demand self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

### Broad network access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

### Resource pooling:

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence [5] in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

### Rapid elasticity:

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

### Measured service:

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

## EXISTING SYSTEM:

- Boldyreva et al. presented an IBE scheme with efficient revocation, which is also suitable for KP-ABE. Nevertheless, it is not clear whether their scheme is suitable for CP-ABE.
- Yu et al. provided an attribute based data sharing scheme with attribute revocation ability. This scheme was proved to be secure against chosen plaintext attacks (CPA) based on DBDH assumption. However, the length of cipher text and user's private key are proportional to the number of attributes in the attribute universe.
- Yu et al. designed a KP-ABE scheme with fine-grained data access control. This scheme requires that the root node in the access tree is an AND gate and one child isa leaf node which is associated with the dummy attribute.
- In the existing scheme, when a user leaves from a user group, the group manager only revokes his group secret key which implies that the user's private key associated with attributes is still valid. If someone in the group intentionally exposes the group secret key to the revoked user, he can perform decryption operations through his private key. To clarify this attack, a concrete instance is given. Assume that the data is encrypted under the policy "professor AND cryptography" [6] and the group public key. Suppose that there are two users: user1and user2 whose private keys are associated with the attribute sets {male, professor, cryptography} and {male, student, cryptography} respectively. If both of them are in the group and hold the group secret key, then user1can decrypt the data but user2can't. When user1is revoked from the group, he can't decrypt alone because he does not have the updated group secret key. However, the attributes of user1are not revoked and user2 has the updated group secret key. So, user1can collude with user2 to perform the decryption operation. Furthermore, security model and proof were not provided in their scheme.

## DISADVANTAGES OF EXISTING SYSTEM:

- It is expensive in communication and computation cost for users.
- Unfortunately, ABE scheme requires high computation overhead during performing encryption and decryption operations. This defect becomes more severe for lightweight devices due to their constrained computing resources.
- There is a major limitation to single-authority ABE as in IBE [7]. Namely, each user authenticates him to the authority, proves that he has a certain attribute set, and then receives secret key associated with each of those attributes. Thus, the authority must be trusted to monitor all the attributes. It is unreasonable in practice and cumbersome for authority.

## PROPOSED SYSTEM:

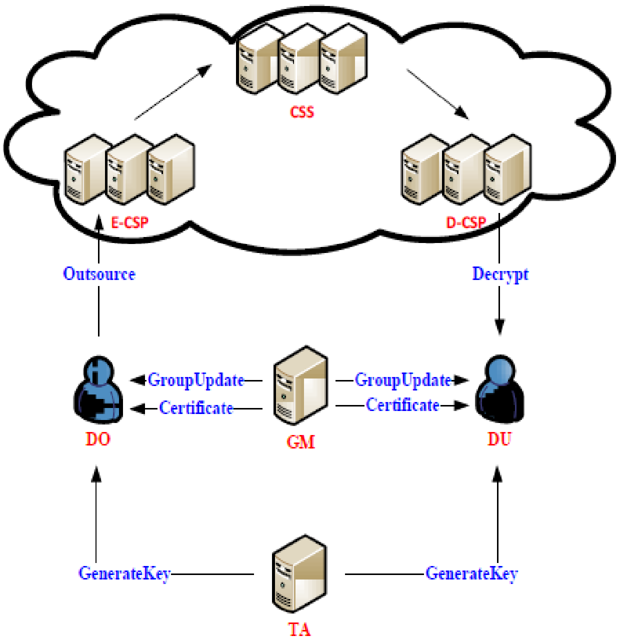
- In this system, we focus on designing a CP-ABE scheme with efficient user revocation for cloud storage system.
- We aim to model collusion attack performed by revoked users cooperating with existing users.
- Furthermore, we construct an efficient user revocation CP-ABE scheme through improving the existing scheme and prove our scheme is CPA secure under the selective model.
- To solve existing security issue, we embed a certificate into each user's private key. In this way, each user's group secret key is different from others and bound together with his private key associated with attributes.
- To reduce users' computation burdens, we introduce two cloud service providers named encryption-cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP) [8].
- The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation.

- In the encryption phase, the operation associated with the dummy attribute is performed locally while the operation associated with the sub-tree is outsourced to E-CSP. T

## ADVANTAGES OF PROPOSED SYSTEM:

- Reduce the heavy computation burden on users.
- We outsource most of computation load to E-CSP and D-CSP and leave very small computation cost to local devices [9].
- Our scheme is efficient for resource constrained devices such as mobile phones.
- Our scheme can be used in cloud storage system that requires the abilities of user revocation and fine-grained access control.

## SYSTEM ARCHITECTURE:



| Symbol | Description |
|---|---|
| TA | Trusted Authority |
| GM | Trusted Group Manager |
| DO | Data Owner |
| DU | Data User |
| CSS | Cloud Storage Server |
| E-CSP | Encryption-Cloud Service Provider |
| D-CSP | Decryption-Cloud Service Provider |

## IMPLEMENTATION MODULES:

- Achieving full anonymity
- Fully Anonymous Multi-Authority CP-ABE
- Security Model
- Security Analysis

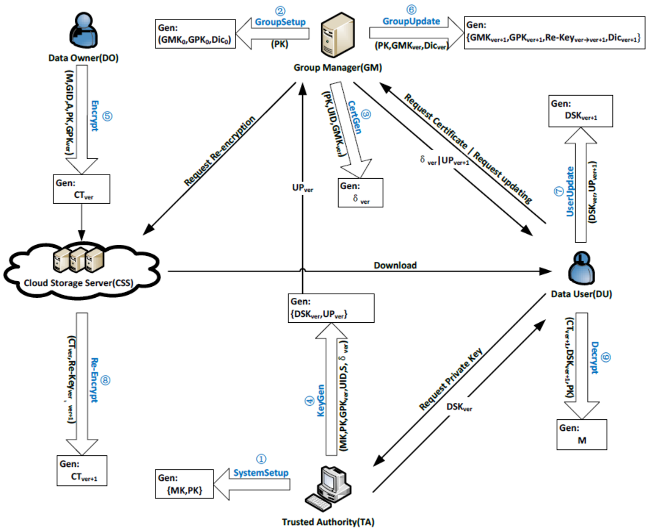


Fig. CP-ABE with efficient user revocation.

## MODULES DESCRIPTION

### Achieving full anonymity

We have assumed semi-honest authorities in AnonyControl and we assumed that they will not collude with each other. This is a necessary assumption in AnonyControl because each authority is in charge of a subset of the whole attributes set, and for the attributes that it is in charge of, it knows the exact information of the key requester. If the information from all authorities is gathered altogether, the complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities. In this sense, AnonyControl is semianonymous since partial identity information (represented as some attributes) is disclosed to each authority, but we can achieve a full-anonymity and also allow the collusion of the authorities [10].

### Fully Anonymous Multi-Authority CP-ABE:

The KeyGenerate algorithm is the only part which leaks identity information to each attribute authority. Upon receiving the attribute key request with the attribute value, the attribute authority will generate H(att (i ))ri and sends it to the requester where att (i ) is the attribute value and ri is a random number for that attribute. The attribute value is disclosed to the authority in this step. We can introduce the above 1-out-of-n OT to prevent this leakage. We let each authority be in charge of all attributes belonging to the same category. For each attribute category c (e.g., University), suppose there are k possible attribute values (e.g., IIT, NYU, CMU ...), then one requester has at most one attribute value in one category.

## Security Model

Setup→**PK**,**MK**k : This algorithm takes nothing as input except implicit inputs such as security parameters. Attributes authorities execute this algorithm to jointly compute a system-wide public parameter **PK** as well as an authority-wide public parameter yk , and to individually compute a master key **MK**k.

KeyGenerate(**PK**, **MKk**, Au) → **SK**u: This algorithm enables a user to interact with every attribute authority, and obtains a private key **SK**u corresponding to the input attribute set Au. Encrypt(**PK**, M, {Tp}p∈{0,...,r−1}) → (**CT**,**VR**): This algorithm takes as input the public key **PK**, a message M, and a set of privilege trees {Tp}p∈{0,...,r−1}, where r is determined by the encrypter. It will encrypt the message M and returns a ciphertext **CT** and a verification set **VR** so that a user can execute specific operation on the ciphertext if and only if his attributes satisfy the corresponding privilege tree Tp [11]. As we defined, T0 stands for the privilege to read the file. Decrypt(**PK**, **SK**u , **CT**) → M or verification parameter: This algorithm will be used at file controlling (e.g. reading, modification, deletion). It takes as input the public key **PK**, a ciphertext **CT**, and a private key **SK**u, which has a set of attributes Au and corresponds to its holder's **GID**u.

## Security Analysis

In the proposed scheme, an authority generates a set of random secret parameters and shares it with other authorities via secure channel, and is computed based on this parameters. It is believed that DDH problem is intractable in the group G0 of prime order p, therefore does not leak any statistical information about . This implies even if an adversary is able to compromise up to (N − 2) authorities, there are still two parameters kept unknown to the adversary.

## Conclusion

In this article, we provided a formal definition and security model for CP-ABE with user revocation. We also construct a concrete CP-ABE scheme which is CPA secure based on DCDH assumption.

To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys.

Additionally, we outsource operations with high computation cost to E-CSP and D-CSP to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed.

## REFERENCES

[1] Jiguo Li, Wei Yao, Yichen Zhang,Huiling Qian and Jinguang Han, Member, IEEE, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", IEEE Transactions on Services Computing, 2016.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th CCS, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE SP, May 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in Theory of Cryptography. Berlin, Germany: Springer-Verlag, 2007, pp. 515–534.

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. 16th CCS, 2009, pp. 121–130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in Proc. IEEE 7th SOSE, Mar. 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2895–2903.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.