# Revocable Data Access Control for Multi-Authority Cloud Storage Using Cipher Text-Policy Attribute Based Encryption

**Kankala Sridhar**
M.Tech, Department of CSE Aurora's Scientific, Technological and Research Academy Hyderabad-500081
sridhar.kankala@gmail.com

**V. Srinivas**
Senior Associate Professor, Department of CSE Aurora's Scientific, Technological and Research Academy, Hyderabad-500081.
srinivassai1549@gmail.com

## ABSTRACT:

*In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such polices is to employ a trusted server store the data and mediate confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call cipher text-policy attribute-based encryption. By using our techniques encrypted data can be secure against collusion attacks. Previous attribute-based encryption systems used attributes to describe the encrypted data and built policies into user's key; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, out methods are conceptually closer to traditional access control methods such as role-based access control(RBAC).In addition, we provide an implementation of our system and five performance measurements. In cloud computing the data security is achieved by Data Access Control Scheme. Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered as one of the most suitable scheme for data access control in cloud storage. This scheme provides data owners more direct control on access policies. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. So This paper produce survey on efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities cooperate and each authority is able to issue attributes independently. Specifically, this paper surveys a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security. This survey shows that revocable multi-authority CP-ABE scheme is secure in the random oracle model and is more efficient than previous multi-authority CP-ABE.*

**Key Words**—Access control; multi-authority; CP-ABE; attribute revocation; cloud storage.

## 1. INTRODUCTION:

**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 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.

### Access Control in Cloud Computing:

Cloud computing is one of the emerging technologies. The cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security.

### Cloud Storage:

The Cloud storage is an important service of cloud computing. The Cloud Storage offers services for data owners to host their data into the cloud. A great challenge to data access control scheme was data hosting and data access services. Because data owners does not fully trust the cloud servers also they can no longer rely on servers to do access control The data access control becomes a challenging issue in cloud storage systems because of data outsourcing and untrusted cloud servers. Therefore **Cloud storage** is a model of data storage where the digital data is stored in logical pool.

### Data Access Control System In Multi Authority Cloud Storage

There are five types of entities in the system AS IN Figure-1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key. For each user reflecting his/her attributes.

## 2. RELATED WORKS:

### 2.1 Multi-Authority Attribute Based Encryption

**Authors:** M. Chase

In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each cipher text. Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes [SW05]. We answer this question in the affirmative. Our scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k. Our scheme can tolerate an arbitrary number of corrupt authorities. We also show how to apply our techniques to achieve a multi authority version of the large universe fine grained access control ABE presented by Gopal et al.

### 2.2 Improving Privacy and Security in Multi - Authority Attribute - Based Encryption

**Authors:** M. Chase and S.S.M. Chow

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every cipher text, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities.

Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

### 2.3 Decentralizing Attribute-Based Encryption

**Authors:** A.B. Lewko and B. Waters

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority.

In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge cipher text and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.

### 2.4 Attribute Based Data Sharing with Attribute Revocation

**Authors:** S.Yu, C.Wang, K.Ren, W. Lou

Cipher text-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher text if and only if his attributes satisfy the cipher text access structure.

Beside this basic property, practical applications usually have other requirements. In this paper we focus on an important issue of attribute revocation which is cumbersome for CP-ABE schemes. In particular, we resolve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort. We achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy servers. Formal analysis shows that our proposed scheme is provably secure against chosen cipher text attacks. In addition, we show that our technique can also be applicable to the Key-Policy Attribute Based Encryption (KP-ABE) counterpart.

### 2.5 Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

**Authors:** M.Li, S.Yu, Y.Zheng, K.Ren, W. Lou

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.

In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for

PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

## 3. EXISTING SYSTEM

In a multi-authority cloud storage system, attributes of user's can be changed dynamically. A user may be join some new attributes or revoked some current attributes. [1]In 2010, S. Yu, C. Wang, K. Ren, and W.Lou, worked on Attribute Based Data Sharing with Attribute Revocation. This paper use semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks. Provide importance to attribute revocation which is difficult for CP-ABE schemes.

**Drawback:** The storage overhead could be high if proxy servers keep all the proxy re-key.

In 2011, S J. Hur and D.K. Noh, worked on **Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems**. This paper proposes an access control mechanism based on cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. This dual encryption mechanism takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. The advantage of this scheme is securely managing the outsourced data. This scheme achieve efficient and secure in the data outsourcing systems. **Drawback:**

- Huge issue in Enforcement of authorization policies and the support of policy updates

In 2011, S. Jahid, P. Mittal, and N. Borisov, worked on **Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation**. The proposed Easier architecture that supports two approaches are fine-grained access control policies and dynamic group membership. Both scheme achieved by using attribute-based encryption, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is the Easier architecture and construction provides performance evaluation, and prototype application of our approach on Face book.

**Drawback:**

- Does not Achieve Stronger Security Guarantees.

In 2013, S. Jahid, P. Mittal, and N. Borisov, worked on **Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption**, This model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved.

**Drawback:**

Existing attribute revocation methods rely on a trusted server or lack of efficiency also they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

Each Attribute authorities (AAs) is trusted but can be corrupted by the adversary. Each user is dishonest and may try to obtain unauthorized access to data.

**Attribute-Based Encryption with Verifiable Outsourced Decryption:**

This scheme changes the original model of ABE with outsourced decryption to allow for verifiability of the transformations in existing system. This new model constructs a concrete ABE scheme with verifiable outsourced decryption also does not rely on random oracles.

### 3.1 ANALYSIS OF EXISTING SYSTEM:

- This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control.
- Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies.
- In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

### 3.2 DRAWBACKS IN EXISTING SYSTEM:

- Chase’s multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, since it holds the master key of the system.
- Chase’s protocol does not supports attribute revocation.

### 3.3 PROPOSED SYSTEM:

- In this paper, we first propose a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system.
- Our attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new cipher text that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously

published cipher texts, if it has sufficient. attributes).

- Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi trusted in some scenarios, our scheme can still guarantee the backward security.
- Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

This paper, surveys a revocable multi-authority CP-ABE scheme [5], to solve the attribute revocation problem in the system. This method is an efficient and secure revocation method. The attribute revocation method can efficiently achieve both forward security and backward security. In backward security scheme the revoked user cannot decrypt any new Cipher text that requires the revoked attribute to decrypt. In Forward security the newly joined user can also decrypt the previously published cipher texts, if it has sufficient attributes. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

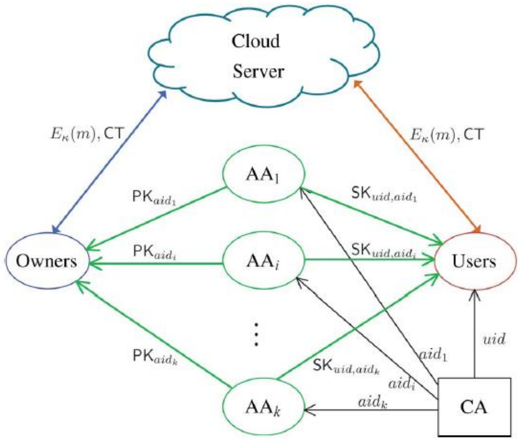
## 3.4 OVERVIEW OF PROPOSED SYSTEM

- Attribute revocation method can efficiently achieve both forward security and backward security.
- An attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, secure in the sense that it can achieve both backward security and forward security.

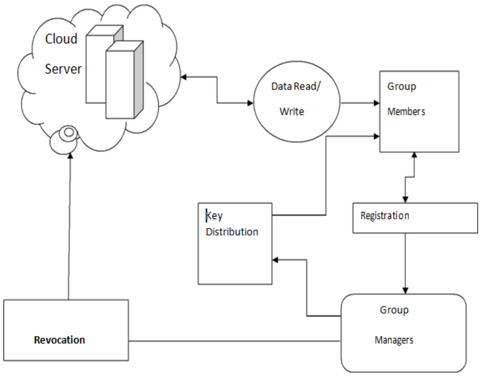
## 3.5 ADVANTAGES OF PROPOSED SYSTEM:

- We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation.
- We greatly improve the efficiency of the attribute revocation method.
- We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a cipher text.

## 4. SYSTEM ARCHITECTURE:



## 4.1 PROPOSED SYSTEM ARCHITECTURE:



- We propose a secure multi-owner data sharing scheme using Diffie-Helman Key exchange. It implies that any user in the group can securely share data with others by the untrusted cloud.
- We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

## 4.2 MODULES:

1. Certificate Authority
2. Attribute Authorities
3. Data Owners
4. Cloud Server
5. Data Consumers

## 4.3 MODULES DESCRIPTION:

### 4.3.1 Certificate Authority:

The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity.

### 4.3.2 Attribute Authorities:

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

### 4.3.3 Data Consumers:

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

### 4.3.4 Data Owners:

Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

### 4.3.5 Cloud Server:

Then, the owner sends the encrypted data to the cloud server together with the cipher texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the cipher text. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

This survey explains a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-authority cloud storage systems is proposed. It eliminates Decryption overhead for users according to attributes .This secure attribute based cryptographic technique for robust data security that"s being shared in the cloud .This revocable multi-authority CPABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .The revocable multi-authority CPABE is a efficient technique, which can be applied in any remote storage systems and online social networks etc.

## 5. CONCLUSION

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

## 6. FUTURE ENHANCEMENT

For future work, we will also seek more sophisticated method to build the user profile, and better metrics to predict the performance (especially the utility) of UPS. We can also implement the hierarchical divisive approach for retrieving the search results. It will gives better performance when compared with our proposed System.

## 7. REFERENCES

[1]. S.Yu, C.Wang, K.Ren, and W.Lou, Attribute Based Data Sharing with Attribute Revocation, in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS"10), 2010, pp. 261-270.

[2]. J. Hur and D.K. Noh, Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems, IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[3].S.Jahid, P.Mittal, and N.Borisov, Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation, in Proc. 6th ACM Symp.
Information, Computer and Comm. Security (ASIACC 11), 2011, pp. 411-415.

[4].M. Li, S. Yu, Y. Zheng, K. Ren, andW.Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption, IEEE Trans. Parallel Distributed Systems, vol. no. 1, pp. 131-143, Jan. 2013. 24,

[5].Kan Yang, and Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage, IEEE transactions on parallel and distributed systems, vol. 25, no. 7, july 2014.

[6] Mr. SanthoshkumarB.J, M.Tech, Amrita Vishwa Vidyapeetham, Mysore Campus, India "Attribute Based Encryption with Verifiable Outsourced Decryption." In International Journal of Advanced Research in Computer Science and Software Engineering" Volume 4, Issue 6, June 2014,ISSN: 2277 128X.

[7] Tejaswini R M1, Roopa C K2 , Ayesha Taranum "Securing Cloud Server & Data Access with Multi - Authorities" International Journal of Computer Science and Information Technology Research ISSN 2348-120X Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014, Available at: www.researchpublish.com