FAC-MACS: Fortified Access Control for Multi-Authority Cloud Storage Using CPABE

Bhuvaneswari Thangaraj¹, S.Umarani², D.Sharmila³

¹PG scholar, Maharaja Engineering College, Avinashi, India
²Assistant Professor, Maharaja Engineering College, Avinashi, India
³Professor & Head, Bannari Amman Institute of Technology Sathyamangalam, India

Abstract

Security and data privacy is paramount to cloud users seeking to protect their gigabytes of vibrant business data from the inquisitive eyes of unauthorized users who are attempting to exceed their authority and also it becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is observed as one of the most seemly technologies for data access control in cloud storage, because it gives more direct control access strategies to the cloud data owners. This CP-ABE scheme provides intrinsic security mechanisms designed to minimize the security attacks and threats in cloud system. In this paper, we design a Fortified Access control for Multi-Authority Cloud Storage Systems, where the process of data access control is strengthened to ensure the safety of the cloud data. Fortified access control to discourse not only the data privacy difficulties in existing cloud storage scheme, by using multiple authorities in the cloud storage system, the proposed scheme can efficiently reaches the tenable access control and revokes the anonymous access to the cloud data. The study and simulation analysis illustrates that proposed well organized Fortified Access Control is both secure and efficient for Cloud Storage Systems.

Keywords: Adversary, Attribute Based Encryption, Secret and Update Keys

1. INTRODUCTION

Similar to Cloud Computing, Cloud Storage has also been growing in popularity recently due to many of the same reasons as Cloud Computing. Cloud Storage delivers virtualized storage on demand, over a network based on a request for a given quality of service (QoS). There is no necessity to purchase storage or in some cases even provision it before storing data. Cloud Storage is an important package of cloud computing, which offers pacts for cloud data vendors to host their data in the cloud. This new prototype of data hosting and access services introduces a great challenge to data access control. Because the cloud data vendors cannot be fully trust on cloud server and they are not equipped to trust on servers to control the data access. Ciphertext-Policy Attribute-Based Encryption is viewed as one of the most appropriate technologies for data access control in cloud storage systems, because if offers more direct access control policies and strategies to the cloud data vendors. In CP-ABE scheme, there is a distinct authority that is responsible for attribute management, key generation, key transfer and key distributions. The authority can be the registered office located in different locations. The cloud data vendors can state the access strategies and encrypt the data according to the strategies. Each user will be supplied a secret key reproducing its attributes. The data can be decrypted the cloud users by verifying its attributes based on the access strategies.

CP-ABE offers two types of systems:
1. Single Authority CP-ABE
2. Multi-Authority CP-ABE

Single Authority CP-ABE: Attributes of the cloud data vendors are managed by sole authority. Extensive research has done for single authority in cloud storage system, a user may clench attributes issued by multiple authorities and the data owners may share the data with the user managed to different authorities which is a great challenge in single authority.

Multi-Authority CP-ABE: Attributes of the different domains and cloud data vendors are managed by different authorities. Multi-Authority CP-ABE is more apt scheme for data access control of cloud storage systems, as users may clench attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities. In this paper, we first propose a Fortified multi-authority CP-ABE scheme, where an expressive, efficient and more secured revocation method is proposed to solve the attribute revocation and anonymous data access problems in the cloud storage system. Efficiency in computation and attribute revocation are the critical requirements while designing the access control schemes.

In Efficient Computation, there are three operations required namely
1. Encryption
2. Decryption
3. Revocation

In Efficient Attribute Revocation, there are two requirements
1. Backward Security
2. Forward Security

In this paper, we design a new fortified multi-authority CP-ABE scheme with efficient decryption and offer an efficient attribute revocation method, and then an
operative access control scheme for multi-authority cloud storage system is designed by applying the prosed methods.

The main offerings of this paper work can be condensed as follows.

✔ We propose a FAC-MACS (Fortified Access Control for Multi-Authority Cloud Storage), an expressive, efficient and more secured data access control scheme for multi-authority cloud storage systems, which is a enhance security scheme and has better performance and efficient computation than existing access control schemes.

✔ We construct a new Fortified Multi-Authority CP-ABE scheme with efficient encryption and decryption. Specially, we design the main computation of the encryption and decryption by using key splitter based method.

✔ We also design and efficient speedy attribute revocation method for multi-authority CP-ABE scheme that acheives both forward and backward security. It reduces computation and communication cost.

The continuing of this paper is systematized as follows.

**Section 2:** Risks and Issues in existing access control Schemes

**Section 3:** Defines the System Model and Security Framework

**Section 4:** Gives the detailed architecture and Implementation of FAC-MACS by using Multi-authority CP-ABE

**Section 5:** Performance and Security Analysis of proposed Scheme

**Section 6:** Conclusion

2. ISSUES IN EXISTING ACCESS CONTROL SCHEMES

Security and reliability are main challenges of cloud computing. Clients are not likely to entrust their data that on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available.

**Some of these techniques are:**

✔ Encryption: Technique use complex algorithm to hide the original information with the help of encryption key.

✔ Authentication: Process which require creating a user name and password.

✔ Authorization: Practice which provides the list of authorized clients, who can access data stored on cloud system.

Some of the issues with the existing access control schemes are summarized as follows:

✔ **Technique 1:** A Secured Cost Effective Multi-Cloud Storage in Cloud Computing


✔ **Author Name:** Prof.V.N.Dhawas, Pranali Juikar, Neha Patekar, Neha Lendghar, Sushant Vartak

✔ **Disadvantages:** Complexity in implementation and dividing more securable data

**Technique 2:** A Secure Cloud Storage System with Secure Data Forwarding

✔ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013

✔ **Author Name:** Aarti P Pimpalkar, Prof. H.A. Hingoliwala

✔ **Disadvantages:** Only Partial decryption is performed by the key server and additional image login leads to unsecure access

**Technique 3:** Secured Cloud Storage using Raptor Codes

✔ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013

✔ **Author Name:** Aarti P Pimpalkar, Prof. H.A. Hingoliwala

✔ **Disadvantages:** Identification of new symbols in traditional code is capable of recovering all the input symbols even in face of a fixed fraction of erasures.

**Technique 4:** Data Security Algorithms for Cloud Storage System using Cryptographic Method

✔ **Journal name:** International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August-2013

✔ **Author Name:** Prakash G L, Dr. Manish Prateek, and Dr. Inder Singh

✔ **Disadvantages:** Performance issues and the Properties of the overheads are not analyzed

**Technique 5:** Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage (CP-ABE)

✔ **Journal name:** IEEE Transaction on Parallel and Distributed Systems, Vol.25, No. 7, July 2014

✔ **Author Name:** Kan Yang, Student Member, IEEE, and Xiaohua Jia, Fellow, IEEE

✔ **Disadvantages:** Issues computation efficiency and the revocation method

3. SYSTEM AND SECURITY MODEL

3.1 System Model

Figure 1 shows the System Model for data access control in multi-authority cloud storage is considered. There are five types of entities in the system.
1. A certificate authority (CA)
2. Attribute authorities (AAs)
3. Data owners or vendors (owners)
4. Cloud server (server)
5. Data consumers (users)

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. For each legal user in the system, the CA assigns a global unique user identity and also generates a global public key for the user. 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 entitlement and revoking user’s attributes according to their role or identity in its domain. In the proposed scheme, every attribute is associated with a multiple AA, but each AA can manage an arbitrary number of attributes. 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 and update key for each user reflecting his/her attributes.

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. The secret key is split into N pieces and stored into multiple key servers. Each owner first distributes 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.

Then, the owner sends the encrypted data to the cloud server together with the ciphertexts. 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 ciphertext; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data. The proposed scheme is able to surface the below challenges:

1) Protect user’s privacy against each single authority.
2) Tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down.
3) Provides the detailed analysis on security and performance to show feasibility of our scheme.
4) The real toolkit of multi-authority based encryption scheme is implemented.

3.2 Security Framework

Figure 2 shows a schematic representation of the proposed security framework. The framework has been built using the below defined components of layers. The proposed scheme is used to control the outsourced data and provide the standard quality of the cloud storage service for the cloud users with an efficient encryption and decryption computations and multiple key server with key splitter techniques. This multi-authority CP-ABE provides authority that is answerable for attribute management, efficient computation, key distribution and the revocation methods.

There are seven layers defined in the proposed scheme. The functionality of those layers can be summarized as follows:

- **Proxy layer**: This proxy layer acts as interface between the users and the rest of the servers available in the cloud.
- **Cloud data server layer**: Data server has two different entities can be recognized as the cloud users and the
Cloud service provider. Multiple data servers are proposed in this scheme to avoid the traffic.

- **Cloud data storage server layer**: All the data and the files are stored in these storage servers which are stored by the both individual customers and organizations. Similar to data server there are multiple storage servers are introduced to handle big volume of data.

- **Cloud Key server layer**: Multiple key servers are proposed in this scheme for efficient computation and attribute revocation method. Key server is used to store the secret key that are encrypted or fragmented by the key splitter.

- **Key splitter**: Key splitter is used to divide cryptographic key K in n safe pieces K1, K2, Kn. Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. Shamir's algorithm is to divide Key in n parts, Kz, Kn such that there is a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. However, K cannot be computed without special part Kt.

- **Cloud consumers layer**: Cloud users are the one who have the data to be stored in the cloud and depend on cloud for data computation and transformation. Cloud consumers can be both customers and individual organizations.

- **Cloud service provider (CSP)**: This layer owns, built and manages the storage servers in distributed manner and functions as live cloud computing systems.

### 4. FORTIFIED ACCESS CONTROL SCHEME

The existing framework of the scheme is modified and to make it more practical to cloud storage systems, in which data owners are not involved in the key generation. Specifically, a user’s secret key is not related to the owner’s key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners. The efficiency of the attribute revocation method is greatly improved. Specifically, in our new attribute revocation method, only the ciphertexts that associated with the revoked attribute needs to be updated, all the ciphertexts that associated with any attribute from the authority (corresponding to the revoked attribute) should be updated. A new revocable multi-authority CP-ABE protocol is proposed based on the single-authority CP-ABE proposed by Lewko and Waters in [16]. That is used to extend multi authority scenario and make it revocable. Apply the techniques in Chase’s multi-authority CP-ABE protocol to tie together the secret keys generated by different authorities for the same user and prevent collusion attack.

### 4.1 FAC Architecture

In FAC architecture, as discussed in previous section, we proposed sever layered architecture in order to improve the cloud security and accessibility.

The proposed scheme is able to safeguard each user’s privacy again single or even multiple authorities and it is lenient against authority mediation and compromising of up to N-2 node authorities does not bring the whole system down.

![Figure 3 System Architecture: Fortified Access Control for MACS](image-url)

The framework of the scheme is modified and to make it more practical to cloud storage systems, in which data owners are not enrolled in the key generation. Specifically, a user’s secret key is not related to the owner’s key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners. The attribute revocation method’s efficiency is greatly improved. Specifically, in this new proposed attribute revocation method, only the ciphertexts that associated with the revoked attribute needs to be updated, all the ciphertexts that associated with any attribute from the authority (corresponding to the revoked attribute) should be updated.

Moreover, in our new attribute revocation method, both the key and the ciphertext can be upgraded by using the same update key, instead of requiring the owner to create update information for each ciphertext, such that owners are not required to store each random number generated during the encryption. The expressiveness of our access control scheme is highly improved, where the limitation
that each attribute can be removed and only appear at most once in a ciphertext.

4.2 FAC Implementation

Figure 4 Display the system model of fortified access control for multi-authority cloud storage using CP-ABE algorithm. There are five methods proposed in this paper for the fortified access control:

1. **Key Generation and Storage**
2. **Key Splitter**
3. **Key Transfer**
4. **Key Retrieval**
5. **Distributed Key Storage**

Methods are summarized as follows:

- **Key Generation and Storage**: User can generate new symmetric cryptographic key $K$ or can store already existing cryptographic keys as required using proposed technique. Key splitter will split the key into $n$ pieces and store each part in different server. One main piece lets $K_n$ of key will be assigned to consumer of application. This piece of key has information of all other pieces and actual key cannot be regenerated without this piece.

- **Key Splitter**: User can split the cryptographic key $K$ into pieces and store it into multiple key servers in distributed manner. Key server can be located in different locations in order to tighten the security of the cloud data. Each piece of key is store in distributed server, so that hacker cannot access or retrieve the keys directly. Key splitter is one of intrinsic method introduced in fortified access control for multi-authority cloud storage.

- **Key Transfer**: User can transfer completely computed key or the component of key on public cloud for data processing. Public Key Cryptographic Standard (PKCS7) will used to transfer such key that is developed by RSA Laboratories and used to wrap data in an envelope to securely transfer it. This protocol used to wrap message in an envelope and signed by sender. Receiver knows the encryption key to decrypt the encrypted message.

- **Key Retrieval**: On the request of key retrieval all, the components will fetch the key from key store through computational server. Client machine will prompt consumer of application to enter his/her piece of key. Original Key will compute on the fly after taking information from consumer on consumer's terminal.

- **Distributed Key Storage**: The goal of this module is to divide cryptographic key $K$ in $n$ safe pieces $K_1, K_2, K_n$. Such that knowledge of any $J$ pieces can be used to compute $K$ easily. These pieces are assigned to $N$ nodes. Shamir's algorithm is to divide Key in $n$ parts, $K_1, K_n$ such that there exists a special part $K_t$ which contains the information of all other parts, and $K$ cannot be computed without $K_t$. However, $K$ cannot be computed without especial part $K_t$.

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any of the parts are sufficient to reconstruct the original secret.

5. PERFORMANCE AND SECURITY ANALYSIS OF FAC

5.1 PERFORMANCE ANALYSIS

Performance of the cloud storage system can be improved with our new proposed scheme. The performance improvements as follows:

- Separate the functionality of the authority into a global certificate authority and multiple attribute authorities which would increase the enactment of the system.

- Assigns a global UID and global AID to each user in the system to distinguish from other user in order to improve the cloud system performance. UID-User Identity, AID-Authority Identity.
✓ Extend the multi-authority scenario and make it revocable

✓ User’s secret keys generated by the different authorities are tied together to prevent collision attacks.

✓ Instead of using the system’s public key to encrypt data, our scheme requires all attribute authorities to generate their own public keys and use them to encrypt the data together with global public parameters and prevents certificate authority from decrypting the ciphertexts.

✓ Each attribute is assigned with version number to solve attribute revocation problem. When an attribute revocation happens only those components associated with the revoked attribute in secret keys and ciphertexts need to be updated.

✓ Improved efficiency by delegating the workload of ciphertexts update to the server by using the proxy re-encryption method, such that the newly joined user is also able to decrypt the previously published data, which are encrypted with the previous public keys, if they have sufficient attributes.

✓ Less communication cost since it does not require the data owner to transmit a new ciphertext component to every non-revoked user since the control is now with the cloud users

✓ The computational cost of the access control scheme is similar to normal access control scheme. Our scheme incurs much less communication and computational cost during the attribute revocation.

✓ Proposed fortified multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and efficient data access control scheme for multi-authority cloud storage systems.

5.2 SECURITY ANALYSIS

✓ Proposes great and enhanced security challenge to data access control in the cloud storage systems.

✓ It achieves both forward and backward security. The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt (backward security). The newly joined user can also decrypt the previously published ciphertexts1, if it has sufficient attributes (Forward Security).

✓ This scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server.

✓ Increased data and file security, it is very difficult for an intruder to access, misuse and destroy the original form of data in the file available in the cloud storage system.

✓ Improve the data and file security in public cloud computing environment by storing file contents in different servers.

✓ Use of multi key server which improves security. In this we generate more than one key server. And split the keys according to the number of server used. So the attacker can’t identify all the keys which are used while storing the data in cloud.

✓ The expressiveness of our access control scheme is highly improved, where the limitation that each attribute can be removed and only appear at most once in a ciphertext.

6. CONCLUSION

This paper mainly describes about the methods and algorithms, which are used for providing the high end of security in cloud storage system and accessing data effectively and securely. On measuring the different previous works, we analyzed the advantages and disadvantages of each work and finally we derived the new technique, which overcomes the drawbacks of previous work by analyzing all the information’s in all state of exploration and by providing the more secured cloud environment. Finally we conclude that CPABE scheme provides multiple authorities that are responsible for attribute management and key distribution. In this new scheme, we enhanced the computational efficiency, attribute revocation efficiency and also enriched the security in the cloud storage system. This fortified multi-authority CP-ABE is a capable technique, which can be applied in any information systems and online social networks and other big data related applications.

REFERENCES


AUTHORS

Ms. Bhuvaneswari Thangaraj has received her Bachelor degree in Information Technology (B.Tech) from Anna University, Chennai, India. Currently she is pursuing Master degree in Information Technology (M.Tech) in Maharaja Engineering College from Anna University. Her areas of interests include Cloud Systems, Artificial Intelligence, Networking, data mining etc.

Dr D.Sharmila completed her under graduation in the year 1996 and post-graduation in the year 2004. She has been awarded Doctorate in the year 2010 from Anna University, Chennai. At present she is working as Professor and Head of Electronics and Instrumentation Engineering in Bannari Amman Institute of Technology, Sathyamangalam. She has over 16 years of teaching experience. She has published her papers in 2 National and 5 International Journals. She has also presented her papers in 9 National and 8 International Conferences

S.Umarani completed her under graduation in the year 2006 and post-graduation in the year 2010. At present she is working as Assistant Professor and Head in Department of Information Technology in Maharaja Engineering, Avinashi. She has over 9 years of teaching experience and has published her papers in 4 International Journals. She has also presented her papers in 4 National and 5 International Conferences.