Fully Anonymous Data Access Provision and Attribute based Encryption Scheme for Efficient Cloud Data Privacy

G.V.M.S. Architha[1] and S. Jyothsna[2]
[1]M. Tech Student, CVR College of Engineering/CSE Department, Hyderabad, India
Email: architha.gadi@gmail.com
[2] Asst . Professor, CVR College of Engineering /IT Department, Hyderabad, India
Email: jyothsna.sundaragiri@gmail.com

Abstract: **Cloud computing is a service based distributed computing where the users can access required services on pay per use basis. Cloud enables users to store data and provides on demand accessibility. As the cloud service providers and cloud users are from different trust domains so security concerns rise out of it. Sharing of resources is the key idea behind the cloud which makes access control, a critical issue in cloud computing. Different configurations for attribute based encryption were used for cloud storage security. The work primarily deals with information protection and the access control. The current work is a semi anonymous privilege control scheme called Anony Control which provides identity and data privacy of user. Also Anony Control-F that fully prevents the information leakage of user and achieves the full anonymity has been presented. Here multiple authorities provide attributes in such a way that each authority will know only one attribute. This is called as multi authority cipher text policy attribute based encryption (CP-ABE). Which guarantees the user's personal information privacy and tolerates collusion attacks on attribute authorities.**

Index Terms: **Access control, Anony Control, Privilege control, Semi anonymity, Anony Control-F, CP-ABE**

I. Introduction

Cloud computing enables the people to share their data with others. People can share their information with others through online social networks such as Facebook and Instagram. These services facilitate communication easily but privacy and data security issues will arise. Unauthorized users and their unauthorized accessibility would be threats to cloud data. Providing data security and controlling unauthorized accessibility are the major concerns of this work.

The authorized users can access data based on access control policy. If the data storage server gets compromised, anyone who has access permission can retrieve the data that is not related to them even if they are in encrypted form. So, such kind of unauthorized access and compromise attacks must be controlled. Multiple access control mechanisms with an efficient encryption system are adopted in the cloud computing environment through ABE.

ABE can be classified into two types

- *Key-policy attribute based encryption (KP-ABE)*
- *Cipher text-policy attribute based encryption (CP-ABE).*

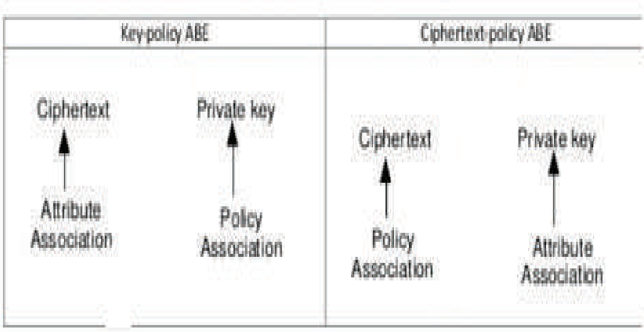


Figure 1. KP-ABE and CP-ABE

In KP-ABE access policy is associated with the private key whereas in CP-ABE, Access policy is associated in cipher text and the data owner will have complete authority about the encryption policy.

II. Related Work

Dfferent attribute based encryption techniques were proposed.

A. *Identity based Encryption*

Initially attribute based encryption called Identity based encryption was presented by "*Shamir*"[9], where the message of a sender indicates an identity and the receiver with a matching identity can only decode it.

B. *Fuzzy based Encryption*

This is a type of public-key encryption in which a cipher text and the private key of a user are based upon attributes. It is also called as attribute based encryption. In ABE algorithm keys and cipher texts are labeled with sets of descriptive attributes and a particular key can decrypt a cipher text only if there is a match between access policy and attribute set.

Anony Control-F prevents completely identity leakage of the user. The proposed scheme of action guarantees user's security against each attribute authority. Partial data is uncovered in the Anony Control scheme and no data is

doi:10.32377/cvrjst1414

revealed in Anony Control-F and can tolerate authority collusion. Multi authority based encryption schemes, Anony Control and Anony Control-F are used. The standard servers are not highly secure. To improve the data privacy on the servers, AES algorithm is used. First the data is encrypted using AES algorithm and later it is encrypted using CP-ABE.

III. Design Analysis

The data has to be confidential as the data is stored in semi trusted servers and there are multiple owners and users in cloud computing environment. For data encryption, public key encryption based schemes were used initially. But it was one to one encryption and has high key management overhead. So one-to-many encryption methods like ABE were used. Here the data is encrypted under access policy which enables users to decrypt using the relevant private key. The owner can encrypt the data without knowledge of the access control list. The main feature of ABE is that it prevents user compromise attacks.

This work is implemented using the following modules

- *Setup:* Generates master key and public key.
- *Key Generation:* Generates a private key for a set of attributes for given master key
- *Encryption:* Encrypts a file based on an access policy for a given public key
- *Decryption:* Given a private key, decrypts the file such that only users who has attributes that match the access control policy can decrypt it.

First, data is encrypted using AES and the AES keys are again encrypted and then decrypted using CP-ABE.

A. Advance Encryption Standard

The Advanced Encryption Standard (AES) is a symmetric encryption technique used to secure sensitive data. AES is based on a design principle known as a substitution–permutation network, a combination of both substitution and permutation, and is fast in both software and hardware

The step by step procedure of AES encryption algorithm using 128-bit key is presented in the following flow chart. AES is using shifting of bits and adding in each round. Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

The symmetric key is generated using AES by following the procedure given in Fig2.

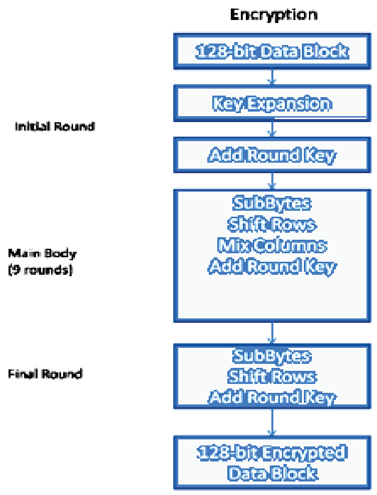


Figure 2. AES process

IV. CP-ABE Algorithm

Cipher text Multi authority ABE (CP-ABE) is used here for data access control in the cloud storage system to prevent centralization of authority. In CP-ABE scheme, user's secret key is tied to a attribute set that represents the user's permissions. A set of attributes is designed for the encryption and the decryption is possible only to the users who have the relevant attributes. Here multi authority CP-ABE is considered i.e. the set of attributes are provided by multiple authorities. Each authority will have a partial set of attributes; with this scheme security can be improved.

The Algorithm followed here is divided into two steps

1. Applied AES for generating symmetric key
2. Applied CP-ABE on the key generated in step 1

CP-ABE does not require a trusted authority like other role-based access control schemes (RBAC) or any form of storage. The encryption itself serves as the RBAC mechanism.

A. Process of Encryption

1. The data owner encrypts the file using AES, this encrypted file called as Data key
2. The above data key is encrypted using attribute set of multiple authorities using multi authority ABE scheme.
3. The encrypted file and access policies are stored in cloud.

B. Process of Decryption

1. The users request the data from the cloud server using the access keys. The user whose attribute set in private key matches the access policy in cipher text can decrypt the file
2. Downloads the decrypted file from the cloud server.

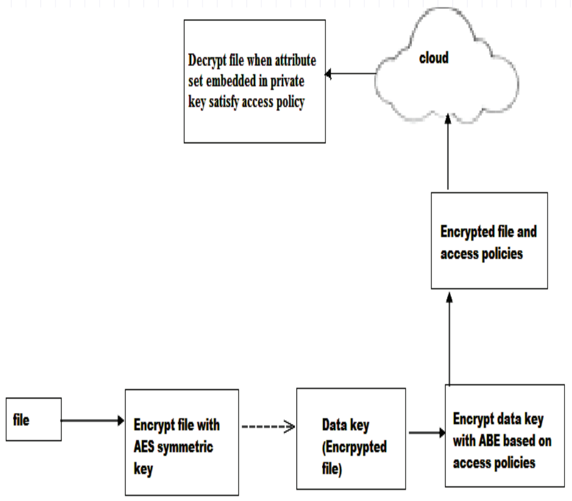

cloud
Decrypt file when attribute set embedded in private key satisfy access policy
Encrypted file and access policies
file
Encrypt file with AES symmetric key
Data key (Encrpypted file)
Encrypt data key with ABE based on access policies

Figure 3. Encrypting data with AES and CP-ABE

V. Implementation

There are four types of entities in this system.

Data Owner: Data Owner encrypts and transfers the file data into the cloud server.

Data Consumer: Data Consumer (user) decrypts and downloads the file from the cloud server.

Attribute Authority: The attribute authorities are the key generators that provide public key to the data owner and private key to the data consumer.

Cloud Server: Cloud server stores the data and provides security.

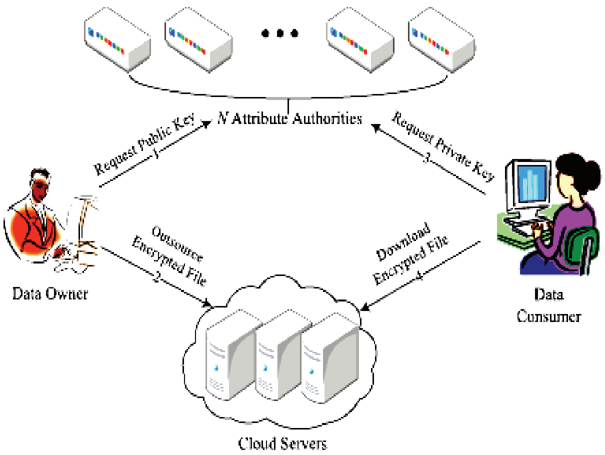


Figure 4. Architectural Flow Diagram

The data owner and the data consumer need to register with the system to access and to perform any operations on files. Central Authority should approve the users and attribute authorities. Attribute authorities provide unique private keys to users only after successful approval. Two attribute authorities are considered to provide private keys to users and these authorities provide keys without knowledge of the user identity information. Thus, anonymity is achieved.

The example considered here is medical data. Attribute authorities generate private keys against user attributes location, experience, specialization and medical degree and presents a cipher text encrypted such that only users with specified attributes able to decrypt it. USER1 have "location" and “specialization” attribute tied to their private keys, and USER2 have "medical degree" and “experience” attribute tied to their private keys. Both groups, therefore, are able to decrypt the encrypted message.

Data owner uploads an encrypted file using a public key generated by attribute authority and adds an access policy such as (India && ENT) && (MD && exp<3). Thus attribute based encryption is achieved.

Users can decrypt the file only if the attributes match the access policy. In the below example, 4 persons with a different attribute set are considered. Two persons have attributes satisfying the access control policy and two others who don’t match the access control policy.

In this example, user 3 and user 4 will not be able to access and decrypt the file and hence these users will get the popup window such as “Sorry the file cannot access by you”, but user1 and user2 can access and decrypt the file as these users can satisfy attributes which are part of access policy. With keys provided by attribute authority the users can access the files in to and from the cloud access.net. Cloud Access provides security-as-a-service from the cloud. It also provides high performance solutions managed from the cloud that meet different business needs and guarantees the protection of cloud services.

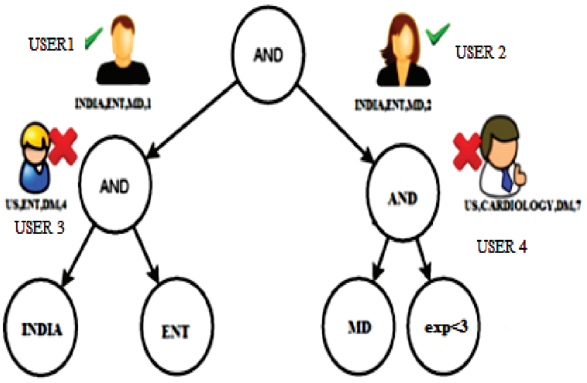


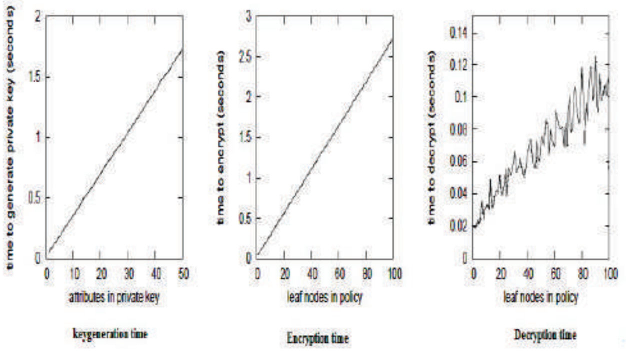
Figure 5. Access Tree

VI. EVALUATION

The performance evaluation of AnonyControl-F and CP-ABE is presented. The below figure displays measurements of private key generation time, encryption time and decryption time produced by running CP-ABE key generation, CP-ABE encryption and CP-ABE decryption on a range of problem sizes.

CP-ABE-key generation runs in time perfectly linear to the number of attributes associated with the key it issues and the running time of CPABE-encryption is almost precisely linear based on the leaf nodes in the access control policy.

The time complexity of CP-ABE key generation and CP-ABE encryption depends on the attributes in a key and the performance of CP-ABE decryption is based on the access policy tree of the cipher text and the attribute set embedded in secret key.



keygeneration time

Encryption time

Decryption time

Figure 6. Time Analysis

VII. CONCLUSIONS

The Access control policy in cloud computing is improved using AnonyControl which is a semi-anonymous attribute-based privilege control scheme and AnonyControl-F which is a fully anonymous attribute-based privilege control scheme. Anony Control-F addresses the user privacy problem in a cloud storage server. User's privacy is maintained at each level. Cipher text storage time and cost of encryption are reduced. Every authority can have a partial set of client's attributes that would not be sufficient to identify client's identity. A multi-authority CP-ABE is achieved and guarantees the confidentiality of data consumers' identity information. The system can tolerate authority compromise. The performance and security analysis proves that Anony Control is secure for data storage in cloud. The Anony Control-F inherits the security of the Anony Control.

REFERENCES

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

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

[3] 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

[4] S. Müller, S. Katzenbeisser, and C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption," *Bull. Korean Math. Soc.,* vol. 46, no. 4, pp. 803–819, 2009.

[5] Taeho Jung, Xiang-Yang Li, Senior Member, IEEE, Zhiguo Wan, and Meng Wan, Member, "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption" IEEE, VOL. 10, NO. 1, JANUARY 2015

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[7] 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.*

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

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

[10] A. Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985,pp. 47–53.

[11] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attributebased encryption supporting efficient decryption test," in *Proc. 8th ASIACCS*, 2013, pp. 511–516.