An Efficient Key Transmission Model in Attribute Based Encryption Scheme in Cloud Computing

[1]S. Praveen Kumar, [2]Gandham Bharathi, [3]Chintala Neeraj, [4]Killamsetty Akilesh,[5]Surendranath
[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[5]sureshchowdary@gmail.com
[1]Department of Information Technology,
[1]GIT, GITAM, Visakhapatnam, India

***Abstract*:**

The key transmission in the file hierarchy ABE scheme has been a preferred model for the problems that occur in cloud computing. In this paper, an efficient key transmission scheme is proposed in cloud computing. The public keys are only needed at the time of encryption; hence transmission of public keys can be handled normally. The secret keys used for decryption are transferred after authorizing the request from the user. The data owner in the proposed model encrypts the data while uploading it, hence eliminating the secure transferring. Even with the number of requests increasing the performance of the model remains

Moreover, the proposed scheme is proved to be secure under the standard assumption. Experimental simulation shows that the proposed scheme is highly efficient in terms of encryption and decryption. With the number of the files increasing, the advantages of our scheme become more and more conspicuous.

***Keywords*: Cloud computing, data sharing, file hierarchy,ciphertext-policy, attribute-based encryption, key transmission**

1.INTRODUCTION

1.1Hybrid Cloud

Hybrid cloud is a cloud computing environment that uses a mix of on premises, private cloud and third-party, public cloud services with orchestration between the two platforms [1].

[2] By allowing the switching of workloads between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment options.

1.2 Architecture of Hybrid Cloud

Establishing a hybrid cloud requires the availability of [3] A public infrastructure as a service (IaaS) platform [4] Construction of the private cloud, either using own resources or using a private CSP [5] Adequate wide area network (WAN) connectivity between those two environments

The company has no control over the architecture of the public cloud. [6] This also includes the selection of suitable hardware within the desired public cloud or clouds. This involves the implementation of suitable hardware within the data center, including servers, storage, a local area network (LAN) and load balancers.

The major method to create an advantageous hybrid cloud is to select the hypervisor and cloud layers that work with the chosen public cloud, making it certain that proper interoperability with the chosen public cloud's application programming interface (API) and services. The employment of suitable software and services also facilitate the instances to switch between the public and private clouds. A developer can develop more progressive applications using the combination of the services and resources between the public and private platforms

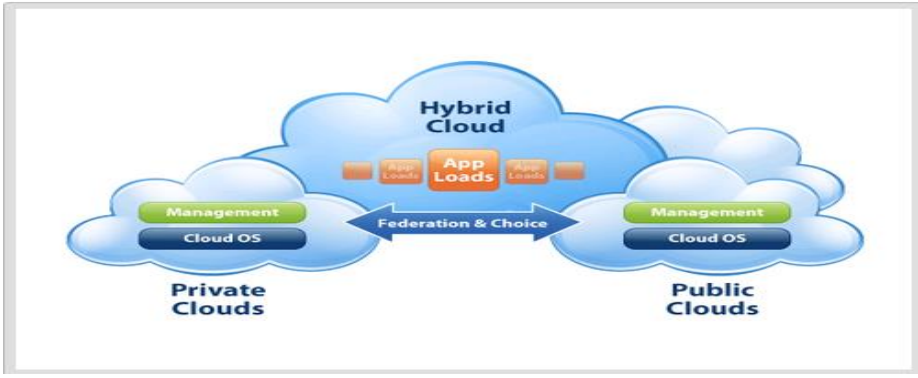


Figure1.2: Design of Hybrid cloud

1.3 Security in Hybrid Cloud

The co-located hybrid cloud approach is that all data is stored inside the private cloud, and it has the advantage of being behind firewalls at all times, even during transmission. Performance loss due to latency over WAN links is avoided, too, as is the elapsed time involved in making data replicas in the public cloud and then keeping them synchronized.

Data at rest is encrypted even the whole data is protected behind a firewall. [7] Authentication of the public cloud instances is also performed by a process of tearing down the private cloud to create and tear down public instances.VPNs are used to limit network access for public instances as an added protection.

1.4 Key Transmission in Hybrid Cloud

The key generation in the model is initiated primarily by obtaining the primary key and master secret key which later is paired with a set of attributes and create a secret key. The secret key is then transmitted by the authority to requested module.

Key transmission is the key factor in the security of hybrid cloud as the data stored may be a public cloud and the transmitted data is encrypted hence the key is required to decrypt the data. The public key is used to encrypt the data.

1.5 Data Sharing in Hybrid Cloud

Data sharing in a hybrid cloud computing environment is a common data center is used to manage all the data. Using Data Sharing we share data among the different cloud user. In the Large IT sectors all offices, research, development centers are all connected together to form a hybrid cloud environment. The user from one cloud need to access the data of another cloud need to send requests to the common data center. Based on the request data provided to the user. The Data center has a large database it contains all cloud data in the network It include project details, timeline details, development details, environment details. Data center doesn't share the whole data with the cloud user it shares only required data for a user for example, researchers need only development details and environment details and others details are kept secure.

2. LITERATURE SURVEY

2.1 Attribute based encryption (ABE)

First presented the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these replicas is to provide security and access control. [8] The main aspects are to provide tractability, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is „Attribute Based Encryption (ABE) "scheme was introduced which consist of key policy attribute based encryption (KP-ABE). A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher text and user secret key. Differs from conventional public key cryptography such as Identity-Based Encryption, CP-ABE is used on one-many type encryptions in which cipher texts are encrypted to many users,, but not only for single user. The scheme proposed by Sahai and Waters, the threshold semantics are very cheap to be used for designing more common general access control system. Cipher-Text Attribute-Based Encryption (CP-ABE) in which the encryption is embedded with specified policies.

2.2 Key Policy Attribute Based Encryption (KP-ABE)

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. Setup: Algorithm takes input K as a security parameter and returns PK as public key and a system master secret keyMK.PK is used by message senders for encryption. MK issued to generate user secret keys and is known only to the authority.Encryption: Algorithm takes a message M, the public keyPK, and a set of attributes as input. It outputs the cipher text

2.3 E KEY GENERATION

Algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches Structure T. The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme.

2.4 Cipher text Policy Attribute-Set Based Encryption (CPASBE)

CP-ABE scheme in which the decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. To solve this problem, cipher text-policy attribute-set based encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et al [8]. ASBE is an extended form of CPABE which organizes user attributes into a recursive set structure. Cipher text Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The desirable feature and the recursive key structure is implemented by four algorithms, Setup, KeyGen, Encrypt, and Decrypt 1. Setup: Here is the depth of key structure. Take as input a depth parameter „d". It outputs a public key PK and master secret key MK. 2. Encrypt: Takes as input the public key PK, a message M, and an access tree T. It outputs a cipher text CT. 3. Decrypt: Take as input a cipher text CT and a secret key SK for user u. It outputs a message m. If the key structure A associated with the secret key SK, satisfies the access tree T, associated with the cipher text CT, then m is the original correct message M. Otherwise, m is null. User attributes are organized into a recursive family of sets and Allowing attributes to combine from multiple sets. Thus, by grouping user attributes into sets and no restriction on how they can be combined, CP-ASBE can support compound attributes. More flexibility and fine grained access is provided by AP-ASBE. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set as well as placing it into a single set.

3.RESEARCH METHODOLOGY

In this study, an efficient key transmission scheme on file hierarchy model access structure is proposed in cloud computing, which is named file hierarchy model CP-ABE (FH-CP-ABE for short). FH-CP-ABE improvises the typical CP-ABE with a better hierarchical structure policy

of access control. The proposals of our model are two facets. Firstly, we propose the efficient key transmission model in the FH-CP-ABE scheme that can reduce the storage cost. Secondly, we also formally prove the security in the FH-CP-ABE model that withstands the attacks.

3.1 Key Generation

The key generation is done primarily by setting up the security parameters. The combination of the security parameters and random numbers generates the public key P K, master secret key M S K.

The public key and master secret key are combined with a set of attributes which creates a secret key S K.

The encryption is thus done by using the public key P K, content keys c k and a hierarchical access tree as input and outputs the integrated cipher text.

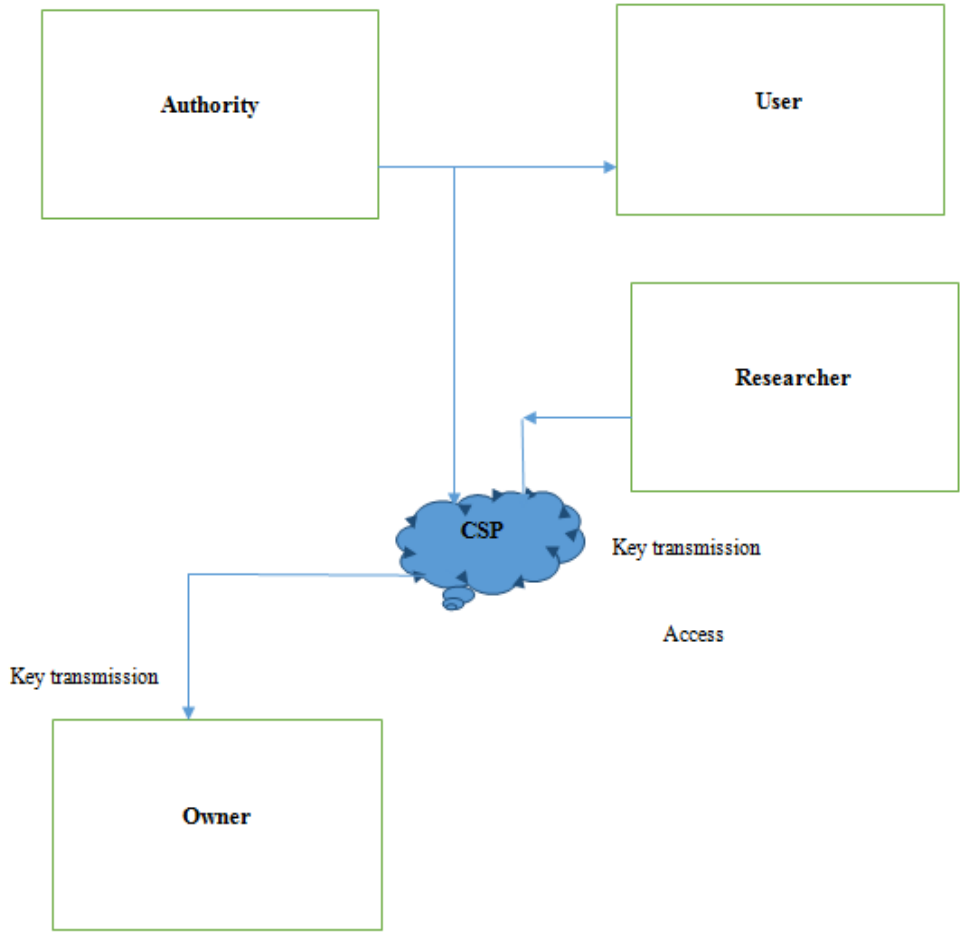
The decryption needs public key P K, secret key S K, where the cipher text can be decrypted.

3.2 Data Security

The provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

3.3 Efficient Model for Key Transmission

Figure3.3: Efficient model for key transmission

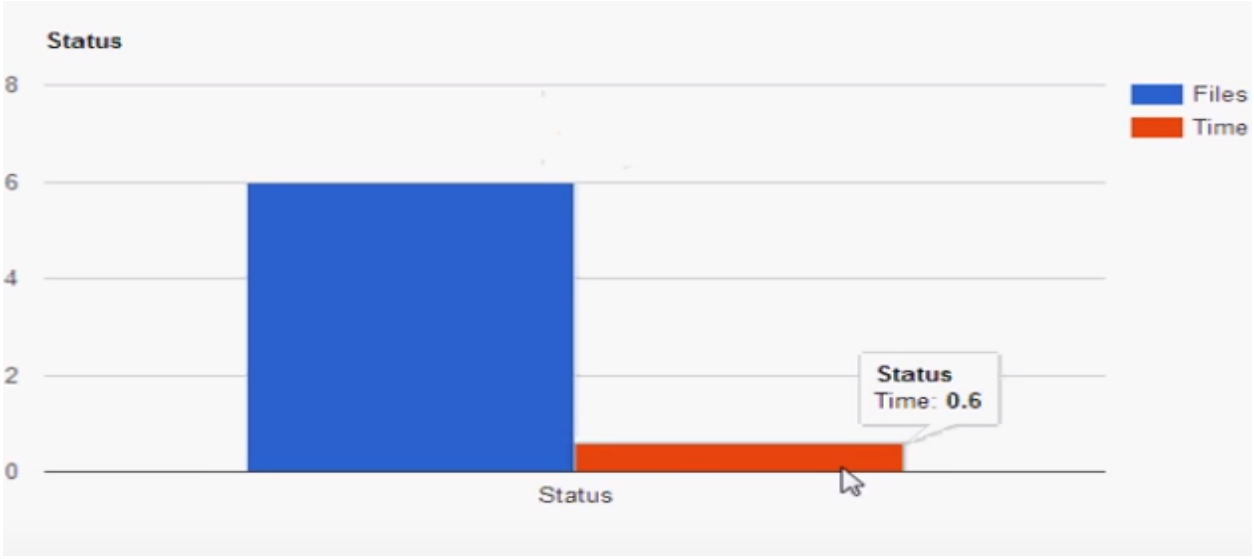


The key transmission in the model is performed only when the encryption or decryption operations are performed. The minimal activity of the key makes it secure (harder to track at the time of attack). The owner module performs the data entry process into the cloud. As the FH-CP-ABE the data is encrypted before uploading into the cloud.

The encryption is done using the public key. The public key is a shared key hence normal transmission is done. The users access the files from the cloud by decrypting the files with a secret key. All the key transmissions are handled by the authority module which shares the key to authorized users

4. RESULT:

.



5. CONCLUSION:

In this paper, we proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption

.

6. REFERNCES:

[1]Jin Li, Yan Kit Li and Xiaofeng Chen, "A Hybrid Cloud Approach for Secure Authorized Deduplication" IEEE Transactions on Parallel and Distributed Systems (Volume: 26, Issue: 5, May 1 2015) 18 April 2014

[2]T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryp-tion with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, vol. 8712. Sep. 2014, pp. 130–147.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp.Secur. Privacy*, May 2007,pp. 321-334.

[4] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Proc. 20th Eur. Symp. Res. Comput. Secur.(ESORICS)*, vol. 9327. Sep. 2015, pp. 146–166.

[5] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. 29th Annu. Int. Conf.Theory Appl. Cryptogr.Techn.*, vol. 6110. May 2010, pp. 62–91.

[6] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator," in *Proc. 16th Int. Conf. Inf. Commun. Secur.*, vol. 8958. Dec. 2014, pp. 274–289.

[7]J.K.Liu,M.H.Au,X.Huang,R.Lu,andJ.Li,"Fine-grainedtwo-factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.

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

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun.Secur., Oct. 2006, pp. 89–98.

[10] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin.J.Electron., vol. 23, no. 4, pp. 778–782, Oct. 2014.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp.Secur. Privacy, May 2007, pp. 321–33