A SECURE WAY OF DATA SHARING BY IMPROVED TWO-PARTY KEY ISSUING SCHEME IN CLOUD COMPUTING

Bhavana C. Julme[1], Mohini R. Jadhav[2], Sarika K. Kaulage[3], Apurva S. Wable[4]

[1]Assistant Professor, PVG's COET, Pune-09
[2]PVG's COET, Pune-09.
[3]PVG's COET, Pune-09.
[4]PVG's COET, Pune-09.

Abstract

Cloud computing is a most convenient and popular way for data sharing which brings various benefits like providing computational resources on demand, cost saving, agility, scalability and flexibility for societyas well as for individuals. The massive amount data shared on cloud storage system contains very valuable information which should provide a high security to data. Cipher text policy attribute based encryption (CP-ABE) is most used technology to deal with the challenge of providing secured data. In existing CP-ABE schemes, data owner has full authority to control the access policy of shared data on cloud. However CP-ABE leads to key escrow problem and also fails to support many facilities to the users of the data. In this paper we are revisiting the attribute based data sharing scheme in order to remove the key escrow problem as well as improve the efficiency and security of shared data resources on cloud storage

Keywords *— Cloud Computing, Attribute Based Encryption, Secure Data Sharing, Removing Key Escrow, And Key Distribution.*

----------***----------

1. INTRODUCTION

Cloud computing is a paradigm which provides computation capacity and huge memory space at a low cost. It also enables users to get intended services irrespective of time and location across multiple platforms and thus brings great convenience. Among numerous services provided by cloud computing such as Apple's iCloud [5], Microsoft's Azure [6] and Amazon S3 [7] can offer more flexible and easy way to shared data over the internet which provides various benefits for our society [4].However, it also suffers from several security threats, which are primary concern of cloud users. Firstly, the outsourced data usually contains valuable and sensitive information whose full control access is with data owner and key authority. Secondly, data sharing is often implemented in an open and hostile environment, cloud server would become a target of attacks. Even worse, cloud server itself may reveal owner's data for illegal profit.

Ciphertext-policy attribute-based encryption (CP-ABE) is an important encryption technology where the secret key is described by an attribute set and ciphertext is associated with an access structure. The data owner (DO) who will upload the data on cloud system can define the access structure for the retrieval of data. The data user can decrypt the data only if the attribute set matches the access structure of the data.

In this paper, we are introducing concept of sharing of data over the cloud system by sharing the key generation process between key authority and cloud service provider (CSP).This perspective improves the key generation technique along with the improved secure way of key generation. The data owner, data provider can be able to choose an access policy based on specific knowledge that underlying data. Furthermore, this owner may or may not know about the data users requirements for accessing the data but owner have this only way to decide the accessing policies in terms of attributes [2]. The data owner generates the data and decides the accessing policies according to the importance of that data. Whenever the data is uploaded, data is secured by encryption techniques using encryption keys generated by collaboration of CSP and KA both. The data users will fetch the data by requesting CSP and KA for accessing the original data. The decryption process will be initiated by using decryption keys. Furthermore, the decided access policies will enhance the security of the data.

1.1 Related Work

S. Wang, K. Liang and J. K. Liu proposed the key issuing protocol to resolve the key escrow problem but also reduce the complexity of access policies. It enhances the data confidentiality and privacy in cloud system [1]. In order to the security for the framework, solution based on identity-based encryption technique was implemented for big data information management. The cloud computing management was done by computing centres using hierarchical levels to manage the access policies [8]. The access control encryption where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over their attributes specifying the user's authority [2]. The data provider will decide a predicates for sharing data and user will be provided with a

secret key along with credentials. A new technology for realization of CP-ABE system for general set of access structure in standard model under concrete and non-interactive assumptions [9]. The central authority in constructing the power to decrypt every ciphertext which is somehow contradictory to the aim of distribution of control to untrusted authorities [10]. In CPABE scheme if an attribute is revoked the user cannot use it in the decryption phase. The scheme allows the encryption to encrypt the message according to an access policy over a set of attributes. If the access policy is satisfied and if the attributes are not revoked they can only decrypt the ciphertext [11].

1.2Our Contributions

We are presenting CP-ABE scheme by successfully resolving key escrow problem as well as improving expressiveness of data by the declaration attribute.

1. We implement key generation process by collaborating KA along with CSP. This will improve the key generation process as none of the single element from CSP or KA can create the whole secret key.
2. We propose the access policy structure by data owner which will decide weight of the data and improves the confidentiality and privacy can be insured.

2. SYSTEM MODEL

The framework of CP-ABE scheme in cloud computing consists of four types of elements. The further paper provides the detailed information about every elements.

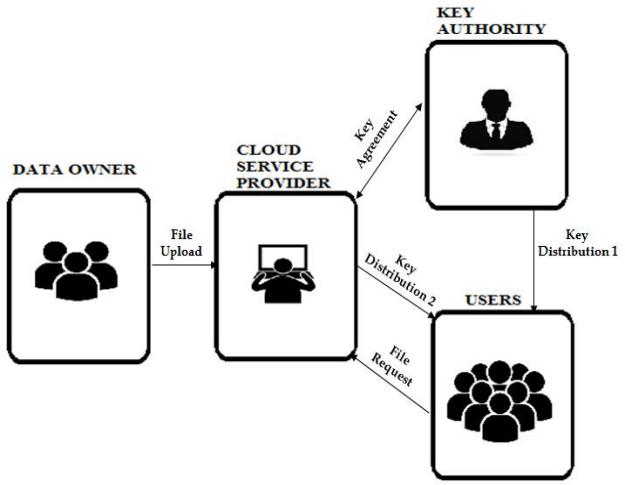

Fig 1: System model for Encryption by two party key Issuing Scheme

1. Cloud Service Provider (CSP): The most important part or we can call manager of cloud server and also a semi-trusted entity. This element provides so many services such as data storage, management, encryption, computation and transmission. In cloud service provider, we are designing a scheme which will generate half part of key along with the system parameters.

2. Key Authority (KA): This is another semi-trusted entity which performs the task of creating another half part of key which is required for encryption or decryption purpose. Key authority is responsible for holding the secretive information about keys.

3. Data Owner (DO): These are the owners and creators of the information which will be stored on cloud system. The aim of defining access structure in charged by data owners. They are responsible for uploading the ciphertext to CSP.

4. Users: This element of system model wants to access the ciphertext uploaded on cloud system. If the attributes of the users matches with the access policies user will be allowed to access the data.

This scheme contains four phases which contains the whole process of encryption and decryption:

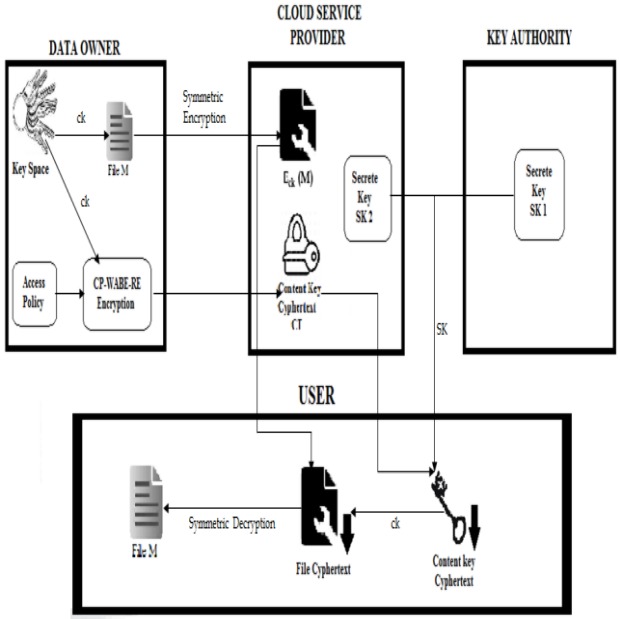

Fig 2: Architecture of Encryption by two party key Issuing Scheme

Phase 1: System Initialization
The first phase contains two setups.

1. **KA Setup:**The half part of master secret key (MSK_1) is generated in this setup phase.
2. **CSP Setup:**The remaining half part of master secret key (MSK_2) is generated here.

The whole master secret key (MSK) is the combination of these two keys (MSK_1, MSK_2) creator in setup phases.

Phase 2: Data Owner Encryption
This second phase contains two encryption processes.

1. **File Encryption:**For the file encryption the data or file M with content key (ck) is needed. The output encrypted file is E_{ck} (M).
2. **Content Key Encryption:**The encryption of content key (ck) is done by access policy (A) which outputs Content key ciphertext (CT).

Phase 3: User Key Generation

This third phase includes Key authority and Cloud service provider Key generation phases.

1. **KA KeyGen:**For generating Secret key (SK_1), Master Secret Key (MSK_1) and weighted attribute S are required.
2. **CSP KeyGen:** In this key generation phase Master Secret Key (MSK_2) is used to generate Secret Key (SK_2) as output.

The user creates the secret key (SK) by using the secret keys generated by both the sub phases of KA and CSP.

Phase 4: Data Decryption

The last phase for retrieving the original data two decryption phases are included.

1. **Key Decrypt:**The original Content Key (ck) is obtained by decryption of Secret Key (SK) using Content key ciphertext (CT).
2. **Data Decrypt:**The decryption of encrypted file $E_{ck}(M)$ is done by using decrypted Content Key (ck).

3. CONCLUSION

In this paper, we implemented CB-ABE scheme by removing key escrow problem in cloud computing. The improved CP-ABE scheme enhances the data security and privacy by providing confidentiality using access policy structure. In this scheme, the key generation process by collaboration of KA and CSP improved the performance and security analysis for enhancing the efficiency and security

REFERENCES

[1]. S. Wang, K. Liang, J. K. Liu. Attribute based data sharing scheme revisited in cloud computing. IEEE Transaction on Information Forensics and security, 2016.

[2]. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute based encryption. *IEEE Symposium on Security and Privacy*, pages321–334, 2007.

[3]. M. Chase and S. S. Chow. Improving privacy and security in multi authority attribute based encryption. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pages 121–130, 2009.

[4]. Jiang hong Wei, Wenfen Liu, Xuexian Hu. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption. IEEE Transactions journal of latex class files VOL. 15 NO. 8 August 2015.

[5]. iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[6]. Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com

[7]. Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[8]. J. Baek, Q. Hieu Vu, J. K. Liu, X. Huang, Y. Xiang. A secure cloud computing based framework for bid data information management of smart grid. IEEE Transactions on cloud computing, 2014.

[9]. B. Waters. Ciphertext policy attribute based encryption: An expressive, efficient and provably secure realization. International Association for Cryptologic Research 2011.

[10]. M. Chase, S. M. Chow. Improving privacy and security in multiauthority attribute based encryption. *ACM Conference 2009.*

[11]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker. Mediated ciphertext policy attribute based encryption and its application. Springer-Verlag Berlin Heidelberg 2009.