SECURE DATA SHARING USING USER SIDE ENCRYPTION IN CLOUD COMPUTING

Abirami R, Buvaneswari A.M, Gayathri K, Harini R

Student, Computer Science and Engineering, SRM Valliammai Engineering College, TamilNadu, India
Student, Computer Science and Engineering, SRM Valliammai Engineering College, TamilNadu, India
Student, Computer Science and Engineering, SRM *Valliammai Engineering College, TamilNadu, India*
Student, Computer Science and Engineering, SRM Valliammai Engineering College, TamilNadu, India

ABSTRACT

Cloud computing is main purpose of data storing and retrieving data in data owners or users so data owners upload some sensitive data in cloud so only valid user retrieve the data so we design attribute-based data searching in cloud computing, become a research hot-spot due to its distinguished long-list advantages. Ciphertext-policy attribute-based encryption (CP-ABE), has turned to be a crucial encryption technology to tackle the challenge of secure data sharing. In the CP-ABE, user’s secret key is by an attribute set, and ciphertext is associated with an access structure. In a CP-ABE, user’s secret keys described by an attribute set, and ciphertext is said to an access structure. Data owner is allowed to access structure over the universe of attributes. A user can decrypt a given ciphertext as long as his/her attribute set matches the access structure over the ciphertext. Employing a CP-ABE system directly into a cloud application which can yield some open problems. All users’ secret keys need to be issued by a completely trusted key authority (KA).

Keyword *User, Data Owner, key, Cipher text, Data Provider,Attribute based encryption*

1. INTRODUCTION

One of the foremost promising cloud computing applications is on-line data sharing, like photo sharing in On-line Social Networks among quite one billion users and on-line health record system. a knowledge owner (DO) is usually willing to store large amounts of data in cloud for saving the worth on local data management. with none data protection mechanism, cloud service provider (CSP), however, can fully gain access to all or any or any data of the user. This brings a possible security risk to the user, since CSP may compromise the data for commercial benefits. Accordingly, the thanks to securely and efficiently share user data is one of the toughest challenges within the scenario of cloud computing. Firstly, all users’ secret keys need to be issued by a completely trusted key authority (KA). This brings a security risk that's mentioned as key escrow problem. By knowing the key of a system user, the KA can decrypt all the user’s ciphertexts, which stands in total against to the will of the user. The expressiveness of attribute set is another concern. As we all know,most of the prevailing CP-ABE schemes can only describe binary state over attribute, during this paper, the weighted attribute is not only extend attribute,but also to simplify access policy. The storage cost and encryption cost for a ciphertext are often relieved. Cipher text-policy attribute-based encryption (CP-ABE), has turned to be a crucial encryption technology to tackle the challenge of secure data sharing.In a CP-ABE, user’s secret key's described by an attribute set, and ciphertext is related to an access structure.DO is allowed to define access structure over the universe of attributes. A user can decrypt a given cipher-text as long as his/her attribute set matches the access structure over the ciphertext. Employing a CP-ABE system directly into a cloud application which can yield some open problems. Firstly, all users’ secret keys need to be issued by a completely trusted key authority (KA). This brings a security risk that's referred to as key escrow problem.By knowing the key key of a system user, the key authority can decrypt all the user’s ciphertexts, which stands in total against to the will of the user know, most of the prevailing CP-ABE schemes can only describe binary state over attribute, in paper, the weighted attribute isn't just for extend attribute expression from binary to arbitrary state, also to simplify access policy. The storage cost and encryption cost for a ciphertext are often relieved

2. RELATED WORKS

The existing pairing-based ABE schemes the number of pairing operations to decrypt a ciphertext is linear to the complexity of the access policy.It would be a significant challenge for users to complete the decryption independently on resource-constrained devices, e.g., mobile phones.In order to reduce the number of pairing operations for users when executing the decryption algorithm, considered outsourcing the heavy computation of decryption to a third-party service, which helps to implement “thin clients.” Existing pairing-based AB-KEMs (KP or CP) satisfy the property of multiplicative homomorphism. Thus, our technique are often applied to most existing AB-KEMs in both KP and CP settings. It provided a requirement of verifiability to the decryption of ABE, but their scheme doubled the size of the underlying ABE ciphertext and the computation costs.Low capacity of users.Possible to some person misbehave to data access

3. PROPOSED WORK

A more efficient and generic construction of ABE with verifiable outsourced decryption supported an attribute based key encapsulation mechanism, a symmetric-key encryption scheme and a commitment scheme. Then, we prove the safety and therefore the verification soundness of our constructed ABE scheme within the standard model. consistent with the cipher text related to an access policy or containing a group of attributes, ABE schemes are divided into two kinds: ciphertext policy (CP) ABE [1] and key-policy (KP) ABE [2]. We apply MD5, Triple DES, ANT algorithm an appropriate transform for the particular secret key to realize outsourcing the decryption. In fact, the transform we used here could also be thought as a subclass of all-or-nothing transforms (AONT).

4.ARCHITECTURE

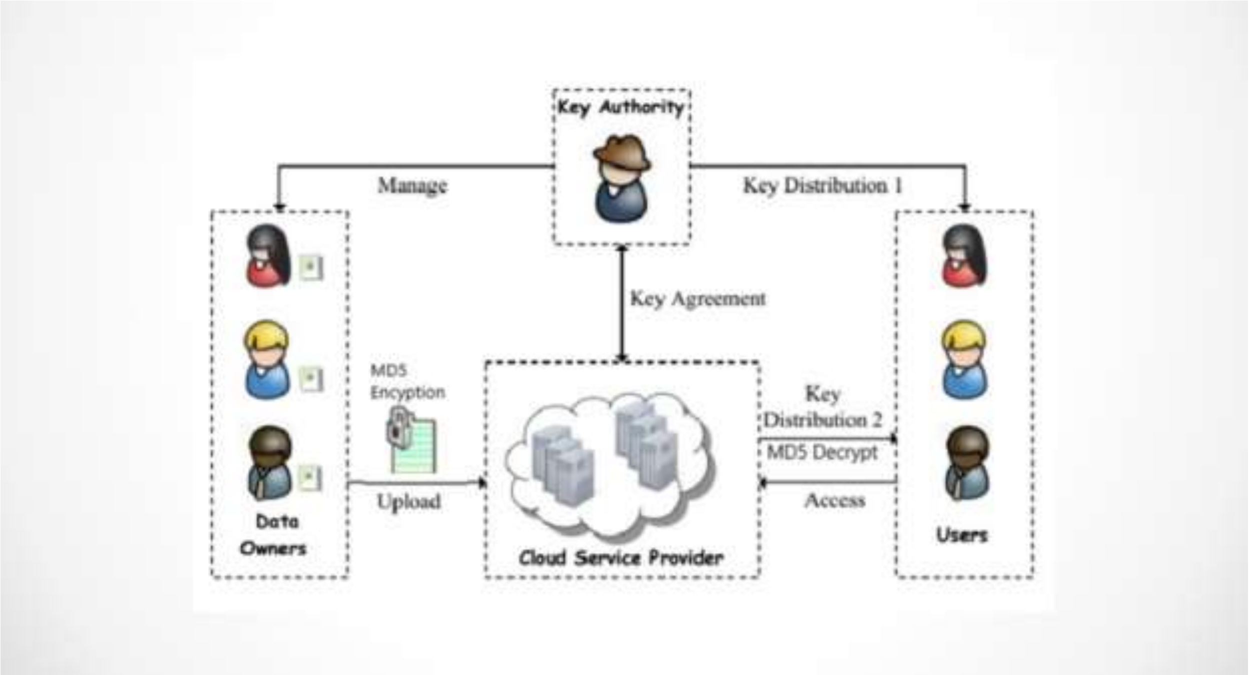

Figure 1: Architecture diagram for the system

Figure – 1: Data provider upload file which are going to be encrypted and stored within the Storage server. Key Authority assigns a key to every file. Users will enter the key that ought to be matched with Data provider, then the info file are going to be accessed by the authorised users.Intruders or third parties will view the encrypted file only.

5.MODULES

- Key Authority
- Cloud Service Provider
- Data Confidentiality
- Data Owner

5.1 KEY AUTHORITY

It's a semi-trusted entity in cloud system. Namely, Key Authority is honest- but-curious, which may honestly perform the assigned tasks and return correct results. However, it'll collect as many sensitive contents as possible. In cloud system, the entity is liable for the users' enrolment. Meanwhile, it not only generates most a part of system parameter, but also creates most a part of secret key for every user.

5.2 CLOUD SERVICE PROVIDER

It's the manager of cloud servers and also a semi-trusted entity which provides many services like data storage, computation and transmission. to unravel the key escrow problem, it generates both parts of system parameter and secret key for every user.

5.3 DATA CONFIDENTIALITY

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To take care of the supply of knowledge confidentiality for dynamic groups remains a crucial and challenging issue. Specifically, revoked users are unable to decrypt the stored file after the revocation

5.4 DATA OWNER

They're owners of files to be stored in cloud system. they're responsible of defining access structure and executing encoding operation. They also upload the generated cipher text to Cloud Service Provider. Users. they need to access cipher text stored in cloud system.

6. ACTIVITY DIAGRAM

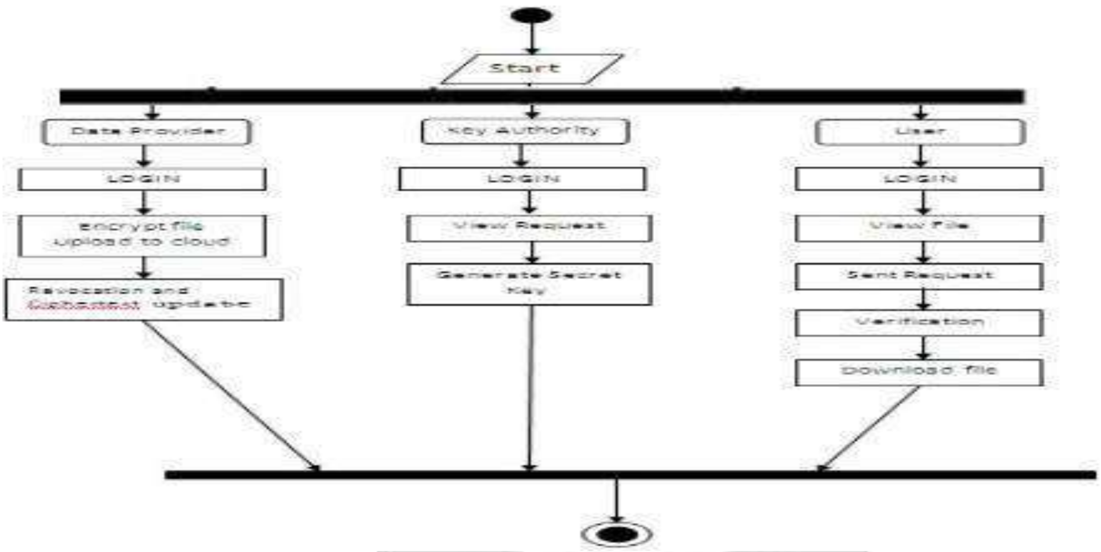

Figure - 2 : Activity Diagram

Figure – 2: It explains the what kind of activity that data provider, key authority and user does.

7. USE CASE DIAGRAM

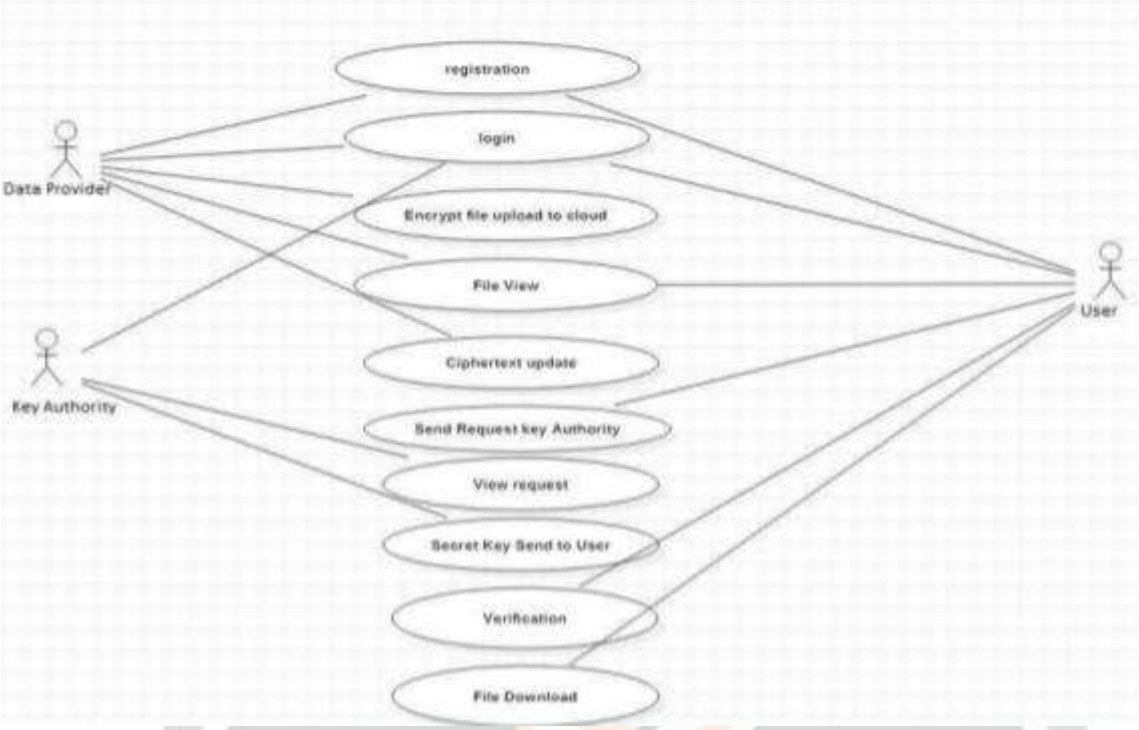

Figure – 3: Use case diagram

Figure – 3: It explains the overall user and data owner process for encryption and decryption.

8. ALGORITHM USED

MD5 message-digest algorithm is that the 5th version of the Message-Digest Algorithm developed by Ron Rivest to provide a 128-bit message digest.MD5 is kind of fast than other versions of the message digest, which takes the plain text of 512-bit blocks, which is further divided into 16 blocks, each of 32 bit and produces the 128-bit message digest, which may be a group of 4 blocks, each of 32 bits. MD5 produces the message digest through five steps, i.e., padding, append length, dividing the input into 512-bit blocks, initialising chaining variables a process blocks and 4 rounds, and using different constant it in each iteration.MD5 produces an output of 128-bit hash value. This encryption of input of any size into hash values undergoes 5 steps, and each step has its predefined task.

8.1 MD-5 steps:

- Append Padding Bits
- Append Length
- Initialize MDBuffer
- Processing message in 16-word block

9.CONCLUSION

In this we designed an attribute-based data sharing scheme in cloud computing.The improved key issuing protocol was presented to resolve the key escrow problem. It enhances data confidentiality and privacy in cloud system against the managers of KA and CSP also as malicious system outsiders, where KA and CSP are semi-trusted. additionally, the weighted attribute [1] was proposed to reinforce the expression of attribute, which can not only describe arbitrary state attributes, but also reduce the complexity of access policy, so as that the storage cost of ciphertext and time cost in encryption are often saved. Finally, we presented the performance and security analyses for the proposed scheme, during which the results demonstrate high efficiency and security of our scheme.

10. REFERENCES

[1] L. Cheung and C. Newport. Provably secure ciphertext policy ABE. Proceedings of the 14th ACM conference on Computer and communications security, pages 456–465, 2007.

[2] A. Balu and K. Kuppusamy. An expressive and provably secure ciphertext- policy attribute-based encryption. Information Sciences, 276(4):354–362, 2014.

[3] J. Hur. Improving security and efficiency in attribute-based data sharing. IEEE Transactions on Knowledge and Data Engineering, 25(10):2271– 2282, 2013.

[4]. Revathi K, A.Samydurai, "Adaptive Deep Convolutional Neural network based Secure Integration of Fog to Cloud Supported IOT for Health Monitoring System", Transactions on Emerging Telecommunications Technologies, Online ISSN:2161-3915, Vol.31, Issue 10, pp.1-18, 2020.

[5] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. Journal of Cryptology, 17(4):297‐319, 2001.

[6] M. Chase. Multi-authority attribute-based encryption. Proceedings of the 4th Conference on Theory of Cryptography, pages 515‐534, 2007.

[7] M. Chase and S. S. Chow. Improving privacy and security in multiauthority attribute-based encryption. Proceedings of the 16th ACM Conference on Computer and Communications Security, pages 121‐130, 2009.

[8] L. Cheung and C. Newport. Provably secure ciphertext policy ABE. Proceedings of the 14th ACM conference on Computer and communications security, pages 456‐465, 2007.

[9] S. S. Chow. Removing escrow from identity-based encryption. Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, pages 256‐276, 2009.

[10] C. K. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou. Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50‐57, 2013.