A SECURE ANTI-COLLUSION DATA SHARING SCHEME FOR ADVANCED ENCRYPTION STANDARD IN CLOUD COMPUTING

P. ASHWINI
Assistant Professor in Computer Science and Engineering Department ,
Springfields Engineering College,
Hyderabad, Telangana.

Abstract
Cloud Computing, users can achieve an growing and balanced methodology for data sharing among the group members and individuals in the cloud with the characters of tiny management and tiny maintenance cost. It provides a security certification for data sharing because outsourced data's are at risk .Due to frequently changing the memberships in the group provide privacy preserving issue ,mainly for an untrusted cloud due to collusion attack or pilot attack. In existing system key distribution is based on secure communication channels[1]. In that key is known to everyone and implementation is very difficult to practice. In this paper, we propose a key distribution without any communication channel and the user can know their private key from their group manager in secured manner. AES Algorithm is used for data encryption and decryption techniques and ring signature is used for key distribution between the group members.
Key Words:*AES Algorithm, Ring signature, pilot attack, cloud computing, privacy preserving.*

1.INTRODUCTION

Cloud Computing ,with characteristics of natural information data sharing with low maintenance and better utilization of resources. In this data can be shared data in secured manner, in cloud it can be achieve secure data sharing in dynamic groups. Cloud computing offers an infinite storage space. In our scheme, secured data sharing can be protected from collusion attack. In this paper the main contributions of this scheme include:

1. The key distribution without any communication channel and the user can securely know their private key from their group manager without any certificate authority because of verification of public key of the user .

2. This scheme can achieve fine grain access control, any user in the group can access their resources and revoked user cannot access the data in the cloud after they are rejected.

3. This can protect collusion attack which means the revoked user cannot get original data from the cloud.

Our scheme can achieve secure user revocation with the help of polynomial function.

4. This scheme are able to achieve fine efficiency, scheme achieve fine efficiency, that is previous users need not updated they are private key when new user adds or rejected from the group.

2.EXSITING SYSTEM

In existing techniques of key policy attributes based on "lazy re-encryption, proxy re-encryption and encryption" to achieve fine-grained data access control without disclosing data contents. In this

schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. It is based on encryption techniques due to secure provenance by leveraging group signature and cipher text. Each user obtains two keys after the registration while the attribute key is used to decrypt the data[16].

Every user in the group gets two key after registration when the private key is used to decrypt the data. Role based encryption techniques is used for secure access control scheme on encrypted data in cloud storage. This scheme can achieve efficient user revocation that combines role-based access control policies with encryption to securely store large data in the cloud. Private key is easily cause collusion attack and can take sensitive data files. The verifications between entities are not concerned.

2.1 Disadvantage in existing system:

- It is difficult to design a secure and efficient data sharing scheme.
- The system had a heavy key distribution overhead.
- The verifications between entities are not concerned, the scheme easily suffer from attacks, for example, collusion attack It is not secure because of the weak protection of commitment in the phase of identity token.

3.PROPOSED SYSTEM:

A secure data sharing scheme proposes, which can achieves the key distribution is secured and sharing the data for dynamic groups. . Key is distributed securely without any communication channels. The user can obtain their private key from the group manager without any certificate authority due to the verification of public key of theuser[15]. Our scheme achieves the fine grained access control with the help of group members list, any members in the group can use the resources in cloud and revoked user cannot access their original data in cloud after they are revoked. It can achieve secure user revocation with the help of polynomial function. It support dynamic group efficiency the other user in the group need to update or recomputed their private key when new user joins or user revoked from the group.

3.1 Advantages:

- It supports dynamic group efficiency.
- The other user in the group need to update or recomputed their private key when new user joins or user revoked from the group.
- The user can securely obtain their private key from the group manager without any certificate authority.
- Propose a secure data sharing scheme which can be protected from collusion attack.

4.SYSTEM ARCHITECTURE:

The system architecture consists of three entities they are large number of group manager, group member, and cloud[16]. Cloud is maintained by the cloud service

provider they provides the storage space for hosting the data files as pay-as-you-go manner. The group manager will generate a private key to all the group members. Group manager takes charge of adding the user and revocation of the user. All the group member will store their data files in cloud and share them to others. In the plan, the gathering enrollment is powerfully changed, because of the new client added and user rejection.

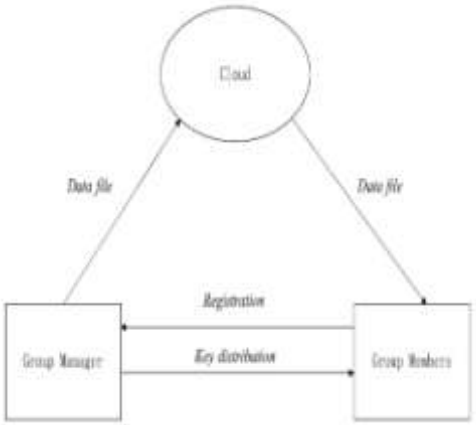

Fig -1: System Architecture

5. ALGORITHM/TECHNIQUE USED:

5.1 Advanced Encryption standard (AES)

5.2 Ring signature

5.1Advanced Encryption standardDescription:

AES is a symmetric block cipher,

- It is based on secret key encryption algorithm[2].

- AES is sequence of 128,192 and 256, no other bits are supported. Based on the bit it will go to cipher engine and it will produce a cipher text.

- A cipher key of AES is also sequence of 128,192 and 256 bits.

- Same step will be performed for both encryption and decryption in reverse order.

- 10,12,14 rounds for 128,192,256 bit keys.

- This key is expanded into individual sub keys, for each operation round. This process is called Key Expansion.

- Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key.

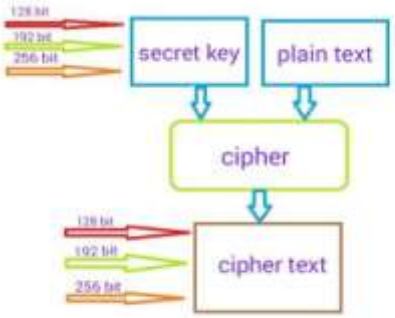

Fig -2: Working Flow of AES

- AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'.
- It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs substitutions and others involve shuffling bits around permutations.
- AES performs all its computations on bytes rather than bits. AES treats the 128 bits of a plaintext block as 16 bytes.

- These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key.
- AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.
- Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows − First row is not shifted. Second row is shifted one byte position to the left. Third row is shifted two positions to the left. Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.
- MixColumnsEach column of four bytes is now transformed using a special mathematical function.

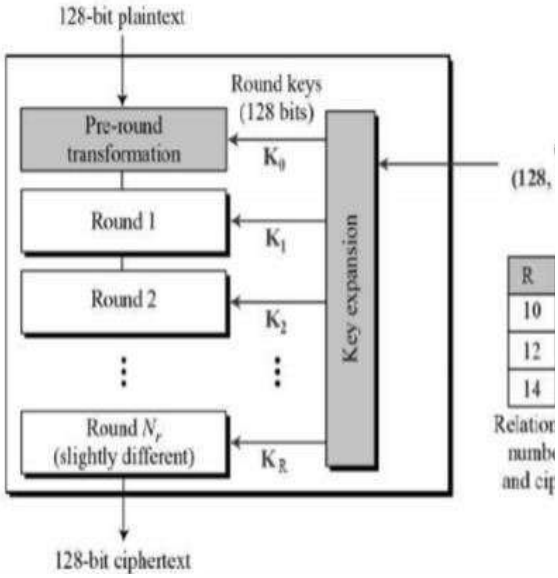

Fig -3:Operations

Encryption Process:which replace the original column. Description of a typical round of AES encryption.

The result is another new matrix consisting of 16, Each round comprise of four sub-processes. The first new bytes. It should be noted that this step is not round process is depicted below, performed in the last round.

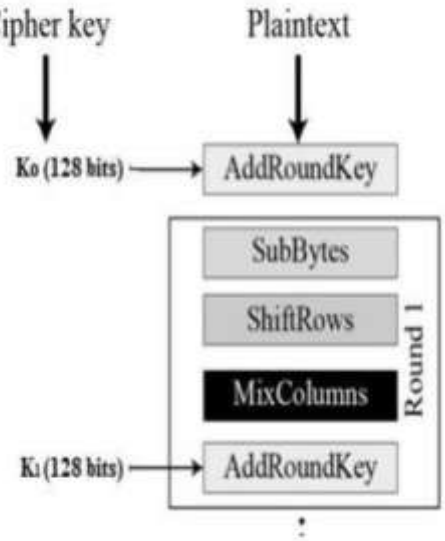

Fig-4: Encryption Process

Add round key the 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key.

If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

Each round consists of the four processes conducted in the reverse order − Add round key Mix columns Shift rows Byte substitution Since sub-processes inAES.

5.1.1 Byte Substitution SubBytes:algorithms needs to be separately implemented, The 16 input bytes are substituted by looking up a fixed

although they are very closely related. table S−box given in design[12].

- AES Analysis In present day cryptography, AES is widely adopted and supported in both hardware and software.
- Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.
- The AES algorithm operates on bytes, which makes it simpler to implement and explain[15].

5.2RING SIGNATURE:

- In cryptography, a **ring signature** is a type of digital signature that can be performed by any member of a group of users that each have keys.
- Ring and group signatures are technologies used for signing the data by an individual or some of the group members. Ring signature technology simply hides the individual who signs the data before sending. The ring signature scheme, a group is defined and everyone has their own signature in the group.
- One individual or a group of individual can sign the data for encrypting or decrypting. Security of ring signature is computationally infeasible to find out the secret keys of individuals participating in the scheme keys that are required to generate the signature.
- Ring signatures are like group signatures yet contrast in two key routes: initially, individual signatures cannot be modified and a group can be formed by any number of persons.
- Thus a signature, which is anonymous utilizing the multiple public keys is generally termed as a Ring Signature.[14]
- Ring signatures portray as an approach to release a mystery.
- It also provide the authenticity and anonymity of the end users.
- Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people[5].
- One of the security properties of a ring signature is that it computationally infeasible to determine which of the group members keys was used to produce the signature

Ring signatures are similar to group signatures but differ in two key ways:

1. First, there is no way to revoke the anonymity of an individual signature.
2. Second, any group of users can be used as a group without additional setup.

Ring signature is a promising candidate to construct an anonymous and authentic data sharing system for end user[7].

It allows a data owner to secretly authenticate his data which can be put into the **cloud** for storage.

5.2.1. Applications of Ring signature:

1. Threshold ring signature
2. Linkable ring signature

3. Traceable ring signature

6.IMPLEMENTATION:

6.1 Group Manager: Group manager takes charge of system parameters generation, adding the user and deleting the user. Group manager is leader of the group.All the other parties in group trust group manager.

6.2 Group members:Group members or group users who are registered in that group. Only registered user can store their data in cloud and share them to others[3]. Group memberships are dynamically changed , its because of the user revocation and new user joins the group.

6.3 Key Distribution: The group manager securely distributes their private key to group members without any certificate authorities. In other existing scheme the goal is achieved by assuming communication channels is secure. However, in our scheme we can achieve it without communication channel.

6.4 Access control: Group members are able to use their resources in cloud for sharing the data and storing the data. Person who are not authorized are unable to access the resources in cloud at any time or at any situation. Revoked users are unable to use the resources in cloud after they are revoked[8].

6.5 Data confidentially: It requires that the persons who is not authorized are not capable of learning the data which is stored in cloud. To maintain the availability of data confidential is still a challenging issue for dynamic groups in cloud. It is mainly for revoked users are unable to decrypt the store data file after the revocation.

7.MODULES

1. User Interface design
2. Signature generation
3. File upload and encryption
4. File access and download.

Fig-5: User Interface design

Fig-6:
Registered Users

Fig-7: Group manager login

8.CONCLUSION

In this, we design a secure anti-collusion sharing the data for dynamic groups in the cloud. User can obain their private key securely from the group manager without any secure communication channels and without any certificateauthories. It supports dynamic group efficiency. Private key of the group member need be updated or recomputed when the user joins or leaves the group. Revoked user are unable to get their original data from the cloud after their revocation. This scheme can achieve secure user revocation.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, January 2010, pp. 136-149. [2]M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apirl 2010.

[3]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5]E.Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6]G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and

Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[7]Shucheng Yu, Cong Wang, KuiRen, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8]R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", in Proc. of AISIACCS, 2010, pp. 282-292.

[9]C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with ConstantSizeCiphertexts or Decryption Keys," in Proc. of Pairing, 2007, pp.39-59.

[10]D. Chaum and E. van Heyst, "Group Signatures," in Proc. Of EUROCRYPT, 1991, pp. 257-265. [10] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Of CRYPTO, 1993, pp. 48

[11]B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "FullyCollusionSecure Dynamic Broadcast Encryption with Constant-SizeCi-phertexts or Decryption Keys," Proc.First Int'l Conf. Pairing-BasedCryptography, pp. 39-59, 2007.

[13]https://en.wikipedia.org/wiki/Advanced_Encryption_St andard.

[14] *J.Kar,"Low Cost Scalar Multiplication Algorithms for Constrained Devices", International Journal of Pure and Applied Mathematics, vol.102, no.3, pp.579-592.*

[15] *V. Goyal, O. Pandey, A. Sahai, and B. Waters, "AttributeBased Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.*

[16] *G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.*