JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE ANTI-COLLUSION DATA SHARING FRAMEWORK FOR CLOUD-BASED DYNAMIC GROUPS

Mr.K.Sundaravadivelu [1],

Assistant Professor, Department of Computer Science, Madurai Kamaraj University.

Mr.M.Sulthan Alavudeen [2],

Assistant Professor, Department of Computer Science, Parvathy's Arts and Science College.

ABSTRACT:

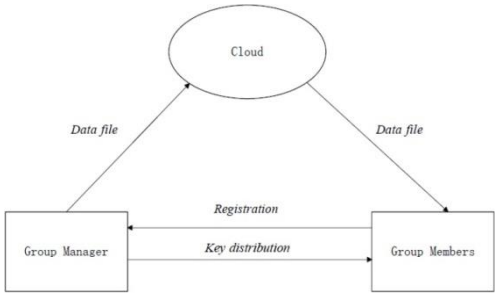
With the use of cloud computing, users can develop a growing and balanced way for data exchange between groups and individuals, with the characteristics of less management and little maintenance expense. Because the security of outsourced data is uncertain, it offers a security certification for data exchange. Due to the group's memberships often changing, privacy protection becomes a problem, especially for untrusted clouds as a result of collusion or pilot attacks. Key distribution in the current system is based on secure communication channels. Everyone is aware of the key, and using it effectively is exceedingly challenging. In this research, we propose a secure way for users to learn their private key from their group manager without the need of any communication channels. Data encryption and decryption methods use the AES algorithm, while key distribution among the group members via ring signature.

Key Words: AES Algorithm, Pilot Attack, Cloud Computing, Preserving Privacy.

INTRODUCTION:

Cloud computing has the advantages of natural information data exchange, inexpensive upkeep, and greater resource usage. This data can be shared in a secure manner, and in the cloud, secure data sharing in dynamic groups is possible. Cloud computing provides limitless storage. In our concept, collusion attacks can be prevented from compromising encrypted data sharing. The primary contributions of this scheme to this study are as follows:

1. Because the user's public key has been verified, key distribution can take place without the use of a communication channel, and users can securely learn their private key from their group managers without the need for a certificate authority.
2. This system can implement fine-grained access control, allowing any group member to access group resources while preventing revoked users from accessing cloud data once they have been rejected.
3. This can prevent collusion attacks by preventing the suspended user from accessing original data on the cloud.
4. Using a polynomial function, our technique enables secure user revocation.
5. This method can achieve high efficiency, meaning that prior users won't need to update their private keys when new members are added or excluded from the group.



EXISTING SYSTEM:

To provide fine-grained data access control without revealing the contents, existing techniques of key policy attributes rely on "lazy re-encryption, proxy re-encryption, and encryption." The secure communication channel is the foundation of this scheme's key distribution security, however it is challenging to really have such a channel in practise. It is based on encryption methods to ensure secure provenance by utilising cypher text and group signatures. After registering, each user receives two keys, and the attribute key is used to decrypt the data.

After registering, each user in the group receives two keys that are used to decrypt data when the private key is utilised.

For a safe access control system on encrypted data in cloud storage, role-based encryption techniques are employed. This method of securing the storage of huge amounts of data in the cloud may effectively revoke users by combining encryption with role-based access control regulations. A collusion attack using a private key is simple to execute and can steal important data files. There is no issue with the entity-to-entity verifications.

DISADVANTAGES OF EXISTING SYSTEM:

The file-block keys must be changed and distributed for a user revocation; as a result, the system incurred a significant key distribution cost.

With the number of data owners and revoked users, the complexity of user involvement and revocation in these schemes grows linearly.

The installation of applications that allow any group member to use the cloud service to store and share data files with others may be hampered by the single-owner method.

PROPOSED SYSTEM:

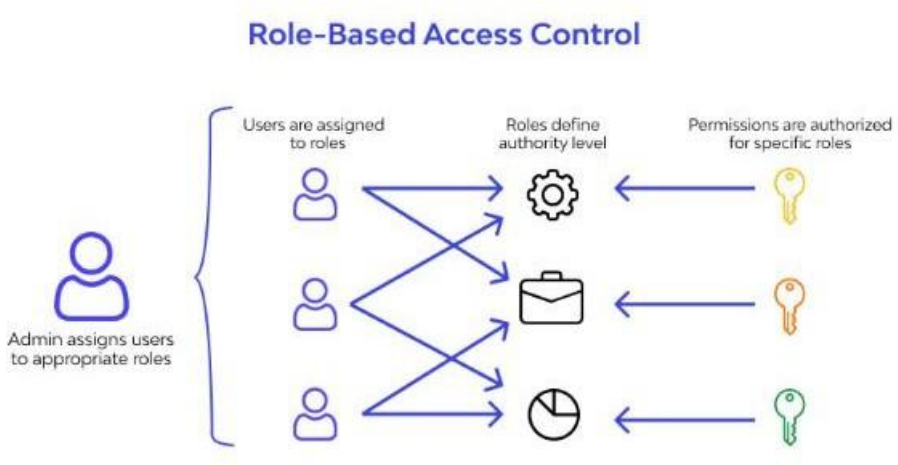
A secure data sharing plan is put forth that can safeguard key distribution while exchanging data with dynamic groups. Without the use of any communication channels, keys are distributed securely. Due to the user's public key being verified, the group manager can provide the user with their private key without the need for a certificate authority [15].

Our system uses a list of group members to achieve fine-grained access control; any group members are able to use cloud resources, and revoked users are unable to access their original data after being revoked.

ADVANTAGES:

The cost of computation has no bearing on the RBAC scheme's total number of revoked users. The process for members to decrypt the data files virtually stays the same, regardless of how many people are suspended.

The payment has no bearing on how many users have their access terminated. The reason is that the number of revoked users has no bearing on the computing cost of the cloud for file upload in our approach, which consists of two signature verifications. The fact that the RBAC system does not take into account communication entity verifications is the cause of the cloud's low compute cost during the file upload phase.

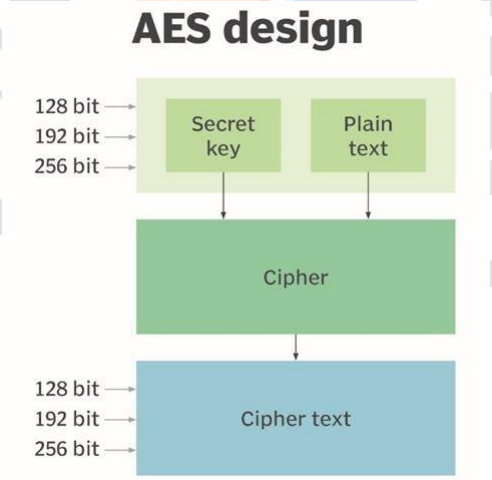


Without using a certificate authority, the user can safely receive their private key from the group manager.Make a secure data-sharing proposal that is impervious to collusion attacks.

ALGORITHM :

ADVANCED ENCRYPTION STANDARD (AES):

AES is a secret key encryption algorithm-based symmetric block cipher.There are only the bits 128, 192, and 256 supported by AES. The bit will be sent to the cypher engine, which will generate a cypher text.AES's cypher key similarly consists of a series of 128, 192, and 256 bits.The same procedure will be followed in reverse order for both encryption and decryption.10, 12, 14 rounds for keys with 128, 192, 256 bits.This key is divided into distinct sub keys for each round of the process. Key Expansion is the name of this procedure.Symmetric or secret-key cyphers require that both the sender and the receiver know and use the same secret key because they employ the same key for both encryption and decryption.



ALGORITHM WORKS ON:

It operates on a network of substitution permutations, where a number of various processes are connected. Instead of using bytes, all computations are performed here using bits. The Advanced Encryption Standard (AES) scenario divides each block of 128 bits into 16 bytes. A 4 and 4 byte matrix is used to settle each 16-bit segment. The length of the key determines the number of rounds involved.

1. **BYTE SUBSTITUTION (SUBBYTES)**

The 16 input bytes are changed in a certain way by using a fixed table. Once more, a matrix with four rows and four columns is created.

2. **SHIFTROWS**

Each of the four rows is shifted to the left, and any exceeding entries are entered on the right.

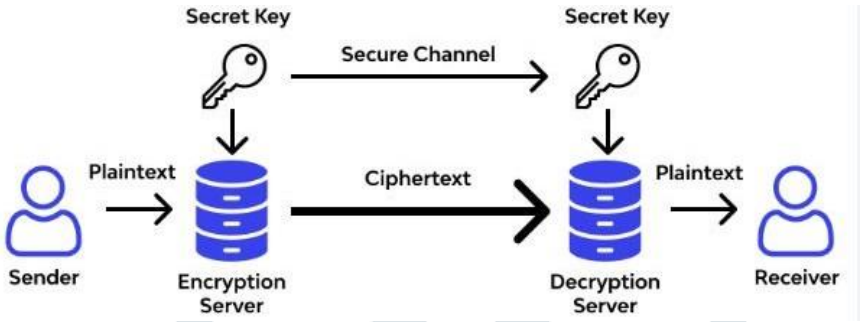
The procedure entails:

To the front row, no shift.

Move the second row one position to the left.

For the third row, two positions were moved to the left. Make a three-position move starting from the fourth row.

The same 16 bytes are used to create a new matrix, but with a number of positional alterations.

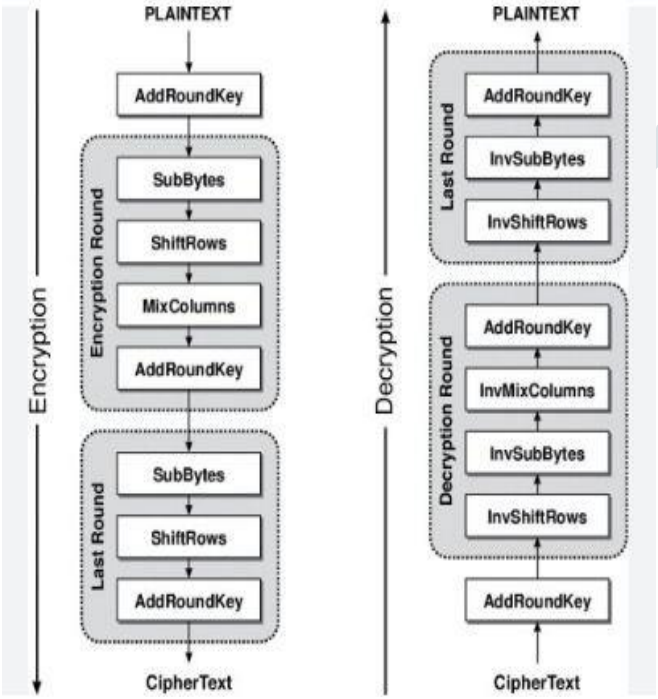


3.MIXCOLUMNS

Each of the four-byte columns is now subjected to a complex mathematical operation. In this case, the method totally transforms the four bytes into four new bytes after absorbing them from one column. As a result, a new matrix is generated with the same 16-byte and 4*4 structure.

4.ADDROUNDKEY

The 16 bytes are now divided into 128 bits and XORed to create a 128 bit round key. If this is the final encryption segment, the output creates the required ciphertext. If not, the subsequent 128 bits are translated into 16 bytes and the subsequent round begins similarly.



CONCLUSION:

In this, we propose a safe anti-collusion data sharing system for mobile groups. Users are able to safely obtain their private keys from the group manager without the need of secure communication channels or certificate authorities. It promotes flexible group effectiveness. When a person enters or quits a group, their private key needs to be updated or recalculated. After being revoked, a user is unable to retrieve their original data from the cloud. With this method, secure user revocation is possible.

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-

[3]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. [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] 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.

[5] 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.

[6] Shucheng Yu, Cong Wang, Kui Ren, 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.

[7] 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.

[8] 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.

[9] 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

[10] 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

[11] 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.

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

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