Journal of
Information Technology & Software Engineering

Rathna et al., J Inform Tech Softw Eng 2015, 5:2
DOI: 10.4172/2165-7866.1000146

Research Article Open Access

Distribute with Proficient Revocation of Data Stored in Clouds

Rathna D, Sankaragomathi R, Thulasika S and Thiruselvan P*

P.S.R.R College of Engineering for Women, Sivakasi, India

Abstract

Access control is processed on centralized form with key distributed center (KDC). Because of this data are affected if any one of the key gets attacks. To recover the data from the overall damage from attacks, providing attributes for the data in decentralized approach. Due to this attribute based access control for data in cloud storage. Secure the data storage in clouds, decentralized access control approach is introduced. Access control provides authentication for the user, in which only valid users are able to decrypt the stored information. User authentication and access control scheme are introduced in decentralized, which prevent replay attacks and supports modification on data stored in the cloud. Access control in clouds is gaining attention because it is important that only authorized users have to access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Clouds are being store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. Decentralized approach and provides authentication without disclosing the identity of the users.

Keywords: Access control; Authentication; Cloud storage; Key distributed center

Introduction

Cloud computing is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources. Cloud computing involves deploying groups of remote servers and software networked that allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. Using homomorphic encryption [1], the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result. The user is able to decode the result, but the cloud does not know what data it has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results. Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. Key distribution is done in a decentralized way [2]. One limitation is that the cloud knows the access policy for each record stored in the cloud A creator on presenting the token to one or more KDCs receives keys for encryption/decryption, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message [3-5].

Existing System

Data are accessed in centralized form on the basis of key distributed center. Key distributed center does not support for authentication. A single failure of KDC can affect the maximum number of data in cloud storage. It is most difficult to maintain the large number of data in cloud for centralized form [6-8]. Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment.

These are the limitations of the existing system:

- Approaches of data storage are only based on centralized form.
- It affects the maintenance of large number of data storage in cloud.
- It does not support the authentication control [9,10] (Figure 1).

Framework

In the decentralized access control some of the modules are used to modify the data which can be invisible.

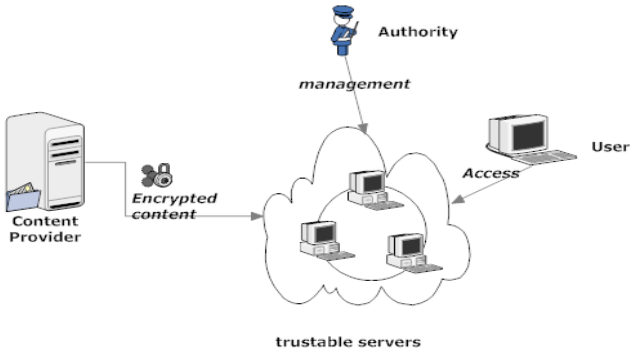

Figure 1: Existing system architecture.

***Corresponding author:** Thiruselvan P, Assistant Professor, P.S.R.R College of Engineering for Women, Sivakasi, India, Tel: 04562 239 091; E-mail: thiruramya14@gmail.com

Received April 15, 2015; **Accepted** May 05, 2015; **Published** May 25, 2015

Citation: Rathna D, Sankaragomathi R, Thulasika S, Thiruselvan P (2015) Distribute with Proficient Revocation of Data Stored in Clouds. J Inform Tech Softw Eng 5: 146. doi:10.4172/2165-7866.1000146

Client/server access control

- It provides access control based on user information.
- In this module cloud verifies the users who are authenticated.
- Anonymous users are authenticate in cloud by some encryption method.
- This original user creates and shares data with other users in the group through the cloud.
- Shared data is further divided into a number of blocks.
- The original user is the original owner of data.
- Data is divided into many small blocks, where each block is independently signed by the owner [11-15].

Access control

- Authorizations for individual users are provided for authenticated users and anonymous users.
- Authorizations are given to users on the basis on key generation.
- The user easily upload the encrypted data's to cloud the ring key for each file uploaded by the user is generated automatically.
- After that the users note their member ring key for that data access to others.
- By data outsourcing, users can be relieved from the burden of local data storage and maintenance.
- The benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data [16-19].

Anonymous executive

- It provides access policy based on users information.
- It provides security for user information based on the attribute based encryption technique.
- We only consider how to audit the integrity of shared data in the cloud with static groups keys.
- It means the group key is pre-defined before shared data is created in the cloud and the membership of users in the group key is not changed during data sharing.
- The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud.
- Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic data.
- A new user can be added into the group and an existing group member can be revoked during data sharing [20-23].

User revocation

- It secures the data from annulled user and data attackers.
- Secret keys of the minimal set of attributes which are required to decrypt the data.
- The owners should change the stored data and send updated information to other users Secure control**.**
- It secures data on the basis access policy and access control technique.
- Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks relating to personal property.
- We only consider how to audit the integrity of shared data in the cloud with static groups keys.
- It means the group key is pre-defined before shared data is created in the cloud and the membership of users in the group key is not changed during data sharing.
- The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud.
- Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic data.
- A new user can be added into the group and an existing group member can be revoked during data sharing [24,25].

Attribute-Based Encryption

A crucial security feature of attribute-based encryption is collusion-resistance. It holds multiple keys should only be able to access data if at least one individual key grants access. It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

AES Algorithm

AES (acronym of advanced encryption standard) is a symmetric encryption algorithm. To encrypt and decrypt text using *AES* encryption algorithm AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant By contrast; the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field [26].

Proposed System and Future Work

Maintaining the large number of data in cloud, decentralized access control approaches is proposed. Involving distribution of secret keys and attributed of all users. Authentication access control only allows the user for reading purpose. Accessing the data by user only satisfying the access policy and authentication. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Revoked users cannot access data after they have been revoked [27-29]. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are

mostly done by the cloud. Efficient search on encrypted data is also an important distress in clouds. Access control is also gaining importance for users. Users can have either read or write or both accesses to a file stored in the cloud. The access policy decides who can access the data stored in the cloud.

Conclusion

A decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials [30]. Key distribution is done in a decentralized way. Data stored in clouds is highly sensitive. We should prevent the data corruption Here we propose a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. Cloud doesn't know about used details, it only verifies the user information. Cloud knows only the access policy of the stored information.

References

1. Ruj S, Stojmenovic M, Nayak A (2012) Privacy Preserving Access Control with Authentication for Securing Data in Clouds. Cluster, Cloud and Grid Computing. IEEE, pp. 556-563.
2. Wang C, Wang Q, Ren K, Cao N, Lou W (2012) Toward Secure and Dependable Storage Services in Cloud Computing. Services Computing 5: 220-232.
3. Li J, Wang Q, Wang C, Cao N, Ren K, et al. (2010) Fuzzy Keyword Search Over Encrypted Data in Cloud Computing. IEEE, pp. 441-445.
4. Kamara S, Lauter K (2010) Cryptographic Cloud Storage Proc.14th Int'l Conf. Financial Cryptography and Data Security. Lecture Notes in Computer Science 6054: 136-149.
5. Li H, Dai Y, Tian L, Yang H (2009) Identity-Based Authentication for Cloud Computing, Proc. First Int'l Conf. Cloud Computing. Lecture Notes in Computer Science 5931: 157-166.
6. Gentry C (2009) A Fully Homomorphic Encryption Scheme. PhD dissertation, Stanford University.
7. Sadeghi A R, Schneider T, Winandy M (2010) Token-Based Cloud Computing Proc. Third Int'l Conf. Trust and Trustworthy Computing. Lecture Notes in Computer Science 6101: 417-429.
8. Ko R K L, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, et al. (2013) Trust cloud: A Framework for Accountability and Trust in Cloud Computing. Services (SERVICES), 2011 IEEE World Congress on. IEEE, pp. 584-588.
9. Lu R, Lin X, Liang X, Shen X (2010) Secure Provenance: The essential of Bread and Butter of Data Forensics in Cloud Computing. Fifth ACM Symp. Information Computer and Comm. Security (ASIACCS), pp. 282-292.
10. Ferraiolo DF, Kuhn D R (1992) Role-Based Access Controls. Proc.15th Nat'l Computer Security Conf, pp. 554-563.
11. Kuhn D R, Coyne E J, Weil T R (2010) Adding Attributes to Role-Based Access Control. IEEE Computer 43 79-81.
12. Li M, Yu S, Ren K, Lou W (2010) Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings. Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (Secure Comm) 50: 39-106.
13. Yu S, Wang C, Ren K, Lou W (2010) Attribute Based Data Sharing with Attribute Revocation. Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270.
14. Wang G, Liu Q, Wu J (2010) Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services. Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737.
15. Zhao F, Nishide T, Sakurai K (2011) Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems. Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC) 83-97.
16. Ruj S, Nayak A, Stojmenovic I (2011) DACC: Distributed Access Control in Clouds. Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (Trust Com), pp. 91-98.
17. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf, 2013.
18. http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud,2013.
19. Jahid S, Mittal P, Borisov N (2011) EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation. Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 411-415.
20. Rivest R L, Shamir A, Tauman Y (2001) How to Leak a Secret. Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565.
21. Boyen X (2007) Mesh Signatures. Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT) 210-227.
22. Chaum D, Heyst E V (1991) Group Signatures Proc. Ann. Int'lConf. Advances in Cryptology (EUROCRYPT), pp. 257-265.
23. Maji H K, Prabhakaran M, Rosulek M (2008) Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance IACR Cryptology ePrint Archive.
24. Maji H K, Prabhakaran M, Rosulek M (2011) Attribute-Based Signatures Topics in Cryptology - CT-RSA, vol. 6558, 376-392.
25. Beimel A (1996) Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Technion, Haifa.
26. Sahai A, Waters B (2005) Fuzzy Identity-Based Encryption. Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473.
27. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Proc. ACM Conf. Computer and Comm. Security, pp. 89-98.
28. Bethencourt J, Sahai A, Waters B (2007) Ciphertext-Policy Attribute-Based Encryption. Proc. IEEE Symp. Security and Privacy, pp.21-334.
29. Liang X, Cao Z, Lin H, Xing D (2009) Provably Secure and efficient Bounded Cipher text Policy Attribute Based Encryption. Proc. ACM Symp. Information, Computer and Comm. (ASIACCS), pp. 343-352.
30. Chase M (2007) Multi-Authority Attribute Based Encryption. Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534.