Research Paper

Engineering

Authentication and Privacy Protection of Data Stored in Clouds Using Attribute Based Access Control

Antony Kumar M Antony Kumar M, P.M.R Engineering College, Chennai.

Praveen Kumar S Praveen Kumar S, Paavai College of Engineering, Namakkal

ABSTRACT *We propose a new decentralized access control scheme for secure data storage in clouds, that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information.*

The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

KEYWORDS : Access policy, Decentralized access control with anonymous authentication, data storage on clouds, key distribution centers (KDCs)

INTRODUCTION

RESEARCH in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing.

In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

Recently, Wang et al. addressed secure and dependable cloud storage. Cloud servers prone to Byzantine failure, where a storage server can fail in arbitrary ways . The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify datafiles as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption .The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords.

Security and privacy protection in clouds are being explored by many researchers. Wang et al. addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied in .Many homomorphic encryption techniques have been suggested to ensure that the cloud is not able to read the data while performing computations on them. Using homomorphic encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext 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.

To this end, we propose Dekey, a new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers. Security analysis demonstrates that Dekey is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement Dekey using the Ramp secret sharing scheme and demonstrate that Dekey incurs limited overhead in realistic environments. Convergent encryption provides a viable option to enforce data confidentiality while realizing deduplication.It encrypts/decrypts a data copy itself.After Key generation and data copy with a convergent key,which is derived by computing the cryptographic hash value of the content of the data copy itself.After key generation and data encryption,users retain the keys and send the cipertext to the clouds.

OBJECTIVES

The main contributions of this paper are the following:

1. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
2. Authentication of users who store and modify their data on the cloud.
3. The identity of the user is protected from the cloud during authentication.
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. 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.
6. Revoked users cannot access data after they have been revoked.
7. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
8. The protocol supports multiple read and write on the data stored in the cloud.
9. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

EXISTING SYSTEM

Existing work on access control in cloud are centralized in nature. Except and , all other schemes use attribute based encryption (ABE). The scheme in uses a symmetric key approach and does not support authentication. The schemes do not support authentication as well. Earlier work by Zhao et al. provides privacy preserving authenticated access control in cloud.

However,the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. 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. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attributes to users. It is also quite natural for clouds to have many KDCs in different locations in the world.

- The cloud is also prone to data modification and server colluding attacks.
- To provide secure data storage, the data needs to be encrypted.
- This is achieved by means of searchable encryption.

Advantages:

1. The clouds should not know the query but should be able to return the records that satisfy the query.
2. The keywords are sent to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search.
3. The problem here is that the data records should have keywords associated with them to enable the search.

DISADVANTAGES

1. A single KDC is not only a single point of failure but difficult to maintain because of the number of users that are supported in a cloud environment
2. Accountability of clouds is a very challenging task and involves technical issues and law enforcement.
3. The correct record are returned only when searched with the exact keywords.
4. Neither clouds nor users should deny any operations performed or requested

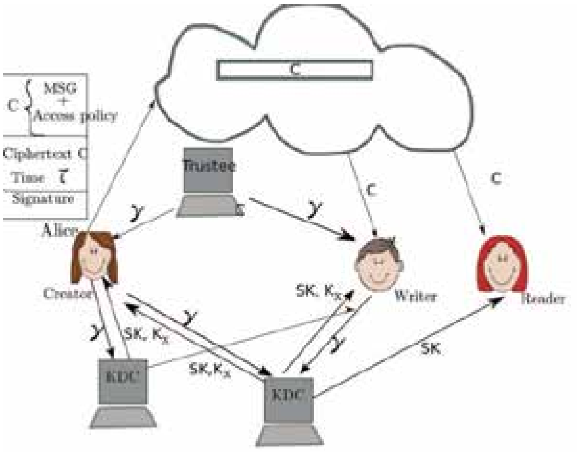
PROPOSED SYSTEM

Proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, Rujet al. proposed a distributed access control mechanism in clouds. However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the preliminary version of this paper, we extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud. In this version we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy.

ADVANTAGES

1. We extend our previous work with added features which enables to authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud.
2. Decentralised access control of data stored in clouds so that only authorized users with valid attributes can access them.
3. The identity of the user is protected from the cloud during authentication.
4. Athenticationof users who store and modify their data on the cloud.
5. 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.
6. Revoked users cannot access data after they have been revoked.
7. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.

ARCHITECTURE



CONCLUSION

We have presented 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. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

A decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks, is achieved. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way and also hide the attributes and access policy of a user. One limitation is that the cloud knows the access policy for each record stored in the cloud.

REFERENCES

[1] 1. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for | [2] Securing Data in Clouds," Proc. IEEE/ ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, | [3] 2012. | [4] 2. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in | [5] Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012. | [6] 3. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in | [7] Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010. | [8] 4. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography | [9] and Data Security, pp. 136- 149, 2010. | [10] 5. H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l | [11] Conf. Cloud Computing (CloudCom), pp. 157-166, 2009. | [12] 6. C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., | [13] http://www.crypto.stanford.edu/ craig, 2009. | [14] 7. A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. | [15] Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010. | [16] 8. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: | [17] A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, | [18] http:// www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013. | [19] 9. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data | [20] Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security | (ASIACCS), pp. 282-292, 2010 |