ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (557-561), Month: April - June 2015, Available at: www.researchpublish.com

Framework for Secure Anonymous Authentication Using DAC in Cloud

Harshitha H S

Visvesvaraya Technological University, Belagavi, P.E.S. College of Engineering, Mandya, India

Abstract: **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 series without knowing the user's identity before storing data. This 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. It also addresses user revocation. Moreover, the 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 control, authentication signatures, encryption.**

I. INTRODUCTION

Cloud computing is a developed technology used to for data storage, which is to store data from different users and online access to computer services or resources. Since cloud storage is more flexible, it is receiving lot of attention in the industrial world.

Clouds can provide several types of services like infrastructures, applications, and several platforms to help developers write applications. Cloud is a platform for data storage and much of the data stored in clouds is highly sensitive for example, social networks and medical records. Thus it is a complex system which requires highly securable processes. So it must need a proper systematic scheme to manage data.

Providing security only is very simple but providing security with privacy is very much difficult. It is very easy for intruders to access the confidential data. So maintaining the privacy is very much important. Since very confidential data's are stored in cloud it is very much needed to maintain the security and privacy. So this area must be concentrated.

The user should be verified and should give appropriate permission for them. Permission criteria are carefully handled because users may change the data unnecessarily. So this area should also be concentrated.

Hence, how the security and privacy are available for the outsourced data becomes a serious concern. 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.

There may be many issues like preserving authorized restrictions on information access and disclosure, main threat accomplished when storing the data with the cloud, guarding against improper information modification or destruction, ensuring timely and reliable access to and use of information. It is important to control the access of data so that only authorized users can access the data.

Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. The problems of access control, authentication, and privacy protection should be solved simultaneously.

II. LITERATURE SURVEY

A literature review is a body of text that aims to review the critical points of current knowledge and/or methodological approaches on a particular topic. For complete study of the system it is necessary to go through each and every technical aspect of the related material in depth. Presented below is the survey of associated technologies and summary of related work done in the past.

User Privacy in Cloud Computing:

User privacy is also required in cloud. By using privacy the cloud or other users do not know the identity of the other user. The cloud can hold the user accounts for the data in cloud, and likewise, to provide services the cloud itself is accountable. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy.

Encryption in Cloud Computing:

The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Search on Encrypted Cloud Data:

Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Security and privacy protection on cloud data:

Users Authentication scheme using public key cryptographic techniques in cloud computing. Many homomorphic encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data. By using this encryption scheme, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the user to verify that the cloud returns correct results.

Accountability in cloud:

Neither the clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed; ABE was proposed by Sahai and Waters. In ABE, a user has a set of attributes in addition to its unique ID.

There are two classes of ABEs.

➢ Key-policy ABE (KP-ABE)

○ Sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes.

➢ Cipher text-policy (CP-ABE)

○ Receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

➢ Chase proposed a multiauthority ABE, in which there are several KDC authorities which distribute attributes and secret keys users. Multiauthority ABE protocol was studied, which required no trusted authority which requires several users to have attributes from at all the KDCs.

➢ Lewko and Waters proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive.

- Green et al. proposed to outsource the decryption task to a proxy server, so that the user can compete with minimum resources. However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously.

- Yang et al. presented a modification; authenticate users, who want to remain anonymous while accessing the cloud.

- To ensure anonymous user authentication ABSs were introduced by Maji et al. This was also a centralized approach. A recent scheme by Maji et al. takes a decentralized approach and provides authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attack.

III. EXISTING SYSTEM

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 data files 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.

Privacy preserving search:

- 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.

Drawbacks:

- The correct records are returned only when searched with the exact keywords.

Storage security:

- Reed-Solomon erasure-correcting codes were used.
- 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.

Disadvantages:

- 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.

IV. PROPOSED SYSTEM

- To propose ABS scheme to achieve authenticity and privacy.
- This is resistant to replay attacks, in which a user can replace fresh data with stale data from a previous write, even if it no longer has valid claim policy.
- This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud.
- This scheme also allows writing multiple times which was not permitted in earlier work.

Advantages:

- 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.
- 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.

V. SYSTEM ARCHITECTURE

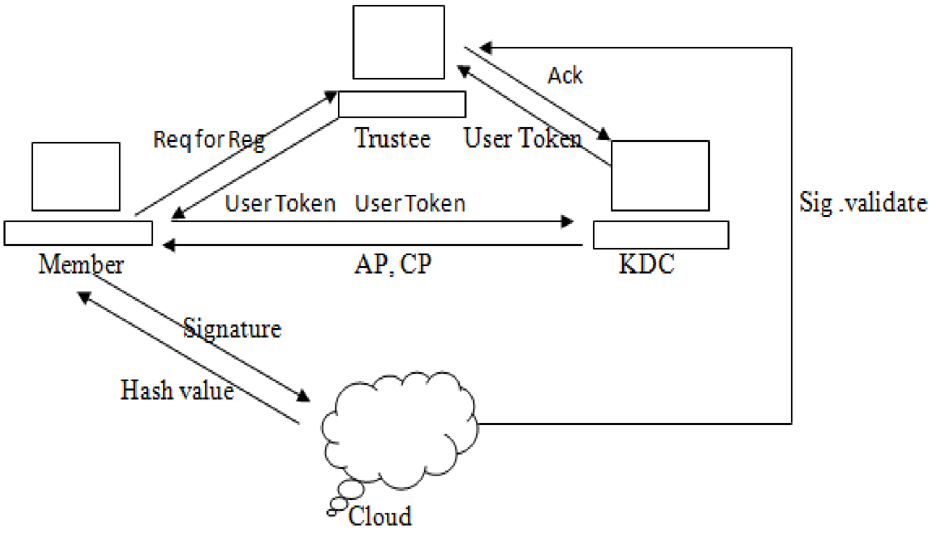

Fig. 1: System Architecture for Anonymous Authentication using DAC in Cloud

The member requests the trustee for his registration. So the trustee will give him the user token. After getting token , the member sends his token for KDC. KDC in turn will send that token to the trustee and get verification. KDC will send the access policy and claim policy to the member. After that member will encrypt the data using the access policy and also generate the signature using claim policy. In the next stage member will send his generated signature to the cloud. Cloud will communicate with the trustee for the signature verification and gets confirm the authorization. After the cloud gets the authorization of the member the cloud allows the data owner to upload the data and stores that data

VI. CONCLUSION

This project explains about decentralized access control technique with anonymous authentication, which hides the user identity, who stores the information and also the one who retrieves the information. The cloud also does not know the identity of the user who stores information, but only verifies the user’s credentials. And also people who have privilege for accessing of data, only those can retrieve the data from the cloud. Thus the data uploaded will be secure. Key distribution is done in a decentralized way. Hence the problem of access control, authentication and privacy protection is overcome.

REFERENCES

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[3] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, http://www. crypto. stanford.edu/craig.

[5] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[6] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[7] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[10] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, 2008.

[11] Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD Thesis. Technion, Haifa, 1996.

[12] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 6632. Springer, pp. 568–588, 2011.

[13] J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, 2011.