A LITERATURE SURVEY ON DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA STORED IN CLOUDS USING KDC

V.R.Mani Megalai, R.Mekala M.E.(Ph.D.)
[1]*PG Student, INFO Institute of Engineering, Coimbatore*
[2]*Assistant Professor, INFO Institute of Engineering, Coimbatore*

Abstract:

This survey proposes a new decentralized access control scheme for secure data storage in clouds which supports anonymous authentication. The cloud verifies the authenticity of the series without significant knowledge in the user's identity before storing information. This scheme also has the added feature of access control. In access control scheme only valid users are able to decrypt the stored data/information. This scheme prevents replay attacks also supports creation, modification, and reading information stored in the cloud. These schemes also address user revocation. Moreover, the authentication and access control scheme is decentralized and robust in nature unlike other access control schemes designed for clouds which are centralized. The computation, communication, and storage overheads are comparable to centralized approaches.

I.INTRODUCTION

Cloud Computing

In cloud computing, users can contract out their computation and storage to servers (also called clouds) using Internet. This frees users from the hardness of maintaining resources on-site. Several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms (e.g., Amazon's S3, Windows Azure) can be provided by cloud to help developers.

A lot of the information stored in clouds is very much sensitive. For example, medical records and social networks are very sensitive. In cloud computing the very big issues are Security and privacy. At first step the user should authenticate itself before initiating any transaction, and on the second step, it must be ensured that the cloud does not alter with the data that is outsourced.

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.

ISSN: 2278 – 909X

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;

II.EXISTING SYSTEM

[1]In 2006 A. Sahai and B. Waters, worked on "Fuzzy Identity-Based Encryption" **In Identity Based Encryption scheme,** A user has a set of attributes in addition to its unique ID. A Fuzzy IBE scheme can be applied to enable encryption .In Fuzzy scheme biometric input used as identity.

Advantages:-

- error-tolerant
- Secure against collusion attacks.

[2] In 2006 V. Goyal, O. Pandey, A. Sahai, and B. Waters, worked on "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ".This paper, the sender has an authorization to encrypt information. A revoked attributes and keys of users cannot write again to stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes.

Advantages:-

- Distribution of audit-log information and screen out encryption.

ISSN: 2278 – 909X

[3] In 2007 J. Bethencourt, A. Sahai, and B. Waters, worked on "Cipher text-Policy Attribute-Based Encryption". By using this approach the receiver has the access policy in the form of a tree. The tree contain attributes as leaves and monotonic access structure with AND, OR and other threshold gates

Advantages:-

- Encrypted information can be kept confidential even if the storage server is untrusted;
- Secure against collusion attacks.

[4]In 2007 M. Chase, worked "Multi-Authority Attribute Based Encryption". This scheme describes several Key Distribution Authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multiauthority Attribute Based Encryption protocol which requires no trusted authority which requires every user to have attributes from at all the KDCs.

Advantages:-

- Allows a more number of attributes.

[5] In 2011 A.B. Lewko and B. Waters, worked on "Decentralizing Attribute-Based Encryption," This paper where users could have zero or more attributes from each authority and did not require a trusted server.

Advantages

- Collusion resistant.

[6] In 2011 M. Green, S. Hohenberger, and B. Waters, worked on "Outsourcing the Decryption of ABE Ciphertexts," .This paper subcontract the decryption task to a proxy Server, so that the user made computation on minimum resources like hand held devices.

Advantages:-

- The user significantly saves bandwidth, without raising the number of transmission.

[7] In 2008 H.K. Maji, M. Prabhakaran, and M. Rosulek, worked on"Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance,".In this paper to ensure anonymous user authentication ABSs were introduced. This was also a centralized approach.

Advantages

- The user significantly saves decryption time, without raising the number of transmissions

[8] In 2011 H.K. Maji, M. Prabhakaran, and M. Rosulek, worked on "Attribute-Based Signatures," This method takes a decentralized approach and provides authentication without
disclosing the identity of the users.

Advantages:-

- secure against a malicious attribute authority

ISSN: 2278 – 909X

A.PROBLEM STATEMENT

- [1][2][3], All these approaches take a centralized approach and allow only one KDC. The KDC is a single point of failure.
- [4][5], In all these cases, decryption at user's end is computation intensive. So, these technique might be ineffective when users access using their mobile/handheld devices.
- [6] In this scheme the presence of one proxy and one KDC makes it less forceful than decentralized approaches. Together these approaches had no way to validate users, anonymously.
- [7][8] This scheme prone to replay attack.

III.PROPOSED SYSTEM

[9]Data stored in cloud follows Distributed access control scheme so that only authorized users with valid attributes can access the data. Authentication of users performs store and modification of the data in the cloud. During authentication the identity of the user is protected from the cloud. The cloud architecture is decentralized, which means that there can be several KDCs for key management. The both access control and authentication schemes are collusion resistant. The collusion resistant attack means that no two users can collude and access data or authenticate themselves, even though they are individually not authorized. Revoked users cannot access data after he/she have been revoked. The proposed scheme is flexible to replay attacks. This proposed protocol also supports multiple read and writes on the data stored in the cloud. The costs of decentralized approach should be less comparable to the existing centralized approaches.

SYSTEM ARCHITECTURE

The architecture of proposed system depicted in Fig.1.There are three users, a creator, a reader, and writer. Creator Alice receives a token _ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token _. There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, 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.

ISSN: 2278 – 909X

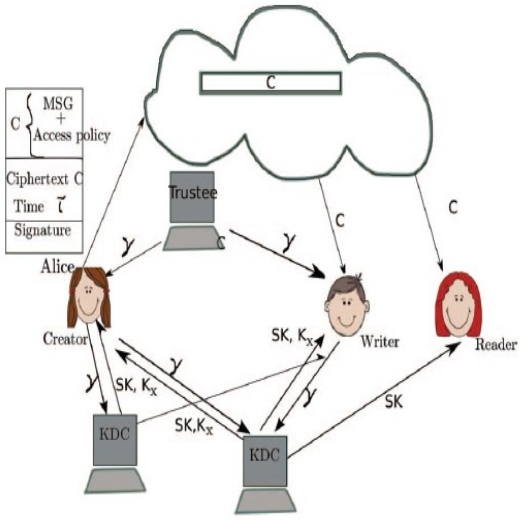

Fig. 1. secure cloud storage model.

Advantages

- Our access control scheme is secure which means no outsider or cloud can decrypt cipher texts.
- Collusion resistant
- Authorized users only can access.
- Resistant to replay attacks
- Protects privacy of the user.
- The cloud is honest-but-curious, such that the cloud administrators can be able to view user's content, but cannot modify data/information.
- Honest-but-curious model of adversary do not tamper with data so that they can keep the system functioning normally and remain undetected.
- Users have rights like either read or write or both accesses to a file stored in the cloud.
- The communications between users/clouds are secured by secure shell protocol, SSH.

Table 1:-Comparative Study on Existing vs. Proposed System

SNO	TECHNIQUE	EXISTING	PROPOSED
1	**Approach**	Centralized	Decentralized
2	**Key Encryption**	Use ABE(Attribute Based Encryption) For secret key	Use KDC(Key Distribution Center) for Key Encryption
3	**Authentication**	Does Not Provide Authentication	authenticate the validity of the message without revealing the identity of the user who has stored information in the cloud.
4	**Type Of Key**	symmetric key approach	Public key Approach
	Attack Model	Resistant to replay attacks,	Resistant to collusion attacks,

ISSN: 2278 – 909X

IV.CONCLUSION

This survey presented a decentralized access control technique with anonymous authentication. This decentralized scheme provides user revocation and prevents replay attacks. Even though the cloud does not know the identity of the user who stores information, but it verifies the user's credentials. This paper made key distribution is done in a decentralized way.

V.REFERENCES

[1]A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[4] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007..

[5] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

[6] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.

[7] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[8] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[9]Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, And Amiya Nayak," Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014

ISSN: 2278 – 909X