International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Anonymous Authentication Using Cloud Based Decentralized Access Control Scheme

K.SHIRISHA A.SWETHA

*M.TECH student , Dept of CSE, VAAGDEVI COLLEGE OF ENGINEERING

**Assistant Professor, Dept of CSE , VAAGDEVI COLLEGE OF ENGINEERING

Abstract: Cloud computing is location that allows users to store the data. Cloud computing is logically developed technology to store data from more than one user. In decentralized access control data is stored securely in cloud and here only valid users are able to decrypt the data stored in cloud and this is added feature of this scheme. This scheme supports anonymous authentication. It also supports construction, variation and reading data stored in cloud and also deals with user revocation. This access control scheme is decentralized and robust which is different from other access control scheme and costs are equivalent to centralized approaches.

Keyword: *decentralized access, access control, attribute based encryption, attribute based signature , cloud storage.*

I. INTRODUCTION

The investigation in cloud computing has received a lot of interest from educational and business worlds.In cloud computing users can contract out their calculation and storage to clouds using Internet. This frees users from problem of maintaining resources on-site. The services like applications, infrastructure and platforms are provided by cloud and helps developers to write application. The data is encrypted for the sake of secure data storage. The data stored in cloud is frequently modified so this feature is to be considered while designing the proficient secure storage techniques. The important concern is that encrypted data is to be properly searched. The cloud researchers have made up security and privacy protection in cloud. In Online social networking access control is very important and only valid user must be allowed to access and store personal information, images and videos and all this data is stored in cloud. The goal is not just store the data securely in cloud it is also important to make secure that anonymity of user is ensured. The situation like user wants to comment on object but does not want to be known. But the user wants the other user to know that he is a valid user. In this paper two protocols Attribute Based Encryption(ABE) and Attribute Based Signature(ABS) are used. ABE and ABS are combined to offer legitimate access control without revealing the identity of the user.

The important offerings of this paper is distributed access control that is only approved users with valid attributes can have entree to data in cloud. The user who stores and modify the data is verified. There are many KDCs for key management because of this the architecture is decentralized. No two users can join together and verify themselves to access data if they are not authenticated.

There is no access of data for users who have been revoked.The process of invalidation or withdrawal of control by authority that is removal of license ,name or position is revocation. The system is flexible to replay attacks. There is support for multiple read and write operations on data in cloud. The costs are analogous to centralized approaches and cloud performs the costly operations.

Problem statement: To provide safe and fast access to cloud for an authorized user without revealing his identity but the user wants the other user to know that he is a valid user. The problems of access control, authentication, and privacy protection are solved.

II. OBJECTIVES AND MOTIVATION

There are three objectives Privacy, Reliability, Accessibility. In Fuzzy Identity Based Encryption, Attribute-Based Encryption For Fine Grained Access Control of Encrypted Data, CP Attribute Based Encryption are all centralized and they have single KDC which is single point of Failure. In Multi-Authority Based Encryption, Decentralizing Attribute Based Encryption system it is very difficult for decryption at user side and users accessing via mobile or handheld devices this may become unsuccessful. In Outsourcing the Decryption of ABE Ciphertexts system there is only one KDC and it does not legalize users secretly, so because of this there is other technique Anonymous Authentication of decentralized access control that will authenticate user anonymously and authenticated access.

III. RELATED WORK

There are two types of ABE. In Key-Policy ABE access policy to encrypt data is given to sender. The attributes and secret keys are given to the receiver by attribute authority and decryption takes place if there are matching attributes. The system consists of three users creator or data owner, writer and reader. Creator will create a file and upload it to cloud. Here creator will receive a token from trustee and trustee is federal government which manages social insurance numbers. The creator will send the id to the trustee then receives token Ɣ from trustee. Here τ is time stamp is used to prevent write old information to cloud when the user is revoked. The creator will then send the token to Key Distribution Centre and there are several KDC in different regions of world.

The creator will then receive Encryption and Decryption keys and signing keys. Here SK are In Cipher text-Policy access policy and attributes are in tree form where leaves are attributes and sequence access structure with AND ,OR and other entrance gates are given to receiver. These approaches have only single KDC which is a single point of failure and less robust than decentralized approaches where there are many KDCs for key management.

IV. SYSTEM ARCHITECTURE

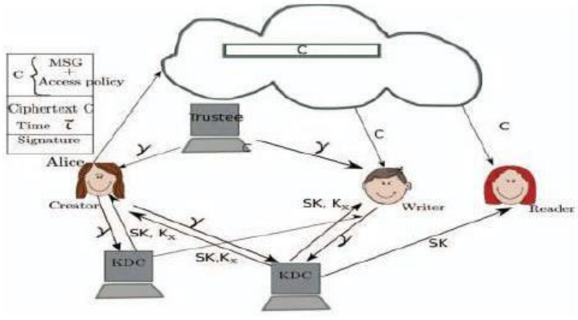

Figure 1: System Architecture

Figure 1: System Architecture

secret keys and Kx are signing keys. The Message is encrypted using access policy X and it decides who have the right to use the data stored in the cloud The Claim Policy ɣ is used to confirm authenticity and message is signed under this claim. Along with the signature c and Ciphertext C is sent to cloud. The signature is verified by cloud and stores the Ciphertext. The Ciphertext C is sent to the reader when reader wants to read the data in cloud. If the user has access policy with matching attributes then the reader can decrypt and read the message. The write operation takes place as file making. The user sends the message with claim policy and it is verified by cloud if the user is authenticated then that user is permitted to write to a existing file.

V. SYSTEM MODULES

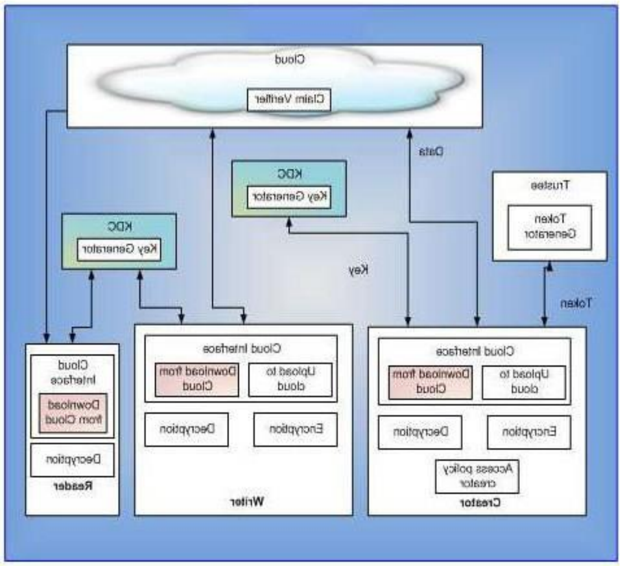

Figure 2: System Modules

Cloud Server Module

The cloud server will store the file created and uploaded by creator. The cloud allows the user to read or write access to file stored in cloud. The user must send the message and claim policy and it is verified by cloud if the user is authenticated then write to existing file is allowed. There is a secure communication between users and cloud.

User Module

Creator,Reader,Writer are different users here. Creator will create a file and upload it to cloud. The creator will encrypt the data with access policy and to prove the authenticity creator uses claim policy ɣ and signs the message using this claim policy. The signature c and ciphertext C is sent to the cloud. Attribute Based Encryption is used for Encryption and decryption of data in cloud .Writer will write to existing file in the cloud. Reader will download the file decrypt it using keys to get original message.

Trustee Module

Trustee is system or server that will verify that content creator is a valid user. This system receives id from creator and creates token and sends it to creator.

KDC Module

There are multiple KDCs and they are located in different regions and it generates encryption and decryption keys and keys for signing. Creator on presenting token to KDC it will provide secret keys and keys for signing. The cloud takes decentralized approach in distributing secret keys and attributes to user.

VI. CONCLUSION

The proposed scheme provides a Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud. It prevents replay attacks and addresses user revocation. The user credentials are verified by cloud who store the data but cloud does not know who the user is. There are multiple KDCs for key management. The access policy for each record is stored in cloud and future work may conceal the feature or characteristics and access policy of user.

REFERENCES

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

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

[3] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.

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

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

[6] 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.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[8] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[10] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud

Computing, ”IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012..

[11] Decentralized Access Control With Anonymous Authentication of Data Stored in Cloud.Authors:Sushmita Ruj,Milos StojMenovics and Amiya Nayak. IEEE Transactions on Parallel and Distributed Systems, VOL. 25, NO. 2, February 2014.

AUTHOR 1 :-

* K.Shirisha completed her B tech in Jayamukhi Institute of Technological & Science and pursuing M-Tech in Vaagdevi College of Engineering

AUTHOR 2:-

**A.Swetha is working as Assistant Professor in Dept of CSE , Vaagdevi College of Engineering