ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

Decentralized Anonymous Authentication of Data Stored in Clouds

Praveen.N, Krishna Kumar.P.R, Vinitha V Yadav

Abstract: ***Distributed computing is area that permits clients to store the information. Distributed computing is consistently created innovation to store information from more than one client. In decentralized access control information is put away safely in cloud and here just substantial clients can unscramble the information put away in cloud and this is included component of this plan. This plan bolsters mysterious confirmation. It likewise bolsters development, variety and perusing information put away in cloud furthermore manages client renouncement. This entrance control plan is decentralized and hearty which is not quite the same as different access control plan and expenses are proportional to incorporated methodologies.***

Index Terms**— decentralized access, access control, attribute based encryption, attribute based signature, cloud storage.**

I. INTRODUCTION

The examination in distributed computing has gotten a considerable measure of enthusiasm from instructive and business worlds. In distributed computing clients can contract out their figuring and capacity to mists utilizing Internet. This liberates clients from issue of keeping up assets on location. The administrations like applications, framework and stages are given by cloud and helps engineers to compose application. The information is encoded for secure information stockpiling. The information put away in cloud is every now and again altered so this component is to be considered while outlining the capable secure stockpiling strategies. The essential concern is that encoded information is to be appropriately sought. The cloud specialists have made-up security and protection assurance in cloud. In Online long range interpersonal communication access control is vital and just substantial client must be permitted to get to and store individual data, pictures and recordings and this information is put away in cloud. The objective is not simply store the information safely in cloud it is likewise vital to make secure that namelessness of client is guaranteed. The circumstance like client needs to remark on article however does not have any desire to be known. However, the client needs the other client to realize that he is a substantial client. In this paper two conventions Attribute Based Encryption (ABE)[1] and Attribute Based Signature (ABS) are utilized. ABE and ABS are joined to offer true blue access control without uncovering the personality of the client.

The critical offerings of this paper is dispersed access control that is just affirmed clients with legitimate ascribes can have dish to information in cloud. The client who stores and change the information is checked. There are numerous KDCs for key administration in light of this the design is decentralized. No two client can join together and confirm themselves to get to information in the event that they are not validated. There is no entrance of information for clients who have been renounced. The procedure of negation or withdrawal of control by power that is evacuation of permit, name or position is renouncement. The framework is adaptable to replay assaults. There is backing for different read and compose operations on information in cloud. The expenses are closely resembling concentrated methodologies and cloud performs the immoderate operations. Issue explanation: To give protected and quick access to cloud for an approved client without uncovering his character however the client needs the other client to realize that he is a legitimate client. The issues of access control, verification, and security insurance are tackled.

II. OBJECTIVE AND MOTIVATION

A. Motivation

Existing methods works on access control in cloud are centralized in nature. Except some all other schemes use ABE. The schemes use a symmetric key approach and does not support authentication. The most previous schemes do not support authentication as well. Much of the previous work takes 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

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Therefore, the expert 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.

B. Objective

1. Distributed access control of data [3] [5][7] stored in cloud so 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 [8].
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. Revoked users cannot access data after they have been revoked.
6. The proposed scheme is resilient to replay attacks.
7. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

III. RELATED WORK

There are two sorts of ABE. In Key-Policy ABE [4][6] access way to deal with scramble data is given to sender. The attributes and secret keys are given to the beneficiary by quality power and unscrambling happens if there are organizing properties. In Ciphertext-Policy access arrangement and properties are in tree structure where leaves are qualities and grouping access structure with AND, OR and other passageway entryways are given to beneficiary. These methodologies have just single KDC which is a solitary purpose of disappointment and less strong than decentralized methodologies where there are numerous KDCs for key administration.

To find the more security of the cloud and more real time oriented task also, we can handles based on the internet clouds like drop box etc. To make double authentication based on image layers and limited of cloud service provider (CSP).Centralized service provider based on the EM2 Web service on the live. To share any important data from the one server into another server based on the KDC Symmetrically methods. But, existing system they have so many other cloud service also. Proposed system we are going to use different ways of cipertext techniques based on the RTOS CLOUDS.

IV. SYSTEM ARCHITECTURE

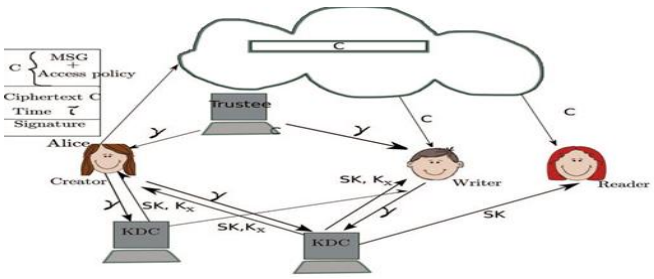

Fig 1: System Architecture

The framework comprises of three clients maker or information proprietor, author and peruse as shown in Fig1 Maker will make a document and transfer it to cloud. Here maker will get a token from trustee and trustee is central government which oversees social protection numbers. The maker will send the id to the trustee then gets token ɣ from trustee. Here τ is time stamp is utilized to forestall compose old data to cloud when the client is denied. The maker will then send the token to Key Distribution Center and there are a few KDC in various areas of world. The maker will then get Encryption [2] and Decryption keys and marking keys.

Here SK are secret keys and Kx are marking keys. The Message is encoded utilizing access arrangement X and it chooses who have the privilege to utilize the information put away in the cloud The Claim Policy ɣ is utilized to affirm legitimacy and message is marked under this case [9]. Alongside the mark c and Cipher text C is sent to

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

cloud. The mark is checked by cloud and stores the Ciphertext. The Ciphertext C is sent to the peruse when peruse needs to peruse the information in cloud. On the off chance that the client has entry arrangement with coordinating traits then the peruse can decode and read the message [10]. The compose operation happens as document making. The client sends the message with case arrangement and it is confirmed by cloud if the client is validated then that client is allowed to keep in touch with a current document. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

V. SYSTEM MODULES

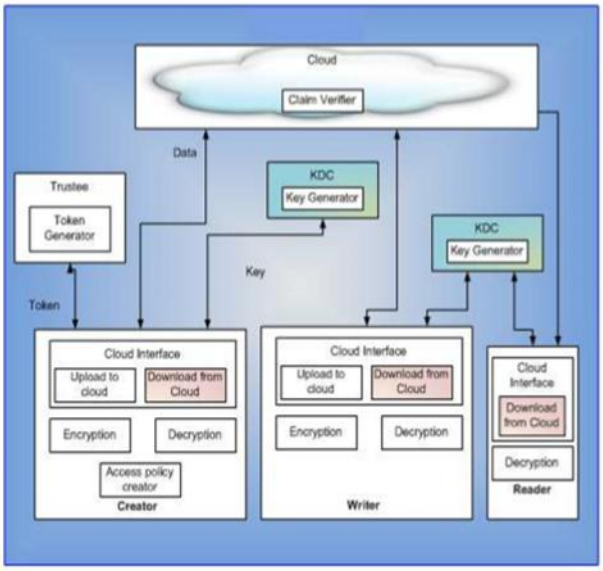

Fig 2: System Modules

A. Cloud Server Module

The cloud server will store the document made and transferred by maker as shown in fig 2. The cloud permits the client to peruse or compose access to document put away in cloud. The client must send the message and claim approach and it is confirmed by cloud if the client is verified then compose to existing record is permitted. There is a safe correspondence amongst clients and cloud.

B. User Module

Creator, Reader, Writer are distinctive clients here. Maker will make a record and transfer it to cloud. The maker will encode the information with access approach and to demonstrate the credibility maker utilizes claim arrangement y˙and signs the message utilizing this case strategy. The mark c and Ciphertext C is sent to the cloud. Characteristic Based Encryption is utilized for Encryption and decoding of information in cloud .Writer will compose to existing document in the cloud. Peruse will download the document unscramble it utilizing keys to get unique message.

C. Trustee Module

Trustee is framework or server that will check that substance maker is a substantial client. This framework gets id from maker and makes token and sends it to maker

D. KDC Module

There are various KDCs and they are situated in various areas and it creates encryption and decoding keys and keys for marking. Maker on introducing token to KDC it will provide mystery keys and keys for marking. The cloud takes decentralized methodology in conveying mystery keys and credits to client.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

VI. CONCLUSION & FUTURE ENHANCEMENT

The proposed plan gives an Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud. It forestalls replay assaults and addresses client renouncement. The client certifications are checked by cloud who store the information however cloud does not know who the client is. There are numerous KDCs for key administration. The entrance approach for every record is put away in cloud and future work may disguise the element or attributes and get to arrangement of client.

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.

ACKNOWLEDGMENT

I feel incredible joy to recognize the bearing and backing of every one of those individuals who have made my work on this anticipate fulfilling exertion and I thank unknown references for supportive proposals.

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.

AUTHOR BIOGRAPHY

Praveen.N received B.E. degree in Computer Science Engineering from VTU Belgaum in 2013. Currently studying in 4th Sem M.Tech (Computer Science Engineering) in Cambridge Institute of Technology KR Puram, Bangalore. Interest in Cloud Security and its applications.

Prof. Krishna Kumar.P.R received the B.E. degree in Computer Science engineering from Kuvempu University in 2001 and M.E degree in Computer Science from Bangalore University in 2006. He is currently pursuing the PhD

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

degree in Internet of Things. His area of interest in Applications of IOT, Cloud Securities. He is currently working as professor in Dept. of Computer Science Engineering Cambridge Institute of Technology, KR Puram, Bangalore.

Vinitha V Yadav received B.E. degree in Computer Science Engineering from VTU Belgaum in 2014. Currently studying in 4th Sem M.Tech (Computer Science Engineering) in Cambridge Institute Of Technology KR Puram, Bangalore. Interest in Cloud Security and its applications.