International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Decentralized Access Control with Anonymous Authentication for Data security in Clouds

K.L.Narasimha Rao[1]; K.Siva Rama Prasad [2]& Ch.Venkatesh [3]

[1]Associate Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana
[2]Assistant Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana
[3]M.Tech CS (PG Scholar),Dept of CSE, Marri, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

ABSTRACT

cloud computing has showed up as a popular design in managing world to back up managing large volumetric details using cluster of commodity computer systems. It is the newest effort in offering and managing computing as a service. The decentralized access control scheme distributes the data stored in cloud to user. Valid user can only access the stored information. The valid users attribute satisfies the access policy that attached to the cipher text. In the proposed decentralized approach, the technique does not authenticate users. When the users have matching set of attributes, can they decrypt the information stored in the cloud the set of attributes possessed by the revoked user. This provides user revocation and prevents replay attacks. Decentralized access control scheme can distribute secret keys for valid user in set of attribute. If the user is not authorized individually decentralized access control distribute authorized secret keys to user in set of attribute such that only that user can encrypt the stored data using its secret key. The proposed algorithm is Token Verification algorithm. Using this algorithm the creator or author of the data can verify who are all modifying the document. The algorithm provides more security in access control and authentication. Moreover, our authentication and access management theme is suburbanized and sturdy, in contrast to different access management schemes designed for clouds that square measure centralized.

Keywords- Decentralized access control; authentication

I. INTRODUCTION

Cloud computing is set of services offered through the internet. Cloud computing is receiving a lot of attention from both academic and industrial worlds. Cloud services are delivered from data centers located throughout the world. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. In cloud computing, users can outsource storage and infrastructure to servers using Internet [2].

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. 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 [1]. 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 [3].

The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. To provide secure data storage the data stored in cloud should be in an encrypted format. There are many types of access control is there in cloud User Based Access Control (UBAC), Role Based Access Control (RBAC) [7] And Attribute Based Access Control (ABAC). In User based Access control scheme there is a list of user that who can access the data. Only those users can access the data that stored in cloud. In Role Based Access Control Scheme the users who having matching set of roles they can access the data and in Attribute Based Access Control the users can access the data only if they having matching set off attributes. According to the access policy the user who satisfies certain conditions only can access the data that stored in cloud [13]. It prevents replay attacks and support creation, modification and reading data stored in cloud.

Cipher text Policy Attribute Based Encryption is a type of ABAC it provides a secure access control. Authentication and access control scheme is decentralized and robust. The valid user in set of attribute that satisfies the access policy attached with the attribute of cipher text means they can modify and store data in cloud. The validity of the user who stores the data is also verified. Using ABE, the records area unit encrypted below some access policy and keep within the cloud [4, 5]. User's area unit given sets of attributes and corresponding keys. Only if the users have matching set of attributes, will they rewrite the data keep within the cloud [6]. Access management in health care has been studied. Access management is additionally gaining importance in on-line social networking where users (members) store their personal info, pictures, and videos and share them with selected teams of users or communities they belong to. Access management in on-line social networking has been studied in [8]. Such information area unit being keeps in clouds. Data stored in clouds is highly sensitive, for example, medical records and social networks. Providing security and privacy are important issues in cloud computing [9].

Two main things are firstly, the user should authenticate itself before initiating any transaction, and on the second one is that, it must be ensured that the cloud does not tamper or interfere with the data that is outsourced or the data which is sent to the user. The wide acceptance of www has raised security risks along with the uncountable benefits so is the case with cloud computing. Also user privacy [10] is 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 to the client, and likewise, the cloud is itself accountable for the services it provides to the

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

client or the user who is accessing the cloud. The validity of the user who stores the data is also verified (by the admin). Apart from the technical solutions to ensure security and privacy in cloud, there is also a need for law enforcement such as access policies provided to the client or the users.

II. EXISTING SYSTEM

Access control in clouds is centralized in nature. All schemes use ABE or symmetric key approach and does not support authentication. Earlier work 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. 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 [14]. Although a decentralized approach is proposed in some of the existing papers, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an earlier work, a distributed access control mechanism in clouds was proposed. However, the scheme did not provide user authentication. The other draw back 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 [12].

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. In key-policy ABE or KP-ABE (Goyal et al.), the sender has an access policy to encrypt data [13]. 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. In Cipher text-policy, CP-ABE, the 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. All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase proposed a multi authority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi authority ABE protocol was studied in, which required no trusted authority which requires every user to have attributes from at all the KDCs.

Recently, 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 serve [7]r. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green et al. proposed to outsource the decryption task to a proxy server, so that the user can compete with minimum resources (for example, hand held devices). 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 [8]. Yang et al presented a modification of, 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

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

authentication without disclosing the identity of the users. However, as mentioned earlier in the previous section it is prone to replay attacks [9].

III. PROPOSED SYSTEM

Maintaining the large number of data in cloud, decentralized access control approaches is proposed. Involving distribution of secret keys and attributed of all users. Authentication access control only allows the user for reading purpose. Accessing the data by user only satisfying the access policy and authentication. 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 Figure.1 implements the architecture of 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.

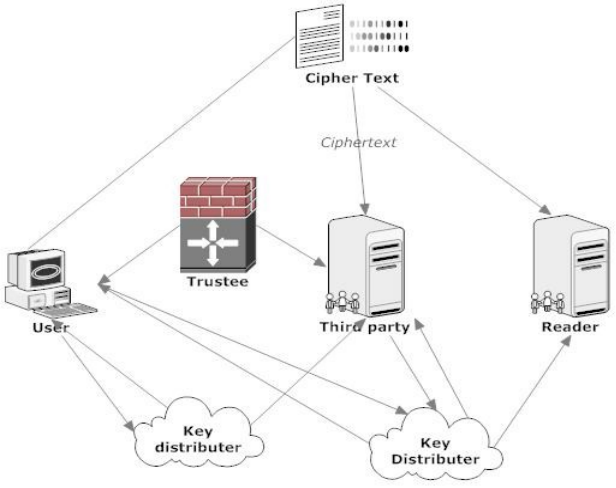

Figure 1: system architecture

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. Access control with authentication is provided on the basis of attribute based access control. It accessed on decentralized form of approach by satisfying the access policy. The data can be stored in a highly secure manner with the use of access policy.

Decentralized Authorization: This module is for authorization process. User is login to the system by giving login id and password. The given id and password is valid means they can enter in to the user window otherwise it will show an error page. Valid user who enters in to user window can read the is the cipher text associated with the access policy and the encrypting party determines the policy under which the data can be decrypted, while the secret keys are associated with set of attribute. The proposed scheme provides user revocation and prevents replay attacks. The user who didn't satisfies the access policy attached to the cipher text the user can be revoked. The revoked user can no longer enter in to the cloud. The algorithm used here is Token Verification Algorithm. It used to verify who all are modifying the data that stored in cloud and what changes they are made. In the system (fig.1) a user want to access some data in cloud means the user must satisfies the access policy attached with set of attributes of cipher text. Authentication check the users identity based on set of attribute. If it is a valid user the authentication centre allow key distribution centers to distribute secret keys to the user. Using its secret key they can decrypt the

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

cipher text or data stored in cloud and invalid user can be revoked. Revoked users can no longer enter in the cloud.

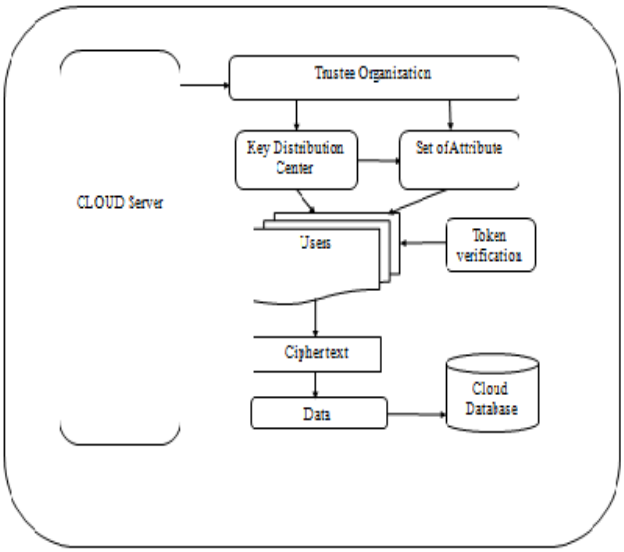

Figure 2: Data store in cloud

Information that is stored in the cloud. This is 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. A decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud.

IV. CONCLUSION

The data which is stored in the cloud is made secure with highly secure access control. A decentralized way to access control technique along anonymous authentication, which provides the user security and prevents replay attacks. The cloud is not aware of the identity of the user storing the information, but verifies the user's credentials. Key distribution center supply in a decentralized way. Data stored in clouds is highly secure. The data corruption will not happen. Efficient search on encrypted data is also an important distress in clouds. Access control is also gaining importance for users. Users can have either read or write or both accesses to a file stored in the cloud. The access policy decides who can access the data stored in the cloud.

REFERENCES

[1]. 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.

[2] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/ craig, 2009.

[3] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[4] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.

[5] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011- 38.html, 2013.

[6] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[7] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[8] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding
Attributes to RoleBased Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

[9] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89- 106, 2010.

[10]. F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained andFlexible Access Control to Outsourced Data with Attribute-BasedCryptosystems," Proc. Seventh Int'l Conf. Information SecurityPractice and Experience (ISPEC), pp. 83-97, 2011.

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

[12] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-BasedAccess Control in Social Networks with Efficient Revocation,"Proc. ACM Symp. Information, Computer and Comm. Security(ASIACCS), 2011.

[13]. S.Seenu Iropia and R.Vijayalakshmi (2014), "Decentralized Access Control of Data Stored in Cloud using Key-Policy Attribute Based Encryption" in preceedings:International journal of Inventions in Computer Science and Engineering ISSN(print):2348-3431.

[14]. R.Ranjith and D.Kayathri Devi (2013), "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication" in preceedings: International journal of Advanced Research in Computer Science and Communication Engineering ISSN (print) :2319-5940.