Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 8, Number 1 (2016), pp. 41-44

http://www.irphouse.com

A Survey on Attribute-Based Anonymous Access Control for Maximum of K-Times in Cloud Computing

Ms. Meera Chandran
M tech Scholar, Department of CSE
M-DIT Ulliyeri, Kozhikode, Kerala, India.

Ms. Nithya V.P
Assistant Professor, Department of CSE
M-DIT Ulliyeri, Kozhikode, Kerala, India.

Abstract

Cloud computing has emerged as the most dominant computational paradigm in recent times. A proper access control is the fundamental security requirement in any cloud environment, to avoid unauthorized access to the cloud systems. This paper proposes a Cloud Access control, which is a cryptographic approach particularly designed for supporting cloud computing environment. In this new notion, a user can authenticate to the cloud computing server anonymously. The server only knows the user acquires some required attributes, yet it does not know the identity of the user. In addition, it provides a limit on the access control. That is, the server may limit a particular set of users (i.e., those users with the same set of attribute) to access the system for a maximum k-times within a period or an event. Further additional access will be denied.

Keywords: Cloud Computing, Key Generation, Attribute Based Access Control

INTRODUCTION

Cloud computing is a promising computing model which currently has drawn far reaching consideration from both the educational community and industry. By joining a set of existing and new procedures from research areas, cloud computing is viewed all things considered a computing model in which assets in the computing infrastructure are given as services over the Internet.

Most of our data is stored on to the cloud. But the data i.e. stored on to the cloud is highly sensitive because here we are trusting on third party who will maintain our data. Sensitive data can be medical records and social network data. So here Security and privacy are two main issues while storing data on clouds. So that whenever user wants to access data on cloud, he should authenticate himself before initiating any transaction. Preservation of user's privacy is also important so that other user and cloud also don't know the identity of the owner of file.

Anonymous authentication is the procedure of accepting the client without the details of the client. So the cloud server doesn't know the details of the client, which gives security to the clients. To understand the concept in detail here we take one example, Suppose A engineering student John, wants to send some reports about some mismanagement by higher authorities of institute A to all the professors of institute A, all the institutes in country and all the students of engineering department. And he also wants to remain anonymous by providing all the evidence of mismanagement. He will store all the data on to cloud. And he will provide access only to authorized users. Here access control scheme is important. There are mainly three types of access control: user based access control, role-based access control (RBAC), attribute based access control (ABAC). ABAC is the extended version of these both. In this user is given some set of attribute, and the data is attached to access policy. The users who will have the valid set of attributes only allow accessing the data.

RELATED WORK

Existing system of attribute based access control is an anonymous authentication in nature and also it can further define access control policies based on different attributes of the requester, environment, or the data object. The concept of attribute-based encryption (ABE) [2], is a promising approach that fulfills these requirements. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) [3] provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data with respect to the security policy. Nevertheless, ABE only deals with authenticated access on encrypted data in cloud storage service. It is impractical to be deployed in the case of access control to cloud computing service: The cloud server may encrypt a random message using the access policy and asks the user to decrypt it. If the user can successfully decrypt the ciphertext, it is allowed to access the cloud

computing service. Although this approach fulfill the requirement, it is highly inefficient.

In addition to ABE, another similar cryptographic primitive is attribute-based signature (ABS) [4] An ABS enables a party to sign a message with fine-grained access control over identifying information. Specifically, in an ABS system, users obtain their attribute private keys from an attribute authority, with which they can later sign messages for any predicate satisfied by their attributes. A verifier will be convinced of the fact that whether the signer's attributes satisfies the signing predicate while remaining completely ignorant of the identity of signer. Thus it can achieve anonymous attribute-based access control efficiently.

Existing system described in K-times anonymous authentication [5], provides privacy preservation and access control in cloud. It uses a centralized concept. Because all the processes are controlled by an authority. Only a single authority has the responsibility to Register, Grand Access and Revoke users. Unfortunately there is disadvantage of inflexibility in nature and also it can only provide a static linkability concept. So that in proposed scheme we are using option for linkability scheme. Another scheme proposed in [6] also provides K-times anonymous authentication access control to cloud. In addition it provides dynamicity. But there are some disadvantages that are no access policy scheme is specified.

PROPOSED SYSTEM

The novel system provides the user privacy as well as data security at the time it also provides the attribute based access control over the data. The user privacy is maintained by anonymous authentication. In Proposed scheme, we can securely access the data on to the cloud using attribute based access control with anonymous authentication. An attribute-based access control scheme is a tuple of five algorithms parameterized by a universe of possible attributes A: (ASetup, USetup, TSetup, AttrGen, and Authentication).

- **ASetup:** This is a setup algorithm to be run by an attribute-issuing authority for the generation of the secret key and public key of the authority.
- **USetup:** This is a setup algorithm to be run by a user to generate the user secret key and public key.
- **TSetup:** This is a global setup algorithm to be run by a trustee for the generation of public reference information.
- **AttrGen:** This is a key generation algorithm to generate the user attribute secret key. This is an interactive protocol between the user and the authority.
- **Authentication:** This is the authentication protocol between the user and the server.

CONCLUSION

In this paper, I have presented an attribute based access control scheme with anonymous authentication, which provides privacy and prevents security attacks. Here cloud doesn't know the identity of the person who accesses the data, but only verifies the user's credentials. The files are associated with file access policies, that used to access the files placed on the cloud.

In future it aims to provide an option for both linkability and unlinkability. So it will provide more privacy to the users. ie. it only link the user previous authentication if it is necessary. And also provide an event oriented access control. In addition to specifying a particular number of accesses we can specify an event.

REFERENCES

[1] "K-Times Attribute-Based Anonymous Access Control for Cloud Computing", IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 9.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[4] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Proc. Cryptographers' Track RSA Conf., 2011, pp. 376–392.