International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 12, Number 2 (2016), pp. 223-226

http://www.ripublication.com

Forward Secure Event Oriented Attribute based Anonymous Access Control for Cloud Computing

Ms. Meera Chandran
M tech Scholar, Department of CSE, M-DIT Ulliyeri, Kozhikode, Kerala, India.
Email: meerachandran92@gmail.com

Ms. Nithya V. P
Assistant Professor, Department of CSE, M-DIT Ulliyeri, Kozhikode, Kerala, India.
Email: nithyaharisree@gmail.com

Abstract

Cloud computing has emerged as the most dominant computational paradigm in recent times. Cloud Access control scheme proposes a new notion called Forward secure event oriented attribute-based anonymous 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 an event oriented 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 within an event. Further additional access will be denied. This paper discusses the access control model used for cloud environment and presents a detailed requirement analysis for developing an access control, specifically for the cloud.

Keyword: Cloud Computing, Access Control

1. INTRODUCTION

Cloud Computing offers various types of computing services to end users via computer networks and it is being widely adopted due to its advantages. Cloud offers comparatively low cost, scalable, location independent platform.

There are still concerns about security and privacy due to its Internet-based management. In the pay-as-you-use style, the cloud service providers may charge

each enterprise or individual user for using the service. The traditional solution is to setup an account for each user. A user is required to login for using the cloud services. The service provider then charges the user based on his/her usage. This solution works perfectly, if privacy is not a concern. Consider the user privacy at the same time, account-based access control does not work since it is not anonymous. Recently proposed access control models, such as attribute-based access control (ABAC), can provide anonymous authentication while it can further define access control policies based on different attributes of the requester, environment, or the data object.

2. RELATED WORK

Many research works about cloud storage auditing have been done in recent years. **I. Teranishi, J. Furukawa, and K. Sako** [2], proposed k-times anonymous access control. It allows a user to authenticate him/her to a verifier anonymously. The verifier further knows that whether the user has been authenticated less than k-times. Different from an attribute-based access system, the authorized group of k-TAA has to be fixed a priori, which makes it less flexible in practice.

L. Nguyen and R. Safavi-Naini [3], proposed a dynamic k-times anonymous authentication, which solves the inflexibility problem by allowing the AP's to add and revoke users by keeping a separate list of users. So the Global Setup algorithm is run for the GM & AP. Then the Joining procedure allows both of them to add members to the group. PPT algorithm for revoking a user will revoke the user if the user is traced or crosses the announced bound.

V. Goyal, O. Pandey, A. Sahai, and B. Waters, Proposed ABE [4] and [5] CP-ABE. 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) 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. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access.

H. K. Maji, M. Prabhakaran, and M. Rosulek [6], proposed ABS. 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.

3. EXISTING SYSTEM

In the existing system it provide an attribute-based anonymous access control system for cloud computing. A normal anonymous attribute-based authentication system (e.g. ABS) does not allow the verifier to know it is the number of the times the prover has authenticated to the system. In contrast to this, this scheme provides a mechanism to detect whether the user has exceeded k-times for accessing the system using some defined claim-predicate (within a period or a single event). At the same time the user is anonymous to the system at any time.

4. PROBLEM DEFINITION

Main issue associated to the access control scheme is that achieving anonymity and privacy at the same time. There are many research works on K-Times anonymous access control has been done in recent years. Critical security problems with the existing surveys are computational anonymity, linkability, key exposure problem. Existing computational anonymity can reveal the identity of the users. Next problem is the linking i.e. existing works only provide linkability or unlinkability. Both are necessary in different situations. Current technique not solves the key exposure problem. So if the signature was leaked then it is required to resign all the files. K-Times Attribute Based Access Control scheme aim to provide user privacy and security at the same time. Also aim to solve the problem of option for linkability & unlinkability, event oriented linkability, and key exposure problem.

5. PROPOSED SYSTEM

In the proposed system attribute based anonymous access control is obtained by using a tuple of five algorithms. Elgamal key pair generation algorithm is used for the generation of keys users, attributes issuing authority, and trusted authority. This key generation is based on bilinear pairing.

- **TSetup:** Run a global setup Elgamal key generation algorithm for the generation of public reference information.
- **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.
- **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.

In this proposed implementation it provides 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 this implementation provides an event oriented access control. In addition to specifying a particular number of accesses we can specify an event. Also it provides a forward security by solving the key exposure problem.

4. CONCLUSION

This paper describes various algorithms which are based on anonymous user authentication. It will provide an efficient attribute based authentication. And also support event oriented access control and solves key exposure problem.

REFERENCES

[1] Tsz Hon Yuen, Joseph K. Liu, Man Ho Au, Xinyi Huang, Willy Susilo, "k-Times Attribute-Based Anonymous Access Control for Cloud Computing", IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 9.

[2] I. Teranishi, J. Furukawa, and K. Sako, "k-times anonymous authentication (extended abstract)," in Proc. ASIACRYPT, 2004, pp. 308–322.

[3] L. Nguyen and R. Safavi-Naini, "Dynamic k-times anonymous authentication," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, pp. 318–333.

[4] 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.

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

[6] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures," in Proc. Cryptographers'Track RSA Conf., 2011, pp. 376–39.