ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Anonymous User Authentication on Cloud: A Review

Deepika Dargan

M.Tech Student, Dept. of Computer Science & Engineering, B.S.Anangpuria Institute of Technology and Management, Faridabad, Haryana, India

ABSTRACT: Cloud computing as a technology which is used to store the data and information on cloud so that users on the cloud can use the available services according to their demand. Various algorithms are used to make cloud secure and deal with storage issues. Here we mainly concentrate on business cloud where various organizations store their data. Basically, data about organization's business plans stored on cloud. In this paper, we discuss about accessing the data on cloud anonymously for this various algorithm like attribute based revocation used for secure data access in the cloud, Cryptographic access control protocol called K2C (Key To Cloud) is used for securing data access, k-times attribute-based anonymous access control, which a user can authenticate himself/herself to the cloud computing server anonymously up to some limit. After discussing all these, their advantages and disadvantages and what needs to be done in future are also described in this paper.

KEYWORDS: cloud service provider (csp); Attribute based revocation; K2C (Key to Cloud); k-times Attribute-based Anonymous Access Control; Attribute Based-Hierarchal Key Updating (AB-HKU); Lazy Revocation

I. INTRODUCTION

Now a day's cloud is used for storing the data. Cloud computing is basically a combination of traditional technologies with new way of storing and securing data. Cloud service is available 24/7.cloud is basically useful as it is fast , scalable, low cost, access data on-demand, business agility and many more. There are various types of cloud namely private cloud which is used within a private organization for their private storage and computation purposes. Public cloud is a type of cloud which is used by any type of organizations for various types of purposes. Community cloud is also one of the types of cloud in which it is used for a particular community. Hybrid clouds are certain types of cloud in which it is used both as a public and private cloud. These types of cloud are called the deployment models of the cloud.

Various types of security issues addressed on cloud are the third party cloud service provider (csp) cannot be trusted as no longer used files get deleted to save storage capacity. Second, certain sensitive data which are present in an organization are made hidden to some users to provide the integrity and confidentiality of the data but it creates dispute among them that organization did not trust them. So the concept of anonymous user authentication is more useful in this situation. In this user cannot able to know who applied the security constraints on data for that user. Data privacy should be maintained anonymously.

So the Algorithm which are based on anonymous user authentication -Attribute based revocation used for secure data access in the cloud, Cryptographic access control protocol called K2C (Key To Cloud) is used for securing data access , k-times attribute-based anonymous access control, which a user can authenticate himself/herself to the cloud computing server anonymously.

II. RELATED WORK

Attribute based revocation is based on the concept of group signature and revocation list. In which each user have some set of attributes and their keys. When the user's set of attribute matches with the access policy only then individual user can decrypt the file. The group signature concept was introduced in by Chaum and Van Heyst [1] allows any user who is in that group to sign the data. Group signature also used for verifying whether the user is authorized or not. For handling authority and authentication revocation list is used. Revocation list contained the list of revoked users who are unauthorized. So, that if they again try to revoke then it should first check in revocation list.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Cryptographic access control protocol called **K2C (Key To Cloud)** provide user centric privacy for sharing and storing data on untrusted cloud .Earlier cloud is considered as trusted domain but it is not hold for long time so its security should be considered on priority.K2C is designed on the concept of lazy revocation and key-updating scheme, referred to as AB-HKU. AB-HKU scheme supports revocation access for hierarchies without requiring complex cryptographic data structures.

The scheme which is based on attribute based anonymous access control is **k-times Attribute-based Anonymous Access Control**. In this the user with particular set of attributes can access the system for maximum of k-times with in a period. When the number of access exceed the limit user can not be able to access the system any more. In this Attribute- based signature is used .ABS allows to sign a message with fine-grained access control based on their attributes. ABS is capable to provide un-linkable and anonymous attribute access control with unlimited access so k-times access control is implemented to provide limited access to particular user.

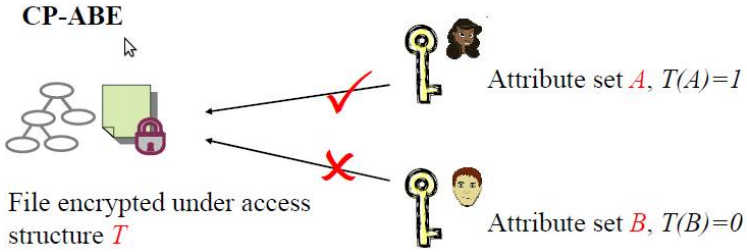

Fig-1: Assigning Attribute[2]

III. ACCESS CONTROL TECHNIQUES

A. *User based access control(UBAC):*
The access control list which contains the list of users who are authorized to access data is called user based access control. Clouds cannot use this because there are many users.

B. *Role based access control (RBAC):*
In role based access control Users can be classified on the basis of their own roles. The user who has matching roles can be able to access the data. Roles are defined by system itself.

C. *Attribute based access control (ABAC :)*
In this users are given set of attributes and the data with some access policy. The user can access the data that have valid set of attributes and also satisfying the access policy.

IV. DESIGN GOALS

A. *Security:* It provides confidentiality and integrity of stored data against cloud providers and unauthorized end-users.
B. *Privacy-preserving:* Access rights of a specific end-user as well as his usage trends should not be visible to other users or cloud service providers.
C. *Efficiency and Scalability:* To reduce cost, it should support lazy revocation. Also, the complexity of operations should be inde-pendent of number of data objects and users in the system.
D. *Flexibility:* Data hierarchies should be maintained which helps in accessing all the files. Also, they should be able to grant/revoke part of their access rights to/from other users in a decentralized and scalable manner.
E. *Simplicity and Extensibility:* All the algorithms are simple to understand.

V. WORKFLOW COMPARISON

A. ***Attribute based revocation***
Attribute based Revocation algorithm works in a group. When user from a particular group with set of attributes access data from cloud then whether user is authorized or not should be checked and if it is not then that user is added in the revocation.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

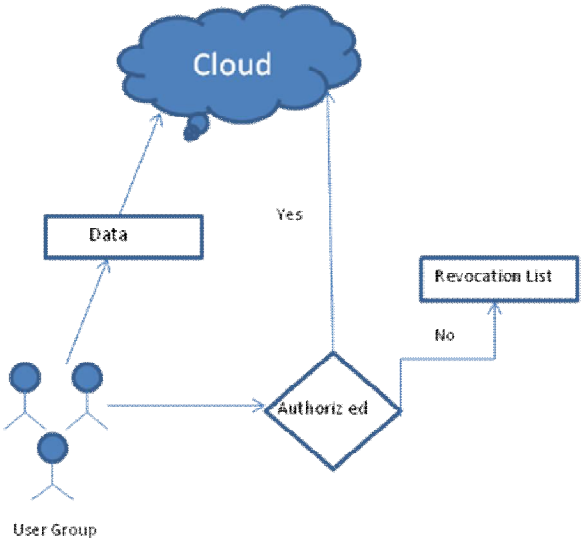

Fig-2: Revocation List Functionality

B. ***K2C (Key To Cloud)***

Key To Cloud Algorithm work on Hierarchal key updating scheme. If user having most recent key for decrypting the folder then that key automatically used for decrypting hierarchal inner folders and files. With key updating schemes, Lazy Revocation is also used , which means eliminates the extra re-encryptions until the next write access. It improves the performance. Lazy revocation, first introduced in Cephues, is a technique which reduces the overhead of revocation at the price of slightly lowered security [7].

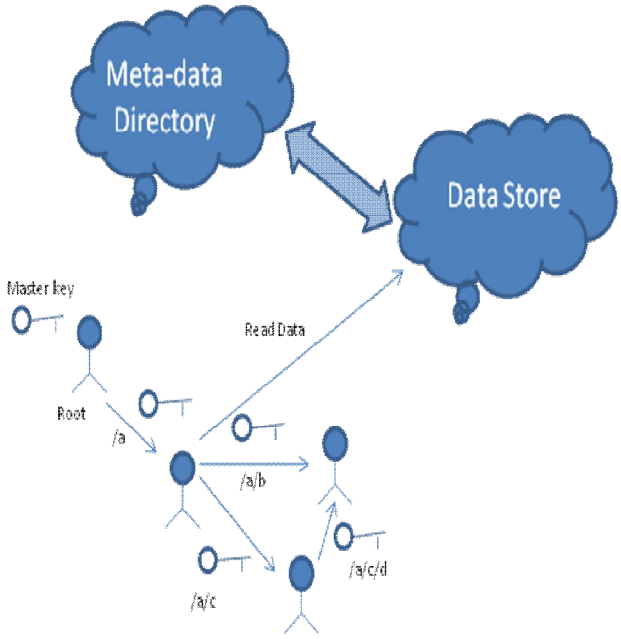

Fig-3: Key- Updating Scheme

C. ***k-times Attribute-based Anonymous Access Control***

K-Times algorithm works on the concept of event –oriented access control. In this, an authorized user can access the data on cloud only for k-times per event. Additional access should be denied.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

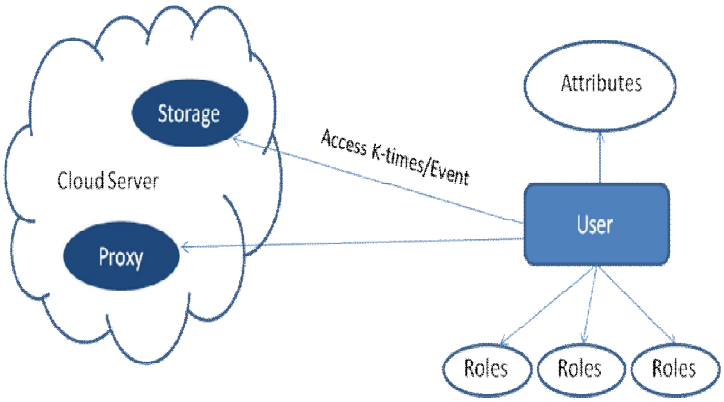

Fig-4: Event - Oriented K-times Algorithm

VI. ADVANTAGES

Some of these advantages are:

A. Computation overhead is minimized. During revocation, it is not necessary to update the keys of every user when there is a Group revocation happens.
B. Data confidentiality, anonymity, collusion resistance and integrity are achieved. As the computations are shared between the user and the administrator and the cloud, the performance of the algorithm is good.
C. These algorithms are scalable, efficient, and cost effective as in K2C algorithm key updating scheme is very cost effective. In this cost depend upon the data size of the object. Proxy re-Encryption is used to off-load re-encryption.
D. K-times algorithm is unlinkable, means it is not possible to find the anonymous user. It is Event-oriented Access control.
E. These algorithms are not restricted to number of user.

VII. ISSUES

Major issues are:

A. Maintaining confidentiality and integrity.
B. Revocation list required to be updated timely.
C. The hierarchy of folder should not be so much deep.
D. As it takes time to search the inner files and folders.
E. In this the key which is using must be updated and correctly generated.
F. Issues facing in reading and writing the file process also are a major concerned.

VIII. CONCLUSION

In this paper, we describe various algorithms which are based on anonymous user authentication. Their advantages, disadvantages and the description of main concept which is used in that algorithm with their workflow diagram and comparison between them in terms of efficiency , scalability and many other factors.

IX. FUTURE SCOPE

The future plan is to improve the efficiency of algorithm and make them more secure. Some techniques like Proxy re-encryption should be used in more efficient way. There will be a plan to combine the entire three algorithm main concept to make a more secure algorithm having all the features.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

REFERENCES

1. D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp.257-26sss5, 1991.
2. Karthikeyan.C, Vignesh.R "Data Access Control in Cloud Using Attribute Based Revocation Algorithm" Comm. ACM, vol. 2, Special Issue 1, pp. 2320-9798, March 2014
3. Michael Backes, Christian Cachin, and Alina Oprea. Secure Key-Updating for Lazy Revocation. In Research Report RZ 3627, IBM Research, pages 327–346. Springer, 2005
4. J. Bethencourt, A. Sahai, and B. Waters. Cipher text-policy attribute based encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM Conference on Computer and Communications Security, pages 89–98. ACM, 2006.
6. Dominik Grolimund, Luzius Meisser, Stefan Schmid, and Roger Wattenhofer. Cryptree: A folder tree structure for cryptographic file systems. In Proceedings of the 25th IEEESymposium on Reliable Distributed Systems, pages 189–198, Washington, DC, USA, 2006.IEEE Computer Society.
7. Kevin Fu. Group sharing and random access in cryptographic storage file systems. Technical report, Masters Thesis, MIT, 1999.

BIOGRAPHY

Deepika Dargan is currently pursuing M.tech degree in Computer Science and Engineering at B.S.Anangpuria Institute of Technology and Management, Faridabad, Haryana, India. Her areas of interest in research are cloud computing and it's Security.