International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Special Issue 39 (KCCEMSR) (March 2016), PP. 84-86

SECURE CLOUD BASED DATA ACCESS CONTROL SYSTEM

Piyush Deolikar[1]; Sibin Jacob[2]; Ankit Konchady[3]; Atul Korde[4]
[1-4]B.E. Students
Department of Electronics and Telecommunications Engineering
K.C. College of Engineering & Management studies & Research
Kopri,Thane(E)-400 603, India
[1]pdeolikar@gmail.com;[2]bugsy.macho@gmail.co m;[3]ankit.konchady@gmail.com;
[4]atul.korde@gmail.com

Abstract— **Cloud based access control system refers to a type of networked based access control system whereby an application can be run on connected servers instead of local servers. Cloud can be used to store data, share resources and also to provide services. Technically, there is very little difference between public and private cloud architecture. However, the security and privacy of the data is a very big issue when sensitive data is being entrusted to third party cloud service providers. Thus encryption with a fine grained access control is inevitable to enforce security in clouds. Several techniques implementing attribute based encryption for fine grained access control have been proposed. Under such approaches, the key management overhead is a little bit high in terms of computational complexity. Also, secret sharing mechanisms have added complexity. Moreover, they lack mechanisms to handle existence of traitors. Our proposed approach addresses these requirements and reduces the overhead of the key management as well as secret sharing by using efficient algorithms and protocols. Also, a traitor tracing technique is introduced into the cloud based access control system two layer encryption environment.**

I. INTRODUCTION

Cloud based access control system is a widely used technology that aids in sharing data as well as resources and services through the internet. Cloud based access control system has lots of beneficial characteristics such as agility, reduced cost, device and location independence, easier maintenance, multi tenancy, performance, broad network access etc. Today the based access control system world has attracted lots of organizations as well as individuals to store data on clouds for easily sharing data and thus to reduce the cost of sharing. It is well known that a coin will always have two sides. Even though the advantages of cloud data sharing are a boon, the security of the private data is a serious issue in case of really sensitive data. The private data should be made available only to the users who are authorized to use it.

Cloud based access control system requires the user to transfer their data to the cloud service provider for business as well as storage purposes. Cloud service providers cannot be fully trusted too. Even though data sounds to be a simple thing, it is the most important asset for a business organization. If sensitive data is disclosed to the public or any other competitors of organizations, serious consequences may follow. Thus when cloud is used, priority goes to ensure that the data is kept confidential and that not even the cloud service provider has access to the data that is transferred to the cloud. The responsibility to keep the data safe from unauthorized access is to the organization itself in case of private clouds. But in case of public clouds, there are chances of data theft through internet. Therefore in public clouds, before uploading data to the clouds for sharing, the data owner will encrypt the data. By this method, the cloud service providers will not be able to access the data. Along with this, in order to avoid unauthorized users from accessing the data, the encryption should be done taking into consideration the access control policies (ACPs) of the organization. The attributes specified in the ACPs reveal private information. So they should also be protected.

It also helps face insider threats. Other attribute based encryption as well as proxy re- encryption based methods where proposed earlier but they couldn't efficiently add or revoke users, attributes or policies. Other simple group key management techniques also lacked scalability as well as user attribute privacy. Recently proposed approach based on broadcast group key management address these issues. We observe that, adding new users, revoking users and updating ACPs is performed by running the key generation algorithm again and thus producing a new key and public information. The key generation being done is the most computationally expensive operation in the scheme. This is improvised in this paper by incorporating a newer version of the key management algorithm used. We also observed that the secret sharing protocol can be made more efficient by handling multiple conditions at the same time. Otherwise the communication and computation costs will increase in proportion to the number of attributes. The existence of traitors is also handled in the proposed scheme along with an audit log. The remainder of the paper is organized as follows: Section 2 introduces the related works. Section 3 gives an overview of the overall system that utilizes the fast group key

management and secret sharing. Section 4 presents the basic building blocks of this system. Section 5 gives a detailed description of the proposed system and shows how to trace the traitors and thus prevent pirates from accessing the data. Section 6 presents the experimental results and section 7 concludes the paper and outlines future research directions.

II. WORKING

Cloud-based access control system provides a convenient and cost-effective solution to most of security issues faced by web users. The existing system has lots of drawbacks, which makes the user n his data vulnerable to attacks. His data is under constant threat of getting accessed by multiple unauthorized persons. So, in this world of continuously increasing web users, a better, more secure n protected way of storing data is the need of the hour

Since cloud based access control system is basically web storage, an application is required to store the data and documents. This application is made using software ECLIPSE. This application initially asks d user to login using the username and password. Once the username and password is accepted by the application, it gives the following option:- 1.Image 2.Video. Basically the application asks the user to upload either an image or video. Once the user uploads his data into the application, it encrypts the data using an algorithm called AES. The encrypted data is stored into the web storage called cloud.
Whenever the authorized user wants to use his personal data, he can access it since it is stored in the cloud storage. Only the authorized user can access this data on his personal device (mobile). Any unauthorized access will not be allowed under any circumstances. If an unauthorized user tries to access this personalized data on any other device, he will be detected and a warning will be sent to him. Along with it, the device details of the unauthorized user will be exposed to the authorized user. This phenomena is called Traitor Detection.

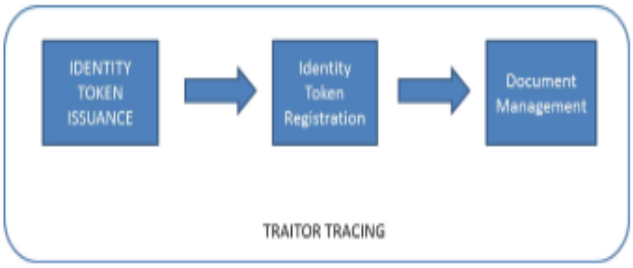

Fig.Overall Architecture of the System

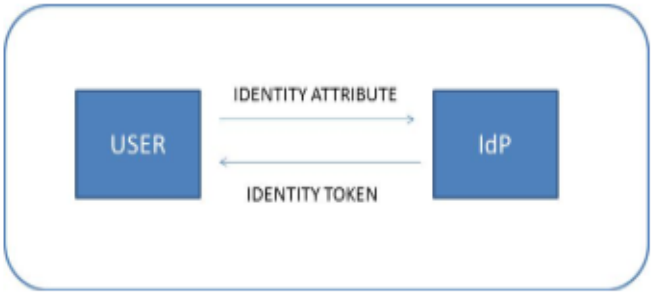

Fig. Identity T oken Issuance

A. . Flowchart

This scheme consists of mainly four entities, Owner, User, Cloud and the Identity Provider (IdP).Owner defines the access control policies and uploads encrypted documents to the cloud. Cloud holds the encrypted data of the owner, public information indexed to the policy configurations and the audit log. dP is a trusted third party that issues identity tokens to the users based on the identity attributes confirmed by the user. This is done based on a commitment scheme such as Pedersen commitment. User will register to the owner to get access to the encrypted data in the cloud after authentication.

B. 2Traitor detection algorithm

It is always nice to maintain audit logs when accessing data. A log is maintained in the proposed system that does not let anyone identify the user based on the log entries. Only the encrypted identity tokens are stored in the audit logs. The decrypted identity is shown to the owner only when an adversary is detected.

An ideal solution to stop piracy is almost impossible to achieve in reality. It is practical to assume that some piracy will occur but counter measures can be taken to deal with the threat. Broadcast encryption schemes and traitor tracing schemes can be effectively combined in order to minimize the damage caused due to piracy.

It is assumed in this work that the identity tokens generated by the identity provider are not revealed to the user. Th e pirate can access the files if he gets the secrets assigned to the user, since all other parameters in the key derivation algorithm are public values. As shown in fig., the set of secrets for each policy configuration i.e., each subdocument, are extracted during the initial stage. Thus the policy configurations are attached with a set of secrets. So whenever the user wants to access to a subdocument, the index of the secrets provided to the cloud is found and the corresponding registered identity token to which those secrets are assigned is extracted. If and only if there is a match, the subdocument can be decrypted with the original key from FACVBGKM.

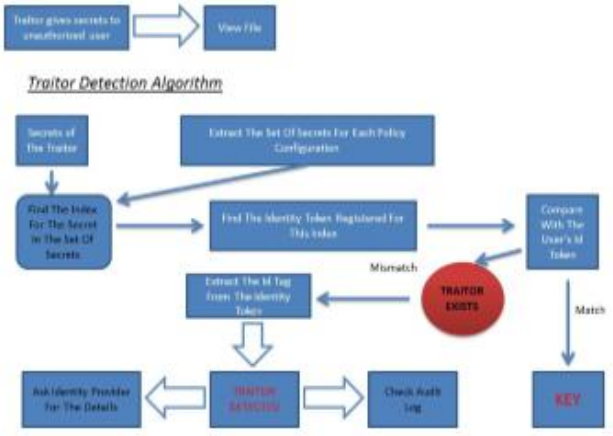

Fig.T raitor Detection Algorithm\

III. CONCLUSION

Cloud computing services have introduced a modern trend of outsourcing the data storage and manipulation functions to third party cloud service providers. But, serious security issues may arise due to the same. We have proposed an extension to the FACV-BGKM scheme for attribute based fine grained access control with better user addition and revocation computations, better evaluation of expressive access control policies and security and attains better computational complexity at the expense of higher space complexity and pre - computation. It does not provide total security but provides the best one yet.

REFERENCES

1. R. Buyya, C. ShinYeo, J.Broderg and I. Brandic, "Cloud computing and emerging it platforms : Vision, hype and reality for delivering computing as the 5th utility"

2. M. Armbrust, A. Fox, R. Grifth, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A.Rabkin, I. Stoica and

   M. Zaharia, "A view of cloud computing"

3. William Stallings "Cryptography And Network Security"

4. David Salomon "Data Compression : The Complete Reference"

   a. Khalid Sayood "Introduction To Data Compression

5. Y. Challal and H. Seba, "Group key Management Protocols: A Novel

   a. Taxonomy," Int'l J. Information Technology.

6. Sherman and D. McGrew, "Key establishment in large dynamic groups using one way function trees,"Software Engineering.

7. Mohamed Nabeel, Ning Shang and Elisa Bertino,

   "Privacy Preserving Policy-Based Content Sharing in Public Clouds".

8. "Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl.