Decentralized Access Control of Cloud Data

Mariya[1] Mrs. Sumana K R[2]
[2]Assistant Professor
[1,2]Department of Computer Network Engineering
[1,2]National Institute of Engineering, Mysore

Abstract— the paper proposes a new decentralized access control scheme that supports anonymous authentication to provide secure data storage in clouds. In our proposed system, without knowing the user's identity the cloud verifies the authenticity of the user before data is being stored. It consists of additional feature of access control through which only valid users are able to decrypt the stored information. This proposed scheme supports creation, reading and modification of the data stored in the cloud, it also avoids replay attacks. Existing systems authentication and access control schemes are centralized, where as our proposed system has decentralized access control scheme plus it is robust. The decentralized access control scheme addresses user revocation.

Key words: RBAC, ACL

I. INTRODUCTION

Using cloud computing, the user becomes free from the hassles maintaining of resources on site. He can obtain the storage and computations to servers using internet. It can provide many types of services related to infrastructures, applications and platforms. Security and privacy plays a very important role in cloud computing, since it consists of sensitive data. On one hand it should be ensured that the cloud shouldn't tamper the data which is obtained, and on the other hand the user has to authenticate himself as a valid user before initiating the transaction. Privacy is used to hide the authorized user's identity from the unknown user. The cloud is accountable for the services it provides and the user is accountable for the data it outsources. User validity is also verified when data is stored. The data needs to be encrypted to secure the data storage. However, data can be modified and this property needs to be taken into account while designing a cloud. Searchable encryption has an important concern in clouds. It enables to return the records that satisfy the query, without the cloud knowing the query. The keywords are sent to the cloud in an encrypted form, the cloud then returns the result without knowing the actual keyword which has been specified for search. Cloud maintains accountability because both cloud as well as the users cannot deny any operations performed or requested, because it involves law enforcement and technical issues. A log of transactions has to be maintained.

Let us consider a specific situation in our paper: A student of a university wants to send series of reports regarding the malpractices happening within in the university to the authorities of the university. The student wants to hide his identity while publishing the evidence of malpractices. Hence the student stores the data on cloud. Here access control plays an important role, so that only authorized professors can access the data, and makes sure that the information comes from the reliable source. The simultaneous problem of privacy, authentication and access control needs to be solved.

Access control is important so that only authorized users can access the valid service. They are of 3 types: User Based Access Control (UBAC), Attribute Based Access Control (ABAC) and Role Based Access Control (RBAC). In UBAC, has a list of authorized users to access the data that is called access control list(ACL) but it is not feasible because the cloud may contain many users. In RBAC, the authorized users are classified based on the individual roles. Data can be used by the users only if their roles matches and the roles are defined by the system. In ABAC, the authorized users are given attributes and are attached with access policy. Due to which they are extended in scope. Only the users with a specific set of attributes satisfy the access policy and through which they can access the data. It is necessary to ensure the anonymity of the user, not just to securely store the data on cloud. Say suppose, a user wants to stored important information on cloud and doesn't not want to be recognized. For example he writes a comment on an article, indicating he is a valid user but does not want his identity to be disclosed and wants his data to be stored on cloud, during this situation cryptographic protocols are used like ring signatures, group signatures, and mesh signatures. Since there are large number of users ring signature is not feasible option, pre-existence of a group assumes a group signature which is not possible in cloud. The mesh signature does not ensure if the data is coming from a single user or many. To overcome this disadvantage a new protocol is used that is Attribute Based Signature (ABS). In this the message should also consists of claim predicate, which helps in identifying if the user is a valid user or not without disclosing his identity. Other users can also verify the message and user stored in cloud. The ABS and ABE are combined to determine authenticated access control.

II. EXISTING SYSTEM

The existing system is centralized in nature for access control. The existing system does not use attribute based encryption (ABE). It does not provide support for authentication and uses a symmetric key approach. The centralized approach indicates that a single key distribution center (KDC) will distribute the attributes as well the secret keys to all the users. Earlier work provided authenticated access control in terms of privacy preserving in cloud. Since the cloud environment has large number of users and it becomes difficult to maintain a single KDC, this leads to failure not only at a single point but at many points too. Therefore we expect the cloud to have many KDC's at different locations in the world indicating it to be decentralized approach which will enable distributing attributes and keys to the users.

A. Problem Statement:

As there are large number of users on cloud a single KDC will never be sufficient at a single point, hence becomes difficult to maintain.

B. Solution:

The identity of the user is hidden when the information is stored, plus the validity of the message is authenticated, these are the additional features used.

III. PROPOSED SYSTEM

Our proposed system is decentralized in nature, this technique authenticate the users through which they can remain anonymous while accessing the cloud. In the previous work, we proposed a distributed access control technique in the cloud, however it did not provide authentication to the users. The drawbacks with respect to users were, they could store and create the file and other users could only read it, write access was not allowed to users other than the one who created it. In the initial version we elaborate on our previous work by adding an features which enables to authenticate the message validity without revealing the identity of the user since the user had stored information on cloud. In this system we use attribute based signature scheme in order to obtain privacy and authenticity. The proposed system also helps in addressing user revocation which was not addressed earlier.

A. Objectives:

- The authenticity of the user is verified without knowing the user's identity in the cloud before storing the data.
- The additional feature is that only valid users have access control and can decrypt the stored information.
- The scheme supports creation, reading, and modification of data stored in the cloud, they avoid replay attacks.
- This scheme also addresses user revocation.

B. Methodology:

In attribute based encryption (ABE), the user has a unique ID along with the additional set of attributes. The attribute based encryption (ABE) has been classified into 2 class, they are key-policy ABE and ciphertext-policy ABE. The sender has an access policy to encrypt the data in KP-ABE.

The writer cannot write back stale information if the keys and attributes are revoked. When the receiver receives the secret keys and attributes from the specific attribute authority, they can decrypt the information if the attributes matches.

In CP-ABE the access policy is obtained by the receiver in the form of a tree, with attributes in the form of leaves and monotonic access structure with OR, AND other threshold gates

IV. SYSTEM REQUIREMENT AND SPECIFICATIONS

This section shows the functional requirements that are to be satisfied by the system. The entire requirement exposed here are essential, that is, a system would not be acceptable that does not satisfy some of the requirement presented here.

A. Software Specification:

1) Operating System : Windows XP/7
2) Tool : Visual Studio 2012
3) Language : ASP.net, C#.net
4) Database : SQL Server 2008

B. Hardware Specification:

1) Processor : intel/AMD
2) Ram : 256Mb
3) Hard Disk : 20 GB.
4) Speed : 1.1 GHz
5) Input device : Standard Keyboard and Mouse
6) Output device : S VGA Color/LCD.

V. LITERATURE SURVEY

A. Privacy Preserving Access Control with Authentication for Securing Data in Clouds [1]:

This paper is about securing the data in clouds through new privacy preserving authenticated access control scheme. The authenticity of the user is verified without knowing the user's identity before storing the information in cloud. It also enables the valid user to decrypt the stored information through a feature called as access control. It avoids replay attacks. Enables to read, modify and create data but prevents writing on it. The computation, communication and storage overheads are similar to centralized approach. The proposed system is decentralized and robust in nature.

B. Toward Secure and Dependable Storage Services in Cloud Computing [2]:

Cloud storage enjoys the on-demand high quality cloud applications without the burden of software management and local hardware. It also enables user to store their data remotely. Since the advantages are clear, the services are relinquishing user's physical possession of their data outsourced. This process provides a risk in the security toward the correctness of data in the cloud. In order to overcome this problem and achieve secure and dependable cloud storage services we introduced a flexible distributed storage integrity auditing mechanism, which utilizes the distributed erasure-coded data and the homomorphic token. This proposed system has a advantage with respect to auditing it has lightweight communication and cost of computation is less. The result of auditing not only ensures strong cloud storage correctness guarantee, but also achieves fast data error localization, which identifies the server misbehaving. We consider that the cloud data is dynamic in nature, the proposed system further supports efficient and secure dynamic operations on the data outsourced, which includes block detection, appending and modification. The proposed system show that they are resilient against Byzantine failure, highly efficient, malicious data modification attack and even server colluding attacks.

C. Fuzzy Keyword Search over Encrypted Data in Cloud Computing [3]:

Cloud consists of many sensitive data. In order to provide protection in terms of privacy sensitive information are been encrypted before they are outsourced, this makes data utilization an important task. Through the searchable encryption a user can search the data only through keywords and specific file of interest. This has been a very big disadvantage in cloud and affects system usability, rendering user searching experiences very frustrating and system efficacy very low. This disadvantage is overcome in this paper. Fuzzy keyword search greatly enhances system usability by returning the matching files when users'

searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. This solution reduces storage and representation overheads through advanced technique on construction of fuzzy keyword sets and edits distance to quantify keywords similarity.

D. Ciphertext-Policy Attribute-Based Encryption [4]:

This paper is based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) wit constant ciphertext length. The number of computation pairing is constant. In this technique the encrypted data is kept confidential even if the server where the data is stored is untrusted, this method is secure against collusion attacks. ABE systems used attributes to describe the data encrypted and built policies within the user's keys, in our system attributes describe the user's credentials, and party encrypting data determines the policy who can decrypt the data. This method is closed to RBAC (Role-Based Access Control).

VI. CONCLUSION

This paper is based on the decentralized access control scheme wit anonymous authentication, which avoids replay attacks and enables user revocation. In this the cloud stores the data before knowing the identity of the user, but only verifies user's credentials. Here key distribution is done in the decentralized way. The disadvantage is that the cloud knows the access policy of each record stored within it. Future development regarding this topic would be hiding the attributes of the access policy.

REFERENCES

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy reserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.
[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. , pp. 441–445, 2010.
[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010

