International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Decentralized Access Control of Data Stored In Cloud Using Attribute Based Encryption and Hidden Attributes

Sumedha Tathavadekar[1], Vikas Maral[2]

[1]P.G. Student, Dept. of Computer Engineering. KJCOEMR Pune, SavitribaiPhule University of Pune, India

[2]Professor, Dept. of Computer Engineering, KJCOEMR Pune, SavitribaiPhule University of Pune, India

Abstract: ***Cloud computing's multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. We implemented secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches.***

Keywords: Cloud storage, Access control, authentication, attribute-based encryption

1. Introduction

Cloud computing is a metaphor used for utility and computing resources, and it may be servers, storage, applications and networks. Cloud computing has become a buzz in the present market, where a lot of research has been done based on the attention of both industrial market and academic needs. Cloud has certain essential characteristics, service models and few deployment models which provide various applications (Google Apps, Amazon's S3, Nimbus, and Windows Azure).

Most of the data which are stored in clouds are very sensitive, for example, medical records and social networks. Security and privacy has become a big issue in clouds. On the other hand, the user has to authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. Privacy of the user is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Law enforcement is also needed along with technical solutions to ensure security and privacy.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often related to health, important documents or even personal information. Access control is also gaining importance in online social networking where users store their personal information, pictures and videos and share them with selected groups of users or communities they belong to. Apart from storing contents securely in the cloud, it is also required to make certain about the anonymity of the user. For instance, if the user needs to store certain controversial information but does not want himself to be recognized, that means if a user wishes to comment on an article, but does not want his identity to be disclosed. Certainly, the user must be able to provide a proof that he/she is a valid user who stored information without disclosing the identity.

Current works on access control in cloud are based on centralized access. Even if decentralized approaches were proposed, they do not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where single key distribution center (KDC) distributes secret keys and attributes to all users.

2. Literature Survey

1. Privacy Preserving Access Control with Authentication for Securing Data in Clouds

S. Ruj, M. Stojmenovic, and A. Nayak proposed privacy preserving access control scheme. A privacy preserving access control scheme for data storage, which supports anonymous authentication and performs decentralized key management.

Advantages:

User revocation and access control policies highly contributed.

2. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

V. Goyal, O. Pandey, A. Sahai, and B. Waters proposed the sender has an authorization to encrypt information. A revoked attributes and keys of users cannot write again to

stale information. The attribute authority receives attributes and secret keys from the receiver and he/she is able to decrypt information if it has matching attributes.

Advantages:
Distribution of audit-log information and screen out encryption.

3. Multi-Authority Attribute Based Encryption

M. Chase proposed several scheme describes Key Distribution Authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority Attribute Based Encryption protocol which requires no trusted authority which requires every user to have attributes from at all the KDCs.

Advantages:
Allows a more number of attributes.

4. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance
H.K. Maji, M. Prabhakaran, and M. Rosulek proposed anonymous user authentication ABSs were introduced. This was also a centralized approach.

Advantages:
The user significantly saves decryption time, without raising the number of transmissions.

5. Attribute-Based Signatures
H.K. Maji, M. Prabhakaran, and M. Rosulek proposed decentralized approach and provides authentication without disclosing the identity of the users.

Advantages:
Secure against a malicious attribute authority

6. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption
M. Li, S. Yu, K. Ren, and W. Lou proposed Attribute based encryption (ABE) techniques. Attribute based encryption (ABE) techniques to encrypt each patient's PHR file.

Advantages:
High degree of data privacy and authentication is maintained.

3. Ststem Architecture

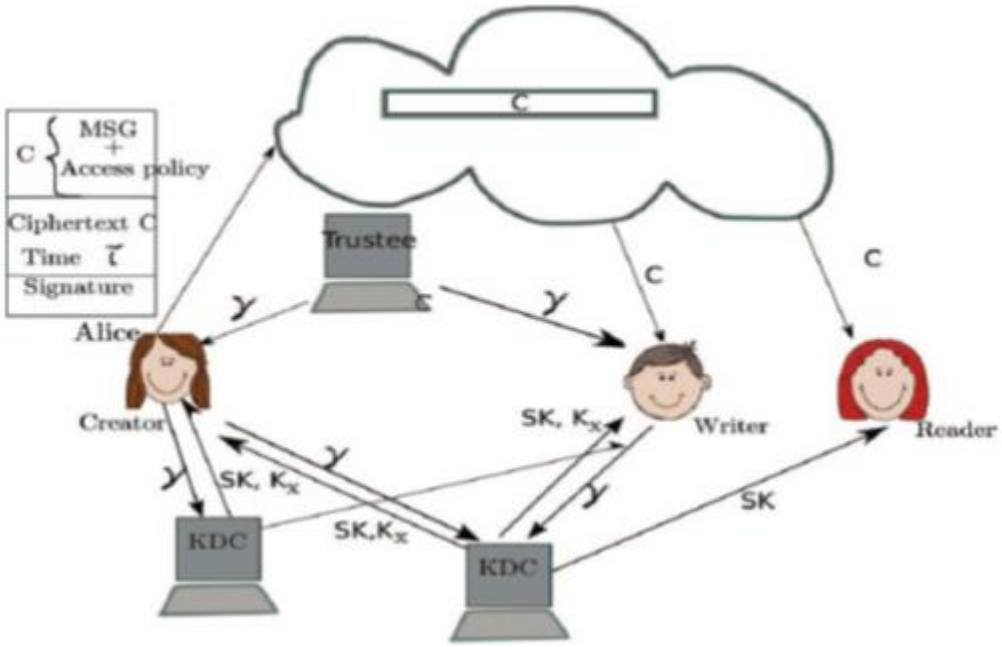

Figure 1: Secure Cloud Storage Model

This scheme consists of use of the two protocols ABE and ABS. There are three users, a creator, a reader, and writer. Creator Alice receives a token ɤ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token ɤ. There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The ciphertext C with a signature c is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

A. Data Storage in Clouds (Creator):
A user Uu first registers itself with one trustees. The trustee gives Identification Number (like Aadhaar Card No). By using Identification number (KDC) will generate private key and its attribute and through these data is encrypted using AES and stored in cloud.

B. Reading from the Cloud (Reader):
When a user requests data from the cloud, the cloud sends the cipher text C. Decryption proceeds using algorithm AES. It will gives original data to user for read.

C. Writing to the Cloud (Writer):
To write to an already existing file, the user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, is allowed to write on the file.

D. User Revocation:
To prevent replay attacks it should be ensured that users must not have the ability to access Data, even if they possess matching set of attributes.

4. Conclusion

Cloud storage security and privacy risks are identified and a Security as a Service design is proposed which could securely access data from CSP. The motivation behind this research lies in the fact that for many organizations the final barrier to adopting Cloud computing is whether it insufficiently secure. After analyzing cloud storage security and privacy risks, data protection requirements and security applied to current cloud storage services (Amazon's Cloud Drive and DropBox), the Decentralized Access Anonymous Authentication for cloud storage services is proposed. Thus proposed design of the service meets most of the defined security and privacy requirements.

References

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc.IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
[3] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
[4] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
[5] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
[6] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.
[7] SushmitaRuj, Milos Stojmenovic, and Amiya Nayak , " Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014