International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 14351-14356

http://www.ripublication.com

Privacy and Secure Revocable Data Access Control In Multi-Authority Cloud

Dr. R. Vasanthi[1] R Bhavani[2] S Dhanalakshmi[3] K Kalpana[4]
[1] Professor/ CSE, [2]PG Student, [3&4] AP/ECE
[1,2 ,3&4]Affiliated to Anna University Chennai,
Idhaya Engineering College forWomen,Tamilnadu
vasanthiattur@gmail.com,bhavanirajendiran@gmail.com

Abstract

Cloud computing provides Cloud storage as a service to the users for hosting their data in the cloud. Data access control is the well-organized method to provide data security in cloud. Cipher text-Policy Attribute-based Encryption (CP-ABE) is mostly considered for data access control in cloud storage. The existing CP-ABE is difficult to apply in multi-authority cloud storage due to the attribute revocation problem. The proposed revocable multi-authority CP-ABE scheme provides solution to the attribute revocation problem. The proposed scheme updates the components of the revoked attribute only and generates latest secret keys for the revoked attribute and forwards it to the non-revoked users who have the attributes as revoked attributes. The backward security and Forward security is assured. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself.

Index Terms: Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

Introduction

Cloud storage is an important service of cloud computing, which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access

policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

The data hosting and data access in cloud initiate a challenge in data access control. The cloud servers cannot be fully trusted by data owners, they cannot be able to rely on servers to do access control. The data owners cannot be able to assign the data access policies for the users according to their attribute relationship. In multi-authority cloud storage systems, user's attributes can be changed dynamically. A user may have new attribute generated by several other authorities and the user may revoke some of the current attributes. The users data accessing permission is should be changed accordingly with the dynamic adoption of new attribute entitling and attribute revocation.

Multi-authority CP-ABE is mostly considered technology for data access control in cloud storage systems. Users may hold various attributes issued by multiple authorities. The data access policy over the attribute is defined by the authorities and not by the data owners. The existing system is not applicable for multi-authority cloud storage due to its attribute revocation problem. If any attribute is revoked means all the Cipher text associated with the authority whose attribute is revoked should be replaced or updated. The existing system relies on a trusted server.

Techniques System Initialization and Authentication of users in Cloud

A. Registration:
Input : New user, AA **(Attribute Authorities)**
Output: Id from CA **(Certificate Authorities)**
Each user registers to the CA by providing their details. CA provides a global unique ID and certificate for each user who entering into the system. AA should also be registered to the CA. For each AA, CA provides Global unique ID and submits the certificates provided for each user in the system. The user details, AA details are stored in database.

B. Authentication:
Input : User ID
Output: Deny/access by CA
Users provide the id obtained from CA, while login for the data access in CSP. CSP validates the id using the details stored in database. If the id is valid, users are allowed for the data access in cloud, Otherwise access is denied for the user.

C. Secret Key Generation Algorithm:
Input : User ID.
Output: User's Secret Key.
After logging into the system, user provides its id to AA. AA verifies the user's certificate (Details) with the Certificate key submitted by the CA. If the user is an authorized user, AA assigns attributes and generates a secret key for the user. And AA forwards the user list and its assigned attribute to the data owner.

Data Processing and Encryption by Owner:

A. Data Processing:
Input : Attribute from AA
Output: Access control policy
The data owners first split the data into multiple components according to logical granularities. Data owner collects the attributes generated by the AA and design the access policy for each attributes.

B. Encryption By Owner:
Input : Access control policy, Content Key
Output: Encrypted Data.
The data owner encrypts the data with content keys using symmetric encryption algorithm. Then the content keys are encrypted based on access policies of each attribute and send the encrypted data together with Cipher texts to the cloud.

Data Decrypt By User:

A. Decryption Algorithm:
Input : user request for data.
Output: Decrypted data.
The user requests for the data to the cloud. If the users attribute and access control rights are satisfied, user can download the data from the cloud. User first decrypts the data for the content keys using their secret keys. Using the content keys user decrypts the original data.

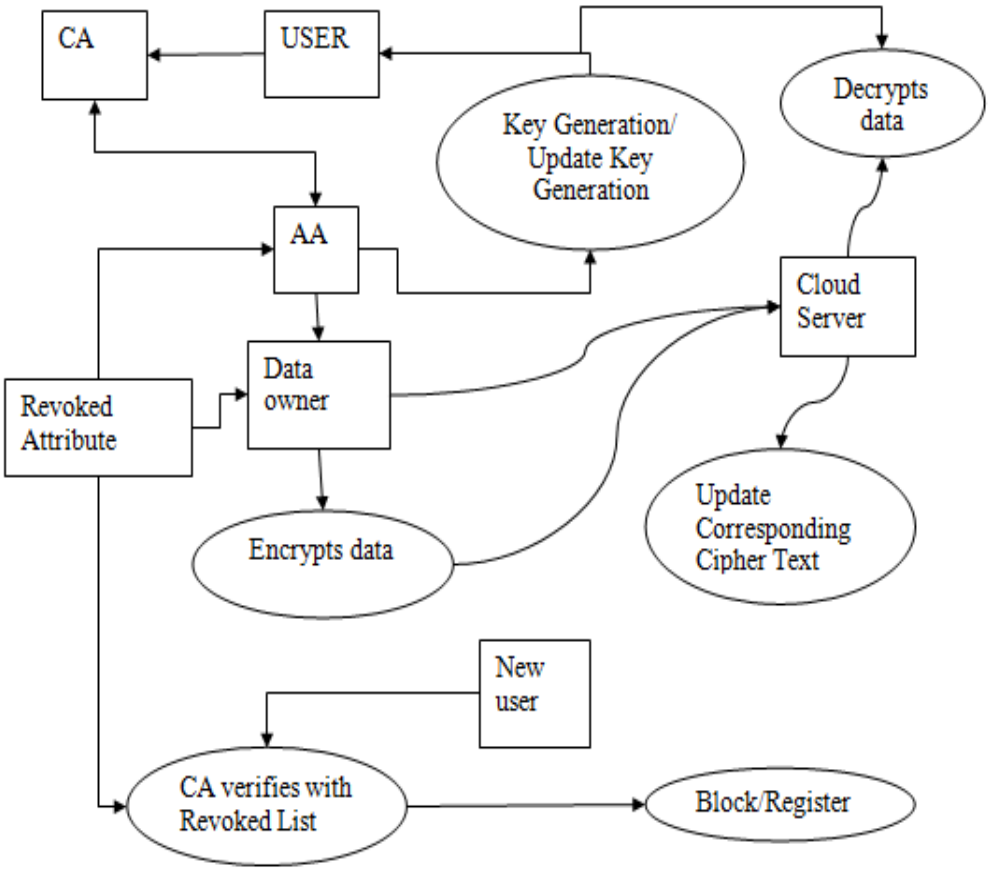
Attribute Revocation:

A. Update Key Generation:
Input : Revoked User's Attribute.
Output: Update Version key.
When an attribute is revoked from the system, the corresponding Attribute Authority generated an update version number for that particular revoked attribute. Then, AA generates an updated version of secret key and forward it to the users entitled with the revoked attribute belonging to that AA. Using the new updated secret key, user can decrypt the data.

B. Cipher Text Update:
Input : Revoked Attribute's cipher text
Output: update version Cipher Text.
When the secret key for the revoked attribute is updated corresponding cipher text is updated. The cipher text update is done in cloud. The cipher text update not only can guarantee the backward security of the attribute revocation, but also can reduce the storage overhead on users.

Blocked Revocation Attribute
Input : Revoked user list
Output : Denying the access in the Registration phase.
The revoked user can access the system after doing the registration process again and get the access according to access control policy. After registration the revoked user may try to access the system using his/her old authentication details. The unique identity of the user such as Social Security Number (SSN)/ General Identity card number is added in the revocation list. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself. Whenever user enters into the system with token, authentication is done as follows: Hash value of the token is calculated and it is matched with the stored hash value in the database. If it is matched, they are authenticated user else their access is denied.

Architecture Diagram of Proposed System



Related Work

Sreedevi N [2] Storing personal medical records on the cloud server leads to need of Encryption Mechanism .**Jahid S [4]** Problem of finding an expressive CP-ABE system under a more solid model. **Takashima K [7]** Alleviate the key leakage problem in the settings of multi-authority ABE.**John Bethen court [1]** unable to efficiently handle more expressive types of encrypted access control. **Chase M[3]** In the multi authority scheme as stated, each user must go to every authority before he can decrypt any message.

Conclusion

A revocable multi-authority CP-ABE scheme can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. The revocable multi-authority CP-ABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

Future Work

Cloud generates hash value for the received encrypted data. Generated and received hash values are compared by the Cloud. If both are same it means that data has not been modified. If the data is modified, Cloud reports the information to the data owner and asks to re-encrypt the data.

References

[1]. Bethen court J. et al (2007), Cipher text-Policy Attribute-Based Encryption', in Proc. IEEE Symp. Security and privacy (S&P'07), pp. 321-334.

[2]. Sreedevi N. (2013),'Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation', International Journal of Innovative Research in Computer and Communication Engineering, Vol.1, Issue3.

[3]. Chase M. (2007), 'Multi-Authority Attribute Based Encryption', in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), pp. 515-534.

[4]. Jahid S. et al, (2011), 'Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation', in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), pp. 411-415.

[5]. Kan Yang et al (2014), 'Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage,' IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7.

[6]. Natarajan Meghanathan (2013),' Review of Access Control Models for Cloud Computing', CS & IT-CSCP, pp.77-85.

[7]. Takashima K. et al (2010), 'Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption', in Proc. Advances in Cryptology-EUROCRYPT'10, pp. 62-91.

[8]. Waters B. (2011), 'Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization', in Proc.4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 53-70.