© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Data Revocation System Over Cloud

Sunil Sahane, Vipul Mahajan

Computer Engineering, G.H. Raisoni College of Engineering & Management, University of Pune, Pune, Maharashtra, India

ABSTRACT

Cloud era brought revolution of computerization world. One can access the data from anywhere and at any time with different devices. In this paper, we propose a secure data retrieval system using Attribute Based Encryption for the centralized database over cloud. Where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed to multiple authorize user over cloud. Using ABE key the prevention of unauthorized data access is done and maintains data security.

Keywords : Access control, ABE-key, multiauthority, verification, MD-5, AEs

I. INTRODUCTION

The text encryption has emerged with the advancement in the communication techniques. Using the various encryption techniques, a plaintext can be converted into a random figure. Thus, no information about the original text can be observed.

These optical encryption techniques are considered as symmetric cryptographic methods. Amazon EC is a web service that provides data resizable compute capacity in the cloud so we can bundle the operating system, application software and associated configuration settings into an Amazon Machine Image (AMI).

The project is a web application that could be used to generate a on-time unique identification key when a user register with self-attribute information. Once user has register in system then two different keys will be generated, 1st is public key & 2nd is Private key. So when a person have a this key then he has do encryption and decryption operation on data, which transfer from one-to-another over centralized cloud using internet service. Hence operation on both end for (sender and receiver)encryption and decryption of data. The main purpose of this project is to provide accessibility and security to the user data when transmission takes place. Using centralized storage user can view, encrypt, decrypt his data from anywhere at any time just by login.

II. METHODS AND MATERIAL

A. Existing System

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval [1]. Since some users may change their associated attributes at some point, or some private keys might be compromised, key revocation (or update), revocation of any attribute or any single user in an attribute group would affect the other users in the group. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

B. Proposed System

The ciphertext-policy ABE (CP-ABE) provides a way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy [1] [6]. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes.

The key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets.

C. Module

CP-ABE Method:

In Cipher text Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

Algorithm of Attribute base key generation:
Step 1: Start
Step 2: Data retrieval system has three modules
Step 3: Check with user Registration key in Module Database.
Step 4: Retrieve the Data from cloud.
Step 5: retrieve the original (decrypted) data

D. System Architecture

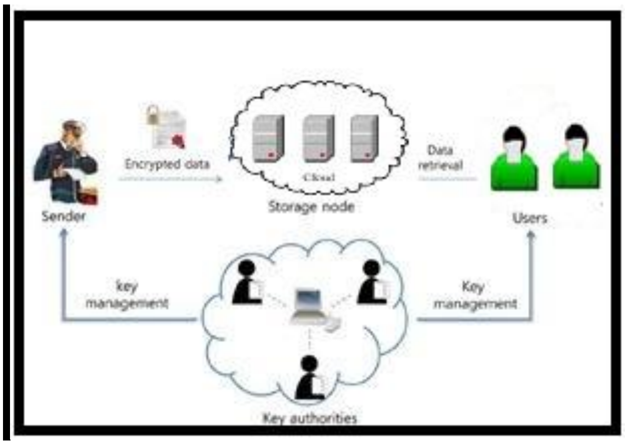

Figure 1 : System Architecture

Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

III. RESULTS AND DISCUSSION

A. Advantages

- The timestamp generated makes it almost impossible to decrypt the data, means provide a high security.
- Who stores the information, but one and only verifies the user's credentials.

B. Disadvantages

- It needs absolute accurate processing.
- High Bandwidth required when performing operation on database.
- Cloud storage cost is more than general storage.

C. Application

- ABE system is used in various IT industries, Business for data Process.
- This technique can be used to transfer important information in the
- Military services.

IV. CONCLUSION

The conclusion of the paper is to present a secure data retrieve from cloud. Its provides user revocation and prevents to the replay attacks. The cloud doesn't know the identity of the user who stores the information, but one and only verifies the user's credentials.

V. REFERENCES

[1] Secure Data Retrieval for Decentralized Disruption Tolerant Military Networks, Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM- (year-2014).

[2] O.P. Kreidl and T.M. Frazier, "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System,"IEEE Trans. Reliability, vol. 53, no. 1, pp. 148-166, Mar. 2004.

[3] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in Proc.IEEE INFOCOM, 2006

[4] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006

[5] M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM

[6] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009

[7] D. Ragsdale, C. Carver, J. Humphries, and U. Pooch, "Adaptation Techniques for Intrusion Detection and Intrusion Response System," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 2344-2349, 2000.