INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PRIVACY PRESERVING USING BROADCAST GROUP KEY MANAGEMENT IN PUBLIC CLOUD

Praveen Kumar Goud Uppala[1], Mr.Suresh Babu Kare[2]

[1]PG Scholar, Department of Computer Science, School of Information Technology, JNTUH, Hyderabad, Telangana, 500085, India.
[2]Assistant Professor, Department of Computer Science, School of Information Technology, JNTUH, Hyderabad, Telangana,500085, India.
[1]praveen.k0594@gmail.com, [2]kare_suresh@yahoo.co.in

Abstract

In public cloud, sharing documents in a set of group is a difficult task, in order to overcome this problem it is done by encrypting the document with different keys, this leads to encrypting many times. We are going to introduce a concept to manage it with Broadcasting Group Key. In this scheme adding, revoking and updating can be done easily by updating public information given.

The algorithm depends on the grouping data: the algorithm mainly focuses on different groups present in cloud and total number of keys that are generated. Using this algorithm the user can only decrypt if they satisfies the policy.

Index terms: Encryption, Privacy, Group Key Management, Cloud Computing, broadcast.

1. Introduction

The advancement in technology such as cloud computing, sharing the data using third party provider has become easier. However, such cloud provider cannot be trusted to protect the confidentiality of the data. In fact, privacy and security issue has been major concern for much organization. Data often encode sensitive information and should be protected as mandate by various organizational policies. Encryption is the common approach to protect the confidentiality. However, encryption alone is not sufficient as organizations often have to enforce fine grain access control on data. Such control is often based on attributes, referred to as identity attributes, such as the role of users in organization, projects on which the users are working. These are called attribute based systems. Therefore an important requirement is to support fine grained access control, based on policies specified using identity attributes over encrypted data.

In third party cloud service, a crucial issue is that the identity attributes in the access control policies often reveal sensitive information and leak confidential information. The confidentiality of the content and privacy of the user are thus fully not protected. Further, privacy, both individual as well as organizational is considered as key requirement in all solutions, including cloud services for digital identity management. Further, as insider threats are one the major sources of data theft, identity attributes must be strongly protected even access with organizations. With the involvement of cloud computing the insider threat is no longer limited to organizations. Therefore, protecting the identity attributes of the users while enforcing attribute based access control both within organization as well as in cloud is crucial.

An approach to support fine grained selective attribute-based access control is to encrypt each content portion to which the same access control policy applies with the same key and then upload the encrypted content to the cloud. One approach to deliver the correct keys to the users based on policies they satisfy is to use a hybrid solution where the keys are encrypted using a public key cryptosystem such as attribute based encryption(ABE) or proxy re-encryption(PRE). However, such an approach has several weaknesses: it cannot efficiently handle adding/revoking users to identity attributes, and policy changes; it requires to keep multiple copies of the same key, it incurs high computation cost. Therefore, a different approach is required

It is worth nothing that a simplistic group key management (GKM) scheme in which the content publisher directly delivers the symmetric keys to corresponding users has some major drawbacks with respect to user privacy and key management. On the one hand, user private information encoded in the user identity attributes is not protected in the simplistic approach. On the other hand, such a simplistic key management scheme does not scale well as the number of users becomes large and when multiple keys need to be distributed to multiple users. The goal of this paper is to develop an approach which does not have shortcomings.

We observe that, without utilizing public key cryptography and by allowing users to dynamically derive the symmetric keys at the time of decryption, one can address the above weakness. Based on this idea, we first formalize a new GKM scheme, called broadcast GKM (BGKM) and then give a secure construction of the BGKM scheme and formally prove its security. The idea is to give secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information. A key advantage of BGKM scheme s that adding users/revoking users or updating acps can be performed efficiently and only requires updating the public information of minimal trust, key indistinguishability, key independence, forward secrecy, backward secrecy and collusion resistance with minimal computational , space and communication cost.

Using our BGKM scheme, we are going to develop attribute based access control mechanism, where if a user is able to decrypt the contents if and only if it satisfy the identity attributes, whereas the content provider and cloud does know about the users identity attributes.

Background Work

Existing System

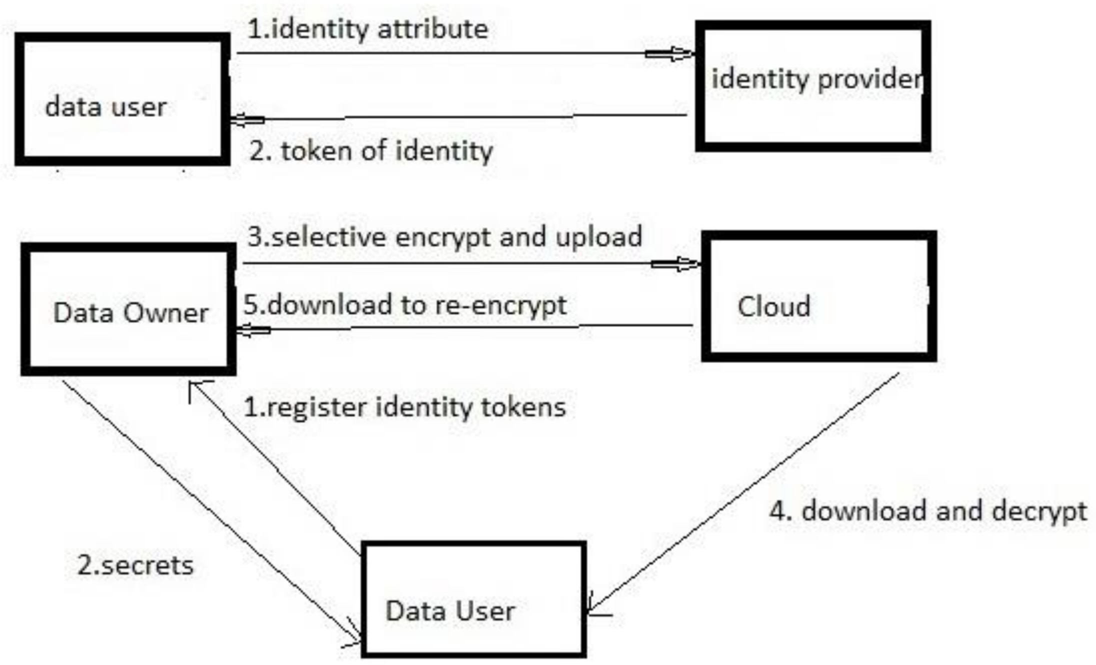
The third-party cloud services that are involved in a crucial issue is that the identity attributes in the access control policies(accesses control policies) often reveal privacy-sensitive information about users and leak the confidential information about the content. Thus, the privacy of users and confidentiality of the content are not fully protected if the identity attributes are not protected. Further, as insider threats are one of the major sources of data theft and privacy breaches, identity attributes must be strongly protected even from accesses within organizations. Privacy both individual as well as organizational are key requirements in all solutions, including cloud services. With the involvement of cloud computing the insider threats are not longer limited to organizational perimeter. Therefore, protecting the identity attributes of the users while enforcing attribute-based access control both within the organization as well as in the cloud is crucial.

Proposed System

We first formalize a new GKM scheme, called broadcast GKM (BGKM), and then give a secure construction of the BGKM scheme and formally prove its security**.** The main idea of this is to give secrets to users based on their identity attributes and later allow them to derive actual keys based on their secrets and some public information. Main advantage of the BGKM scheme is updating ACPs, adding users and revoking users, and requires only updating the public information. Our BGKM scheme satisfies the requirements of forward secrecy, backward secrecy, minimal trust, key independence and collusion resistance with minimal computational, space, and communication cost.

Using our BGKM scheme, we develop an attribute-based access control mechanism where a user is able to decrypt if the identity attributes satisfy the content provider policies, whereas the content provider and cloud do not know anything about user's identity attributes. A use can derive only the encryption keys associated with the portions the user is entitled to access.

Architecture Diagram



Group Keys Broadcasting Management

Requirements for secure Management of Group Keys

They are several requirements for effective Management of Group Keys

- Minimal trust requires the managing group key to place trust on small number of entities,
- Key hiding requires that with given public information, it is hard for anyone outside the group to gain the share group key.
- Key independence requires that the leak of one key does not comprise other keys.
- Storage requirements for keys and other relevant information should be minimal.
- Backward secrecy means that a newly joining group member cannot access any old keys.

Broadcast Group Keys

Managing group keys schemes require 0(n) or at least 0(log n) private communication channels to perform the rekey operation. In such schemes, rekeying is performed with a single broadcast without using private communication channels. These schemes are similar to secret sharing but have different purpose. Group keys broadcasting management schemes allow each valid user to recover the secret by using only their secret share. These schemes will not give users the private keys. Instead users are given secret which is combined with pubic information to obtain the actual private keys. Such schemes have the advantage of requiring a private communication only once for the initial secret sharing. Such schemes assure forward and backward security by only changing the public information and without effecting secret sharing given to existing user.

Contribution

Our scheme involves four main components

Data owner
Data user
Identity providers
Cloud service providers

Our approach is based on the following phases

1). Generating User Identity

It generates tokens for users. It is in the form of specified electronic format. These tokens are secured from outside environment. These tokens are used while registering with the cloud storage.

2). Registration with Token

The cloud user has to register with the data owner to access the data stored in the cloud. In order to access the data the user need to register with identity token. The data owner generates some secret keys using security generation algorithm, and distribute these secret keys with the cloud user. The user use these secret keys to download and decrypt the data present in the cloud.

3). Managing the document

Policy configurations are predicted by owner groups. The documents are classified into sub parts depending on the policy configurations. Using ACPs in each policy configuration using the key generation algorithm and our approach handles efficiently new user registration and user revocations.

Privacy Preserving

We use cryptographic techniques to protect the privacy of the identity attributes of the users from the server while executing the secure generation algorithm. This technique makes sure that users receive the secret only from valid identity attributes. We use two cryptographic construct, Pedersen commitments and OCBE protocols.

Pedersen commitment

Pedersen commitment scheme is an unconditionally hiding and computational binding commitment scheme which is based on the intractability of the discrete logarithm problem. Setup. A trusted third-party T chooses a finite cyclic group G of large prime order p so that the computational Diffie-Hellman problem is hard in G. Write the group operation in G as multiplication. T chooses two generators g and h of G such that it is hard to find the discrete logarithm of h with respect to g, i.e., an integer such that h ¼ g. Note that T may or may not know the number. T publishes ðG;p;g;hÞ as the system's parameters. Commit. The domain of committed values is the finite field IFp of p elements, which can be implemented as the set of integers IFp ¼f 0;1;...;p1g. For a party U to commit a value x 2 IFp, U chooses r 2 IFp at random, and computes the commitment c ¼ gxhr 2 G. Open. U shows the values x and r to open a commitment c. The verifier checks whether c ¼ gxhr

OCBE protocols

The OCBE protocols provide the capability of delivering information to qualified users in an oblivious way. They are three communications parties, receiver R, sender S and a trusted third party T

- R makes a data request to S.
- Based on the request, S sends to R a predicate GEx0 2P .
- Upon receiving this predicate, R sends to S a Pedersen commitment c ¼ gxhr.
- S checks that cgx0 ¼Q'1 i¼0ðciÞ2i. S randomly chooses ' bit strings k0;...;k '1, and sets k ¼ Hðk0 kkk '1Þ. S picks y 2 IF p, and computes ¼ hy;C ¼E k½M, where M is the message containing requested data. For each 0 i '1 and j ¼ 0;1, S computes j i ¼ð cigjÞy;Cj i ¼ Hðj iÞ S sends to R the tuple

Conclusion

We have proposed an approach to support attribute-based access control while preserving privacy of user's identity attributes for sharing document in an untrusted cloud storage. Our approach is supported by a new GKM scheme which is secure and allows qualified users to efficiently extract decryption keys for the portions of documents they are allowed to access, based on the subscription information they have received from the data owner.

REFERENCES

[1] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A Privacy- Preserving Approach to Policy-Based Content Dissemination," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE '10), 2010.

[2] "Liberty Alliance," http://www.projectliberty.org/, 2013.

[3] "OpenID," http://openid.net/, 2013.

[4] "Microsoft Windows CardSpace," http://msdn.microsoft.com/ en-us/library/aa480189.aspx, 2013.

[5] "Higgins Open Source Identity Framework," http://www. eclipse.org/higgins/, 2013.