Preserving Forward Security Authentication with User Revocation

Atiya Jabeen & Amtul Shanaz

[1]M.E Student, Department of CSE, Deccan College of Engineering and Technology, Darussalam Road, Mandal Nampally, Hyderabad, Telangana, India

[2]Assistant Professor, Department of CSE, Deccan College of Engineering and Technology, Darussalam Road, Mandal Nampally, Hyderabad, Telangana, India

Abstract

Cloud computing provides many services and also convenient ways of data sharing. Data in the cloud can be accessed by an individual or shared among the group and since the data often contains valuable information, security of the data plays a crucial role. Several security mechanisms have been proposed for secure data sharing .This paper reviews some security mechanism which is Identity-based (ID-based) ring signature with user revocation. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. our proposed scheme can achieve fine-grained access control, upon compromised of key of a data owner, he uses forward security mechanism which validates the past signature even if the current secret key is compromised, any user in the same group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

Keywords: Cloud computing, fine-grained access control, dynamic groups, data sharing, revoked users

.

I. INTRODUCTION

Cloud computing is mainly used for resource sharing and with very low maintenance. The cloud service providers (CSPs), such as Amazon, are able to provide a various services to cloud users with the help of powerful various datacenters. Cloud Providers provides a fundamental service is data storage (Storage as-a service). An organization allows its group members in the same group to store and share files in the cloud. By utilizing the cloud, the group members can be completely released from its local data storage and maintenance. A significant risk arises in confidentiality of those stored files. So, the users are not fully trusted the cloud servers operated by cloud provider while sensitive data stored in the cloud. To preserve data privacy and confidentiality, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

Not only content confidentiality but also fine-grained access control must be guaranteed in cloud computing environments. To realize fine-grained access control, the traditional schemes either cause high key management overhead, or require encrypting multiple copies of the content with different users' keys [1]. The emerging trend in utilizing the services of cloud is sharing of data. The data especially sensitive data which is outsourced to the cloud, poses many challenges such as data security and data access control. Data which is to be outsourced is encrypted and stored on the cloud; any user who wants to access the data should decrypt the data. This paper presents various recent approaches in sharing of data as well as revocation techniques.

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. In this paper, we further enhance the security of ID-based ring signature with user revocation system. In that PKG (Private Key Generator) can generate Private Key for all users who are registered in this system as well as PKG can revoked the users whose keys are compromised. Once these users are revoked by PKG then revoked users can not access the existing and future data files from Cloud Server. Due to which we can achieve fine-grained access control over Encrypted Data of Cloud Server.

2. RELATED WORK:

An "Identity-based ring signature", an efficient solution on applications requiring data authenticity and anonymity Identity-based (ID-based) cryptosystem, introduced by Shamir [2], eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID-based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. Ring signature is a group-oriented signature with privacy protection on signature producer. A user can sign anonymously on behalf of a group on his own choice, while group members can be totally unaware of being conscripted in the group. Any verifier can be convinced that a message has been signed by one of the members in this group (also called the Rings), but the actual identity of the signer is hidden. Ring signatures could be used for whistle blowing [3], anonymous membership authentication for ad hoc groups [4] and many other applications which do not want complicated group formation stage but require signer anonymity.

To support multiple user data operation, Wanget al. [5] proposed a data integrity based on ring signature. In the scheme, the user revocation problem is not considered and the auditing cost is linear to the group size and data size. To further enhance the previous scheme and support group user revocation, Wang et al. [6] designed a scheme based on proxy re-signatures. However, the scheme assumed that the private and authenticated channels exist between each pair of entities and there is no collusion among them. Also, the auditing cost of the scheme is linear to the group size. Another attempt to improve the previous scheme and make the scheme efficient, scalable and collusion resistant is Yuan and Yu [7], who designed a dynamic public integrity auditing scheme with group user revocation. The authors designed polynomial authentication tags and adopt proxy tag update techniques in their scheme, which make their scheme support public checking and efficient user revocation. However, in their scheme, the authors do not consider the data secrecy of group users.

Chaum and van Heyst [8] first introduced the concept of group signatures. In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. The variant of the short group signature scheme [9] will be used to achieve anonymous access control, as it supports efficient member-ship revocation. A number of revocation mechanisms for group signatures have been described. All these mechanisms can be applied to the system. The Revocation Authority (RA) publishes a Revocation List (RL) containing the private keys of all revoked users. Consequently the Revocation List can be derived directly from the private keys of revoked users. The list RL is given to all signers and verifiers in the system. It is used to update the group public key used to verify signatures. The given RL, anyone can compute this new public key, and any unrevoked user can update her private key locally so that it is well formed with respect to this new public key. Revoked users are unable to do so.

3. SYSTEM METHODOLOGY:

3.1 System Architecture:

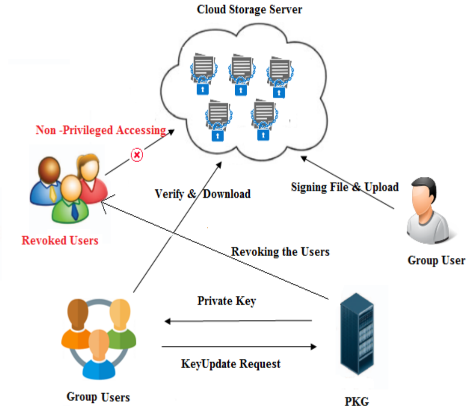

Figure: 1 System Architecture

As illustrated in figure 1, the system architecture consists of three different entities: the

Group Users or Group User, PKG, and Revoked Users.

Group Users or Group User:

In Proposed System Users can register with different Groups and after registration PKG (Private Key Generator) can be generate Private Key for them. Once the users authenticated then they can signing the files (Encrypting) with the same group users and upload into cloud storage server for data sharing. In the same group users can verify the signature and downloaded the files (Decrypting) if Valid. As well as they can send a request to PKG for key updations.

Private Key Generator (PKG):

In this System PKG can generate Private Keys for users and updated the keys also. As well as PKG can revoke the users.

Revoked Users:

Here Revoked Users can not accessing the data files from Cloud Storage Server, due to which we can achieve fine-grained access control over Cloud Storage Server.

Cloud Storage Server:

The cloud storage server, maintained by the cloud service providers, provides storage space for storing data files in a pay-as-you-go manner.

4. SECURITY MODEL

An Identity-based (ID-based) ring signature with user revocation scheme which typically involves two entities, PKG and users (including sender and receiver) is consisted of the following algorithm

Setup:

On input an unary string 1λ where λ is a security parameter, the algorithm outputs a master secret key msk for the third party PKG (Private Key Generator) and a list of system parameters param that includes λ and the descriptions of a user secret key space D, a message space M as well as a signature space Ψ.

Extract:

On input a list param of system parameters, an identity IDi 2 f0; 1g∗ for a user and the master secret key msk, the algorithm outputs the user's secret key ski;0 2 D such that the secret key is valid for time t = 0. In this paper, we denote time as non-negative integers. When we say identity IDi corresponds to user secret key ski;0 or vice versa, we mean the pair (IDi; ski;0) is an input-output pair of Extract with respect to param and msk.

Update:

On input a user secret key ski;t for a time period t, the algorithm outputs a new user secret key ski;t+1 for the time period t + 1.

Sign:

On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set L = fIDi 2 f0; 1g∗ji 2 [1; n]g of n user identities, a message m 2 M, and a secret key skπ;t 2 D; π 2 [1; n] for time period t, the algorithm outputs a signature σ 2 Ψ.

Verify:

On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set L = {IDi € {0; 1} ∗ | I € [1.n]}of n user identities, a message m 2 M, a signature σ 2 Ψ, it outputs either valid or invalid.

User Revocation:

On Input a User ID and PKG can revoke the users with the help of user ID. When user has revoked by PKG then user account status can change as from normal to revoke like IDi → {0, 1}. When revoked users wants to accessing the storage files from CSS, then first CSS can check the revocation list for providing the storage files and if any user is exist in revocation list then CSS can denied for accessing the storage files.

5. CONCLUSION:

Data sharing has become prominent in the current day scenario; therefore much importance is given to the security of data stored in the cloud. Since the data is dynamic, many security and access control schemes are proposed, in this paper, few recent approaches in data security and also some access control mechanisms for revoked users have been presented. Moreover, our scheme can achieve secure user revocation; the revoked users can not be able to get the original data files once they are revoked even if they conspire with the un-trusted cloud.

6. REFERENCES:

[1] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" IEEE TRANSACTIONS ON COMPUTERS VOL: 64 NO: 6 YEAR 2015

[2] X. Wang, Y. Lin, "An efficient access control scheme for outsourced data," Journal of Computers, vol. 7, no. 4, pp. 918-922, 2012.

[3] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer, 1984.

[4] R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 552–565. Springer, 2001.

[5] E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In M. Yung, editor, CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 465–480. Springer, 2002.

[6] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, " Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" in Proc. Of IEEE Cloud 2012, Hawaii, USA, Jun. 2012, pp. 295–302.

[7] B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp.2904–2912.

[8] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp.2121–2129.

[9] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[10] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.