IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

A Study on Proxy Re-Signatures for Public Auditing of Shared Data on the Cloud

Jyothi Anantula
AGI, Ghatkesar, Telangana, India

Abstract: Cloud computing has evolved as the current major technology in IT industry .Among many services provided by the cloud, data service has much importance and is very much susceptible as the data can be shared and modified by different users in the group . As the cloud cannot be trusted, the owner of the data can delegate the task of checking integrity of the shared data .In this paper a study is made on some proxy re-signature schemes and also a public auditing scheme using the idea of proxy re-signatures for efficient integrity checking of data

Keywords: Integrity, Proxy, cloud, shared data

1. INTRODUCTION

In the current era much of the data is being produced and consumed .To store, retrieve and to have computation on the data a cloud can be very much helpful .cloud provides many services such as Saas, Paas and many other services, with which the user or a company can get rid of the burden of having the required resources. With the data stored on the cloud users of group can collaborate with each other , share and modify the data .Though the cloud promises about the security and integrity of the data stored ,it can be compromised due to the existence of hardware/software failures and human errors [2], [3].

To have protection of data, the owner of the data can verify integrity of the data. Various mechanisms have been proposed for integrity verification [4],[5],[6] . In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of all the signatures As the data is no longer with the user, he needs to download the entire data from the cloud to check the integrity of the data which incurs more IO and transmission cost across the network. The overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The idea of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models [6],[7].

With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users [8],[9],[10]. To have security to the shared ,the blocks are signed and the task of signing can be delegated to proxy upon the temporal absence and lack of computing power of the user [11]

In this paper a study is made on some proxy signature schemes, [11] [12] Bleumer, and Strauss (BBS) proposed proxy re-signatures, in which a semi trusted proxy acts as a translator between Alice and Bob. To translate, the proxy converts a signature from Alice into a signature from Bob on the same message. The proxy, however, does not learn any signing key and cannot sign arbitrary messages on behalf of either Alice or Bob. [12].after this proposal not many advances are done until Atinese [11] proposed new definition s and algorithms on proxy resignatures based on bilinear maps.

The idea of proxy re-signatures is used for public auditing of the shared data stored on the cloud where the cloud acts as proxy and re-sign the blocks that were signed by the user.

2 .PROXY RE-SIGNATURE SCHEMES

Proxy signatures have found numerous practical applications, particularly in distributed computing where delegation of rights is quite common. A proxy signature protocol allows an entity, called the designator or original signer, to delegate another entity, called a proxy signer[13] The authors of the BBS paper [12] introduced several potential applications of proxy re-signatures.but has limitations as since it is possible to recover the information that would be stored at the proxy (the re-signature key) by looking at the original signature and its transformation. The BBS scheme is what the authors called "symmetric" [12], which means that, from the re-signature key (which is public!), Alice can recover Bob's secret key or vice-versa Another proxy re-signature scheme proposed by Ateniese [8] proposed two secure proxy re-signature schemes based on bilinear maps. first scheme relies on the Computational Diffie-Hellman (CDH) assumption; here the proxy can translate from Alice to Bob and vice-versa. second scheme relies on the CDH and 2- Discrete Logarithm (2-DL) assumptions and achieves a stronger security guarantee – the proxy is only able to translate in one direction. Constructing such a scheme has been an open problem since proposed by BBS in 1998.

The first is a bidirectional proxy re-signature in which the proxy can translate from Alice to Bob and vice-versa using a single proxy key. The scheme is very attractive for its

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

simplicity. Unlike the bidirectional BBS scheme, here the proxy can keep his proxy keys private. This scheme also allows for multi-use, meaning that a signature may be transformed from Alice to Bob, then from Bob to Carol, and so on. The security of the scheme is based on the Computational Diffie-Hellman (CDH) assumption, i.e., given (g, gx , gy), it is hard to compute g xy, in the random oracle model.

The second scheme is unidirectional in that the proxy can be given information that allows it to translate from Alice to Bob, but not from Bob to Alice. This is the first construction of a unidirectional scheme since it was proposed as an open problem by BBS seven years ago . (In BBS, they refer to such schemes as asymmetric.) Here, we allow the re-signature key to be public so that anyone can act like a proxy but, at the same time, we ensure that certain important security properties are guaranteed based on its unidirectional nature. (We also provide some insight on how one might keep this proxy key private.) The security of this scheme is based on the CDH and 2-Discrete Logarithm

Two secure proxy re-signature schemes: bidirectional and unidirectional. The bidirectional scheme Sbi is based on the short signatures of Boneh et al. The unidirectional scheme Suni is a novel El Gamal-type algorithm over bilinear maps.

The below table gives the comparisions between the two schemes BBS [12] and Ateniese [8].Where S_{Bi} represents birectional proxy resignature scheme and S_{Uni} represents unidirectional proxy rsignature scheme

S.NO	PROPERTY	BBS 12	S_{Bi}	S_{Uni}
1.	Unidirectional	No	No	Yes
2.	Multi-use	Yes	Yes	No
3.	Private Proxy	No	Yes	No
5.	Transparent	Yes	Yes	Yes
7.	Non-interactive	No	No	Yes
8.	Non-transitive	No	No	Yes
9.	Temporary	No	No	Yes

2.1 preliminaries

BBS Re-Signatures [12]. BBS proxy re-signature scheme with global parameters (g, p, q, H), where g is a generator of a subgroup of Z ∗ p of order q = Θ(2k) and H is a hash function mapping strings in {0, 1} ∗ to elements in Zq.

• Key Generation (KeyGen): On input the security parameter 1k , select a random a ∈ Zq, and output the key pair pk = g a and sk = a.

• Re-Signature Key Generation (ReKey): On input two secret keys skA = a, sk B = b (the public keys are not required for this algorithm), output the resignature key rkA→B = a/b (mod q).

• Sign (Sign): On input a secret key sk = a and a message m, select random elements x1, . . . , xk ∈ Zq. Then, compute r = (g x1 , . . . , gxk) (mod p) and extract k pseudorandom bits b1, . . . , bk from the output of H(r). Finally, output the signature σ = (r, s), where s = (s1, . . . , sk) and each si = (xi − mbi)/a (mod q).

• Re-Sign (ReSign): On input a re-signature key rkA→B, a public key pkA, a signature σ, and a message m, check that Verify(pkA, m, σ) = 1. If σ verifies, set r 0 = r and s 0 i = sirkA→B (mod q), and output the signature σB = (r 0 , s0), where s 0 = (s 0 1 , . . . , s0 k); otherwise, output the error message ⊥.

• Verify (Verify): On input a public key pkA, a message m, and a purported signature σ = (r, s), compute H(r) and extract pseudorandom bits b1, . . . , bk. For each g xi ∈ r and si ∈ s, check that (pkA) si = g xi/gmbi (mod p). If all check pass, output 1; otherwise output 0.

Given any pair of signatures (σA, σB), where σA was created by the Sign algorithm and σB is the result of the ReSign algorithm on σA, anyone can compute the re-signature key rkA→B as follows: Let σA = (r, s) and σB = (r, s0) be signatures as described above, where s = (s1, . . . , sk) and s 0 = (s 0 1 , . . . , s0 k). Anyone can compute rkA→B = s 0 1 /s1 = a/b (mod q) and become a rogue proxy. Moreover, from rkA→B, Alice (resp., Bob) can compute Bob's (resp., Alice's) secret key.

Although the BBS scheme satisfies their security definition (the scheme is called symmetric), it is clearly in adequate and cannot be used for many interesting applications, including those suggested in the original BBS paper [8].

2.2. Application of Proxy Resignature

Easy to Manage Group Signatures (using Suni). Proxy re-signatures can be used to conceal identities or details of the structure of an organization. For instance, a corporate proxy sitting on a company's outgoing mail server could translate the individual signatures of its employees, which are perfectly valid signatures inside the organization, into signatures that can be verified with a single corporate public key. The proxy could (optionally) log which employee signed the message for internal auditing, but choose to keep that information company confidential.[8]

3. PUBLIC AUDITING OF SHARED DATA USING PROXY RE-SIGNATURES

To improve the efficiency of data sharing among the group and also to check the integrity of the data a new scheme has been proposed to let the cloud to act as the proxy and convert signatures for users during user revocation.

3.1 Homomorphic Authenticable Proxy Re-Signature Scheme (Haps)

proxy re-signature schemes [8], [12] are not blockless verifiable, to directly apply these proxy resignature schemes in the public auditing mechanism, then a verifier has to download the entire data to check the integrity, which will significantly reduce the efficiency of auditing. Homomorphic authenticable proxy re-signature scheme, which is able to satisfy blockless verifiability and non-malleability.

DOI 10.17148/IJARCCE.2016.56152

This proxy re-signature scheme includes five algorithms: KeyGen, ReKey, Sign, ReSign and Verify In KeyGen, every user in the group generates his/her public key and private key. In ReKey, the cloud computes a re-signing key for each pair of users in the group. It is assumed that private channels exist between each pair of entities during the generation of re-signing keys, and there is no collusion. When the original user creates shared data in the cloud, he/she computes a signature on each block as in Sign. After that, if a user in the group modifies a block in shared data, the signature on the modified block is also computed as in Sign. In Resign, a user is revoked from the group, and the cloud re-signs the blocks, which were previously signed by this revoked user, with a re-signing key. The verification on data integrity is performed via a challenge-and-response protocol between the cloud and a public verifier. More specifically, the cloud is able to generate a proof of possession of shared data in Proof Gen under the challenge of a public verifier. In Proof-Verify, a public verifier is able to check the correctness of a proof responded by the cloud.

CONCLUSION

To efficiently check the integrity of data on the cloud, the idea of proxy resignatures is used, in this study some of the proxy resignature schemes are shown which forms the basis

REFERENCES

1 M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski,G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"A View of Cloud Computing," Comm. ACM, vol. 53, no. 4,pp. 50-58, Apr. 2010.

2 G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07),pp. 598-610, 2007.

3 A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

4 Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

5 H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

6 Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370

7 Giuseppe Ateniese, Susan Hohenberger, "Proxy resignatures :New definations alogorithms and applications" November 28, 2005

8 S.R. Tate, R. Vishwanathan, and L. Everhart, "Multi-User Dynamic Proofs of Data Possession Using Trusted Hardware,"Proc. Third ACM Conf. Data and Application Security and Privacy(CODASPY'13), pp. 353-364, 2013

9 B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM,pp. 2904-2912, 2013.

10 M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: delegation of the power to sign messages. IEICE Trans. Fundamentals, E79-A(9), 1996.

11 M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," Proc. Int'l Conf. the Theory and Application of cryptographic Techniques (EUROCRYPT'98), pp. 127-144, 1998.

12 A. Boldyreva, A. Palacio, and B. Warinschi. Secure proxy signature schemes for delegation of signing rights.Cryptology ePrint Archive, Report 2003/096., 2003.

13 B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM,pp. 2904-2912, 2013.