ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Secure Data Sharing in Clouds by Using High Level Petri Nets

Priti Kanhere[1], Prof. S.A.Patil [2]

M.E Student, Dept. of Computer, JSPM's BSIOTR Wagholi, Pune, India[1]

Asst. Professor, Dept. of Computer, JSPM's BSIOTR Wagholi , Pune, India[2]

ABSTRACT: Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments.

KEYWORDS: Access control, cloud computing, high-level Petri nets (HLPNs).

I. INTRODUCTION

CLOUD computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers [1]. Organizations with a low budget can now utilize high computing and storage services without heavily investing in infrastructure and maintenance [2]. However, the loss of control over data and computation raises many security concerns for organizations, thwarting the wide adaptability of the public cloud. The loss of control over data and the storage platform also motivates cloud customers to maintain the access control over data (individual data and the data shared among a group of users through the public cloud) [4]. Moreover, the privacy and confidentiality of the data is also recommended to be cared for by the customers [5]. The confidentiality management by a customer ensures that the cloud does not learn any information about the customer data. Cryptography is used as a typical tool to provide confidentiality and privacy services to the data [5]. The data are usually encrypted before storing to the cloud. The access control, key management, encryption, and decryption processes are handled by the customers to ensure data security [6]. However, when the data are to be shared among a group, the cryptographic services need to be flexible enough to handle different users, exercise the access control, and manage the keys in an effective manner to safeguard data confidentiality [7]. The data handling among a group has certain additional characteristics as opposed to two-party communication or the data handling belonging to a single user. The existing, departing, and newly joining group members can prove to be an insider threat violating data confidentiality and privacy [7]. Insider threats can prove to be more devastating due to the fact that they are generally launched by trusted entities. Due to the fact that people trust insider entities, the research community focuses more on outsider attackers. Nevertheless, multiple security issues can arise due to different users in a group. We discuss some of the issues in the following discussion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. RELATED WORK

Xu et al. [9] proposed a certificateless proxy reencryption (CL-PRE) scheme for securely sharing the data within a group in the public cloud. In the CL-PRE scheme, the data owner encrypts the data with the symmetric key. Subsequently, the symmetric key is encrypted with the public key of the data owner. Both the encrypted data and the key are uploaded to the cloud. The encrypted key is reencrypted by the cloud (that acts as a proxy reencryption agent) that becomes decryptable by the user's private key. The public–private keys generated in the proposed scheme are not based on the certificates. The user's identity is used to generate the public–private key pair. The proxy reencryption is based on bilinear pairing and the BDH that makes the CL-PRE scheme computationally intensive. The computational cost of the bilinear pairing is high as compared with the standard operations in finite fields.

To reduce the computational overhead of bilinear pairing, Seo et al. [11] introduced a mediated certificateless encryption approach for data sharing in the public cloud that avoids bi- linear pairing. In the proposed scheme, the cloud generates the public–private key pairs for all of the users and transmits the public keys to all of the participating users. Partial decryption is performed at the cloud. Due to the fact that key management and partial decryption are handled by the cloud, user revocation is easier to handle. However, the proposed scheme treats the public cloud both as a trusted and untrusted entity at the same time. From a security perspective, it is not recommended to shift the key generation process to the shared multitenant public cloud environment. Moreover, the decryption is performed twice in the system that reduces the advantage of not pairing to some extent

Khan et al. [7] also utilized the El-Gamal cryptosystem and bilinear pairing for the sharing of sensitive information in the cloud. Moreover, the proposed scheme in [7] utilized the concept of incremental cryptography that divides the data into blocks and incrementally encrypts the blocks. The proposed scheme uses a trusted third party as a proxy that performs the compute-intensive operations of key generation, reencryption, and managing access to the data. However, the computational complexities of bilinear pairing still exist in the system.

Chen and Tzeng [8] proposed a methodology based on the shared key derivation method for securing data sharing among a group. The methodology uses a binary tree for the computation of keys. However, the computational cost of the proposed scheme is high as the rekeying mechanism is heavily employed in the proposed scheme. Moreover, the scheme is not tailored for public cloud systems because certain operations require cen- tralized mediations. A similar Rivest–Shamir–Adleman (RSA)- based approach was also proposed in [12]. However, the scheme was vulnerable against collusion attacks.

III. PROPOSED SYSTEM

Here we propose a methodology named Secure Data Sharing in Clouds (SeDaSC) that deals with the aforementioned security requirements of shared group data within the cloud. The SeDaSC methodology works with three entities as follows:

1) users; 2) a cryptographic server (CS); and 3) the cloud. The data owner submits the data, the list of the users, and the parameters required for generating an access control list (ACL) to the CS. The CS is a trusted third party and is responsible for key management, encryption, decryption, and access control. The CS generates the symmetric key and encrypts the data with the generated key. Subsequently, for each user in the group, the CS divides the key into two parts such that a single part alone cannot regenerate the key. Successively, the original key is deleted through secure overwriting [10]. One part of the key is transmitted to the corresponding user in the group, whereas the other part is maintained by the CS within the ACL related to the data file. The ACL is generated through the parameter submitted by the data owner. The encrypted data are subsequently uploaded to the cloud for storage on behalf of the user. The user who wishes to access the data sends a download request to the CS. The CS, after authenticating the requesting user, receives the portion of the key from the user and subsequently downloads the data file from the cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

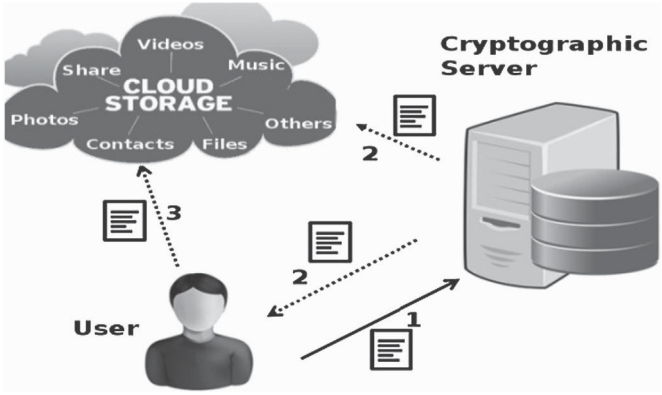

Fig.1 Proposed Architecture

A. Proposed Algorithm :

STEP 1: **PSEUDONYM GENERATION**: THE PSEUDONYM GENERATION ALGORITHM IS RUN BY EACH USER.

Input: ID

Output: Pseudonym P

Step 2: **Convergent encryption:**

KeyGenCE(M) --> K is the key generation algorithm that maps a data copy M to a convergent key K;

EncCE(K, M) --> C is the symmetric encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs a cipher-text C;

DecCE(K, C) --> M is the decryption algorithm that takes both the cipher-text C and the convergent key K as inputs and then outputs the original data copy M;

B. Pseudo Code

P - PSEUDONYM

MK - MASTER KEY

SK - PRIVATE KEY

OK - OUTSOURCIG KEY

M - MESSAGE

CT - CIPHERTEXT

$\text{SETUP}(P, K) \rightarrow (P, MSK)$ (1)

$\text{KEYGEN}(P, MSK, ID_\alpha) \rightarrow SK_\alpha$ (2)

$\text{ENCRYPT}(P, ID_\alpha, M) \rightarrow C_\alpha$ (3)

$\text{RKGEN}(P, SK_\alpha, ID_\alpha, ID_\beta) \rightarrow RK_{\alpha\rightarrow\beta}$ (4)

$\text{REENCRYPT}(P, RK_{\alpha\rightarrow\beta}, C_\alpha) \rightarrow C_\beta$ (5)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

$$\text{DECRYPT}\ (P, SK_{\alpha}, C_{\alpha}) \rightarrow M \quad (6)$$

IV. SIMULATION RESULT

The following times are included in the total time:

1) the key computation time;
2) the encryption/decryption time;
3) the upload/download time; and
4) the time of request and other related data submission to the CS and the cloud.

Fig.2 shows the results for the upload time. All of the constituent times are represented by separate line graphs. The term "others" refers to the fourth constituent time discussed previously. In general, the time to upload the data increased with the increase in the file size. However, in some cases, the marginal increase in the file upload time was small that may be due to the network condition at various times.

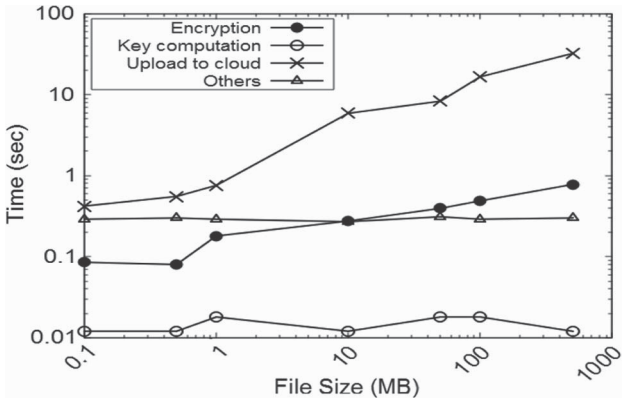

Fig.2 Performance of file uploads for SeDaSC

V. CONCLUSION AND FUTURE WORK

A data-centric authorization solution has been proposed for the secure protection of data in the Cloud. SecRBAC allows managing authorization following a rule-based approach and provides enriched role-based expressiveness including role and object hierarchies. Access control computations are delegated to the CSP, being this not only unable to access the data, but also unable to release it to unauthorized parties. Advanced cryptographic techniques have been applied to protect the authorization model. A re-encryption key complements each authorization rule as cryptographic token to protect data against CSP misbehavior. The solution is independent of any PRE scheme or implementation as far as three specific features are supported.

REFERENCES

1. A. Sahai and B. Waters, 'Fuzzy Identity Based Encryption. In Advances in Cryptology – Eurocrypt' , volume 3494 of LNCS, pages 457–473. Springer, 2005
2. R. Bobba, H. Khurana, and M. Prabhakaran, 'Attribute - sets: A practically motivated enhancement to attribute -based encryption', in Proc.ESORICS, Saint Malo, France, 2009.
3. S. Yu, C. Wang, K. Ren, W. 'Lou,Achiving secure, scalable, and fine-grained data access control in cloud computing', in Proc. IEEE INFOCOM 2010, 2010, pp. 534–542
4. G. Wang, Q. Liu, and J. Wu, 'Hierarchical attribute-based encryption for fine-grained access control in cloud storage services', in ACM Conference on Computer and Communications Security , E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 735–737
5. R. Cramer and V. Shoup, 'Design and analysis of practical public key encryption schemes secure against adaptive chosen cipher text attack', SIAM J. Compute., vol. 33, no. 1, pp. 167–226, 2004.
6. M. Green, S. Hohenberger, and B. Waters, 'Outsourcing the decryption of ABE Cipher texts', in Proc. USENIX Security Symp.,San Francisco, CA, USA, 2011, p. 34.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

7. J. Lai, R. H. Deng, C. Guan, and J. Weng, 'Attribute-based encryption with verifiable outsourced decryption', IEEE Trans. Inf. Forensics Secure., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
8. B. Waters, 'Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization', in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53– 70.
9. V. Goyal, O. Pandey, A. Sahai, and B. Waters, 'Attribute-based encryption for fine-grained access control of encrypted data', in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS '06, New York, NY, USA, 2006, pp. 89–98.
10. E. Coyne and T. R. Weil, 'Abac and Rbac: Scalable, flexible, and auditable access management', IT Professional, vol. 15, no. 3, pp. 14–16, 2013.
11. Dan Boneh and Matt Franklin, 'Identity-based encryption from the Weil Pairing', SIAM Journal of Computing, 32(3):586–615, 2003.
12. Markus Jakobsson, 'On quorum controlled asymmetric proxy re-encryption', In Proceedings of Public Key Cryptography, pages 112–121, 1999.

BIOGRAPHY

Priti Kanhere is a M.E Student in the Computer Engineering Department, JSPM's BSIOTR Wagholi College, Savitribai Phule Pune University. She received Bachelor Of Engineering (BE) degree in 2015 from Solapur University, Pandharpur, MS, India. Her research interests are Cloud Computing.

Sonali Patil is a Assistant Professor in Computer Engineering Department, JSPM's BSIOTR Wagholi College, Pune, MS, India. She Pursuing her PHD from BSAU Chennai.