Privacy Preserving Model in Semi-Trusted Cloud Environment

Amal Alsubaih[1] and Alaaeldin Hafez[2]
[1,2]System department King Saud University, Riyadh, Saudi Arabia

Abstract : **Storing sensitive data in an untrusted storage could lead to privacy violations, mainly due to disclosing of sensitive data by cloud service providers or external attackers. In this work, we address this issue by introducing a secure and fine granular access control solution that enhances the privacy in semi trusted cloud storage. Our solution protects both the data and access control policies confidentiality from privacy violations using proxy re-encryption and access control policy.**

Keywords- privacy preserving; cloud computing; proxy re-encrpytion

I. INTRODUCTION

Cloud computing provides several benefits to the user such as flexible and scalable on-demand services at reduced cost [1]. Many organizations have realized that building their own infrastructure, software or platform require large amount of budget and skilled resources. Moreover, allocating such budget or finding the most suitable skilled resources is not an easy job. Cloud computing provides well monitored resources (i.e. software, platform or infrastructure) according to the organization demand and can be expandable as they requested easily. Such offering pleased many organizations to adopt the cloud computing. Therefore, cloud computing technologies are expanded and improved rapidly to accommodate most organizations requirements.

While there are many benefits to adopt cloud computing, there are also some challenges and risks facing that adoption. One of the biggest challenges facing cloud computing is privacy issues. Sensitive data like personal, financial and medical data is stored, processed and shared in an untrusted cloud could lead to privacy violations, mainly disclose of sensitive data by cloud service providers or external attackers [2]. Moreover, loss of control raises serious concern of privacy since the data owner unaware of the location of his/her data and the operations applied on his/her data in the cloud. Also unauthorized access to the stored data due to the weakness of access control mechanism represents a serious threat to data confidentiality [3, 4]. Numerous cloud service providers have privacy and security problems that need to be addressed [5, 6]. Moritz Borgmann et al [7] studied several cloud storage service providers namely: CloudMe, Wuala, CrashPlan, Dropbox, Mega, TeamDrive, and Ubuntu One. None of them are able to meet all the security requirements sufficiently. Several vulnerabilities are found to name a few: weak authentication, shared files are exposed using the search engines, the data stored without encryption or cloud side encryption only does not prevent the disclosure of the sensitive data by the cloud. Similarly, Amazon S3 provides only a cloud side encryption to the stored data which is not protecting the data confidentiality from the cloud provider [8].

Many researchers have been discussing the privacy and security issues in the cloud [9, 10, 11, 12] .Tim Mather et al pointed that one way to enhance the privacy in cloud is via using security principles which reduce the risk of privacy violation such as unauthorized access or disclosure of sensitive data [13]. Several research works suggested a range of guidelines, recommendations and techniques to enhance the privacy in cloud environment services at early design stage [2,14,15].Yun Shen et al introduced a detailed reviews on a recent technologies used to enhance the privacy, and indicated that the security tools have a direct effect on enabling the privacy to the data [16].

Recently, many researchers propose solutions to address privacy in the cloud [17, 18, 19, 20] those solutions are usually based on data protection using cryptography, and/or authorization. Solutions such as [21, 22, 23] combine attribute-based encryption and a proxy re-encryption to provide data confidentiality and fine-grained access control in cloud; however they did not provide a sufficient protection over accesses control policy since it leaks information about the user and the encrypted data. Moreover, the data owner must re-generate a key for a user when changing in user's access privileges happened. In contrast, our solution protects both the data and access control policies from disclosing and changing in user's access privileges does not affect the user key.

Some solutions such as in [19] consider the cloud service providers as fully trusted and protect the outsourced data

Proc. Of the International Conferenceon Cloud Computing and eGovernance 2013 – ICCCEG 2013.Edited by ManikandanAyappan.© Organizers of ICCCEG 2013 [iccceg@iccceg.org].Published by Association of Scientists, Developers and Faculties, HQ, India.ISBN : 978-81-925233-2-3 || DOI : 10.ASDFOI/925233.001

from unauthorized users using the access control policy only, however our solution considers them as semi trusted and we protect the outsourced data from both the unauthorized users and the cloud using cryptography and access control policy . In this paper we address the privacy issue and propose a solution to achieve secure and fine granular access control over the data stored in semi trusted cloud by using the powerful proxy re-encryption [24] and access control policies. The main contributions of our work are: first, the solution we presented protects both the data and sensitive information and access control policies from privacy violations. Second, user revocation does not involve any data re-encryption or key re-generation to unrevoked users. Third, changing in user's access privileges does not affect his/her key.

The remainder of this paper is organized as follows, section II presents related work, section III discusses system model and design goals, section IV describes our solution in details sections V and VI introduce security analysis and discussion , and section VII concludes the paper.

II. RELATED WORK

The research on data privacy in cloud computing is evolving over the time. Various solutions have been proposed about privacy preserving in cloud environment, those solutions are usually based on concepts like cryptography, and authorization.

Siani Pearson et al. [17] have proposed architecture of a privacy manager that has many features to provide privacy called obfuscation, preferences and personae. However, the solution is not suitable for all cloud applications. Wassim Itani et al. [18] have presented PasS (Privacy as a service) to data stored and process in the cloud. In this approach, providing the privacy of the data in the cloud is depending on the use of a secure cryptographic co-processor and a set of privacy enforcement mechanisms which offer a trusted environment in the cloud. Nevertheless the co-processor is an expensive hardware which makes this solution not practical. Sascha Fahl et al. [25] have introduced confidentiality as a service (CaaS) where the data is protected by two communication layers of encryption. This service can be integrated with other cloud services to provide confidentiality to the outsourcing data , the CaaS is responsible for protection the data while the cloud provider is responsible for storing the data and enforcing the access control mechanism. Chadwick David [19] have built a privacy preserving authorisation system for the cloud on assumption that the cloud can be trusted and the cryptography is not necessarily to protect the data from cloud. The system consists of several components to enforce the privacy policies of the data owner, data controller or the law. Further, the system is able to resolve the conflicts between the policies written by different authorities and different languages and capable to do an obligation before and after the access to the outsourced data. Kamara S et al. [20] have introduced three architectures for a cryptographic storage service in the cloud. They composed of three basic components: data processor which encrypts the data before outsourcing them, data verifier that checks the integrity of stored data and token generator that responsible of creating credentials for data sharing and tokens for data searching. However the communication between the data owner and the users will be a bottle neck when the numbers of search requests increase.

Existing solutions such as [21, 22, 23] provide a secure and fine-grained data access control in the cloud based on several cryptography techniques to protect the outsourced data including attribute-based encryption and a proxy re-encryption. In contrast with those approaches, our solution provides protection to both the data and sensitive data in access control policies.

Yu et al. [21] have proposed an authorization method for data sharing in the cloud environment to prevent unauthorized access to the sensitive data using two type of encryption techniques: the first is the key policy attribute-based encryption that combines an access control policy with an encryption, each data file associated with a set of attributes and each data user has an access privilege embedded in his/her secret key. This access privilege is in a logical expression form over certain set of attributes to define the data files allowed for the user to access. Only the authorized users who satisfy the set of attributes associated with the encrypted data file can decrypt it. The second is proxy re-encryption that enables cloud servers perform re-encryption when they receive instructions from the data owner without knowing the original data. The first encryption is used for fine-grained access control and the second is used to prevent a user whose permissions are revoked from accessing the data in the future.

Similarity, Qin L, et al. [23] have proposed a time-based method called TimePRE also depending on attribute-based encryption and proxy re-encryption however they introduced a new feature that enable user's revocation automatically. Every user has a predetermined access time to the stored data and when it expired the cloud servers automatically re-encrypt the data without receiving instructions from the data owner. Nevertheless, it not suitable for environment where the data owner revokes a user anytime. Moreover, it has a limitation in the length of predetermined access time; it assigns one key to the user with same period of access time to all his attributes or multiple keys to represent different length of access periods to different attributes.

III. SYSTEM MODEL AND DESIGN GOALS

In this section, the system model and the design goals along with our assumptions are introduced.

A. System Model

In our model there are three parties: cloud service provider, data owner and data users. The cloud in the system model is responsible for storing the data, authorizing the users based on the stored policies and re-encrypting the requested data (refer to section III for more information). We assumed that the cloud is semi trusted party, honest to do the required

activity i.e. authorizing and re-encrypting but curious to know the stored data, thus both the data and the policies are hidden from the cloud. The data owner is responsible for encrypting the data before outsourcing it to the cloud, determining the policies and constrains for each data file and encrypting them before outsourcing to the cloud and generating the keys (public/private) for the users and the re-encryption keys for the cloud. When a user requests a file, his/ her request is encrypted before sending to the cloud. The cloud validate the request according to the stored encrypted policies then execute the re-encrypting on the encrypted data using re-encryption key dedicated for the user and send it to the user. At the user' side, he/she decrypts the file using his/her private key.

B. Design Goals

The design goals of our solutions are the following:

1) Protects the confidentiality of the stored data from the unauthorized user and the cloud server not to decrypt them.

2) Protects the confidentiality and privacy of sensitive information in the policies from the cloud.

3) Provide a fine granular access control using the access control polices.

IV. OUR SOLUTION IN DETAILS

A. Preliminaries

The basic idea behind our solution is using Proxy re-encryption [24] with access control policies. The Proxy re-encryption simply converts a cipher text under public key of user A into a cipher text under public key of user B without disclosing the plain text. The policy is in the following format policy (S, O, P, C) . We denote S, O, P, and C as subject, object , permission type and constrains respectively. The subject could be a user, a role in Role-based Access Control (RBAC) or even attributes in Attribute-based Access Control (ABAC) depending on the environment requirements. The permission type could be read, write, or delete. The constrains are the access time, location or any other privacy constrains.

B. Solution Description

In our work there are two main procedures: data owner initialization and user accessing the data and each of them consists of numbers of functions some of them are Proxy re-encryption functions. Next, the functions definitions and the working procedures of our solution are introduced. Summary of notations is shown in table1.

1) Functions Definitions:

The Proxy re-encryption is used to hide the data from the cloud, it consists of the following functions:

- PRE-KeyGen (par , u)□(PKu,SKu):this function is responsible for generating the key pair to the authorized users, it takes a global parameter par and the user id u and output the user key pair (public key PKu, and private key SKu).
- PRE-ReKeyGen (SKo , PKu)□RKo□u: it takes the data owner private key SKo and a user public key PKu and generates the re- encryption key RKo□u.
- PRE-Enc (data, PKo)□C: it encrypts the data using data owner public key PKo to output the cipher C.
- PRE-ReEnc (C, RKo□u)□C': it re-encrypts the cipher C to another cipher C' using re- encryption key RKo□u.
- PRE-Dec(C', SKu)□ data: it decrypts the cipher C' using user private key SKu.

- The following functions are used to hide sensitive information from the cloud:
- Pol-Enc (S, O, PKo)□(S',O'): it takes the subject S and the object O, combines them with salt, hashes them with SHA512 and then encrypts them using data owner public key PKo.
- Match(S', O', policies store)□R: it searches for the two encrypted units in the policies store and return the result of the matching R.

Notation	Description
PKo	Data owner public key
SKo	Data owner privet key
PKu	User public key
SKu	User privet key
RKo□u	User re-encryption key

TABLE 1: Summary of notations description

2) Working Procedures:

The main working procedures are: data owner initialization and user accessing the data.

a) Data owner initialization:

In this process the data owner generates the keys (public/private) for the users using PRE-KeyGen function then distributes them to the users. Moreover, he/she generates a re-encryption key for each user using PRE-ReKeyGen function; this key enables the cloud to convert the encrypted data under the data owner public key to another encrypted data under the user public key without knowing the data. Moreover, the data owner determines the policies for each data file and encrypts the sensitive part of them using Pol-Enc function. In addition, he/she encrypts the data using his/her public key PRE-Enc function. Finally, the data owner outsources the policies, the encrypted data and the encryption keys list to the cloud. Steps from 1 to 4 in Figure 1 illustrate this process.

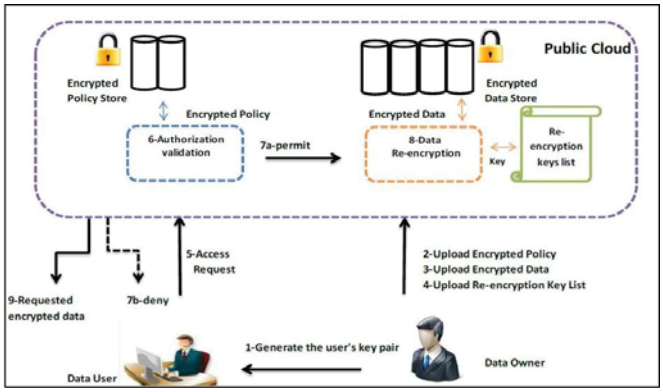

Figure 1: privacy preserving model for cloud environment.

b) User Access:

In this process, the user request access to specific data, his request is encrypted at client side using Pol-Enc function (step5 in Fig1). When the cloud receives the encrypted request, it searches for the request in the policy store to validate the authorization using Match function (step 6 in Fig1). If the user has permissions to the requested data, the cloud performs the next process which is the data re-encryption. It re-encrypts the requested data using the re-encrypting key belongs to the user in PRE-ReEnc function and sends them to the user. At the user' side, the user decrypts the data using his/her private key in PRE-Dec function.

If the user is not authorized to access the data because the matching is not found cloud denies the access and informs the user (step7b in Fig1).

C. User revocation and Permisstions Changing

User revocation process is very expensive process, usually it requires the data owner re-encrypting the data with a new key and re-distributing that key to authorized users, this emerges heavy computation overhead to the data owner because it involves data re-encryption and key re-distribution to authorized users. Some solutions delegate this heavy workload from data owner to the cloud [21]. In our solution, user revocation does not involve any data re-encryption or key re-generation to unrevoked users. The cloud only removes the revoked user re-encryption key from the re-encryption keys list without involving any addition change to other user key or the stored data. Thus, the revoked user cannot access the data without this key.

In regard to changing in user's access privileges, solutions that combine attribute-based encryption and proxy re-encryption [21, 22, 23] generate a new key for a user who permissions are changed. In our solutions, changing in user's access privileges does not affect his/her key. Simply the data owner changes the policy related to the user.

V. PRELIMINARY SECURITY ANALYSIS

Against cloud: our solution protects the confidentiality of the data against the clouds provider via encrypting them using a public key of the data owner thus the cloud cannot know the encrypted data. Moreover, our solution protects the privacy of the policies, the sensitive part of the policies (i.e. subject and object) are hidden from cloud using the encryption.

Against unauthorized access: Unauthorized users will not pass through the authorization validation. Moreover, if unauthorized user somehow accesses the data, he/she would not be able to decrypt the data; since the stored data is encrypted by the data owner public key and only he/she is able to decrypt the data, and unauthorized user does not have the re-encryption key to transfer the encrypted data to another encrypted data under his/her key .

VI. DISSCUSSION

There are three assumptions in this work, first we assume that a robust authentication stage is done prior to our authorization stage and it that authenticates the user and initializes shared session encryption keys to encrypt all ongoing communication afterward, thus, assuring secure channel for all later stages.

Second, although the process of re-encryption every file on the cloud is a power-consumption process, but we are dealing with the cloud computing which can handle such overhead much better than local resources-limited computing.

Third, we encrypted the subject and object only in our policy model and leaving the permission and constraints on clear text, because we believe that revealing the subject or object to the cloud could jeopardize the privacy of users such as the possibilities for the cloud to know the most critical file by knowing the files that grant only the CEO or other important role to access. It is not possible to encrypt the permission (i.e. read or write) or constraints (time or location) because the cloud needs to read the policy to process the right.

VII. CONCLOUTIONS

In this paper, we presented a solution to enhance the data privacy's in cloud environment. Our work is based on using a proxy re-encryption and access control policies. The main advantages of our work are protecting the confidentiality of data and a policy, and it facilitates the processes of user revocation and privileges changing comparing to existing solutions. Our ongoing work addresses expanding authorization to accommodate other aspects of security and privacy and to support more complex policies. Moreover, we will try to solve authorization conflicts and inconsistencies.

REFERENCES

[1] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." *Journal of Internet Services and Applications* 1.1 (2010): 7-18

[2] Pearson, Siani. "Taking account of privacy when designing cloud computing services." *Software Engineering Challenges of Cloud Computing, 2009. CLOUD'09. ICSE Workshop on*. IEEE, 2009.

[3] Jansen, Wayne, and Timothy Grance. "Guidelines on security and privacy in public cloud computing." *NIST Special Publication* (2011): 800-144.

[4] Wang, Jian, et al. "Providing privacy preserving in cloud computing." *Test and Measurement, 2009. ICTM'09. International Conference on*. Vol. 2. IEEE, 2009.
[5] Fahl ,Sascha ,et al" .Confidentiality as a Service--Usable Security for the Cloud ". Trust ,Security and Privacy in Computing and Communications(TrustCom ,)2102 IEEE00 th International Conference on .IEEE , 2102 .
[6] Victor Delgado ".Exploring the limits of cloud computing ". Master's Thesis , 2101 .
[7] Moritz Borgmann, Tobias Hahn, Michael Herfert ,Thomas Kunz,Marcel Richter, Ursula Viebeg ,Sven Vowe " .On the Security of Cloud Storage Services ".SIT Technical Reports, 2102.
[8] http//:aws.amazon.com/s3/#protecting [Accessed on: March 2013].
[9] Zhang ,Gaofeng ,et al" .Key Research Issues for Privacy Protection and Preservation in Cloud Computing ".Cloud and Green Computing (CGC ,)2102 Second International Conference on .IEEE , 2102 .
[10] Almorsy ,Mohamed ,John Grundy ,and Ingo Müller" .An analysis of the cloud computing security problem." the proc. of the 2010 Asia Pacific Cloud Workshop ,Colocated with APSEC2010, Australia. 2010.
[11] Zhou ,Minqi ,et al" .Security and privacy in cloud computing :A survey".Semantics Knowledge and Grid(SKG ,)2101 Sixth International Conference on .IEEE , 2101 .
[12] Takabi ,Hassan ,James BD Joshi ,and Gail-Joon Ahn" .Security and privacy challenges in cloud computing environments ".Security & Privacy ,IEEE 8.6 (2101:)22 -10 .
[13] Mather, Tim ,Subra Kumaraswamy ,and Shahed Latif .Cloud security and privacy :an enterprise perspective on risks and compliance .O'Reilly Media ,Incorporated. 2112
[14] Cloud Security Alliance" ,Security Guidance for Critical Areas of Focus in Cloud Computing V3 ," 2100 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf [Accessed on: January 2013].
[15] Cloud Security Alliance, "Domain 12 Guidance for Identity & Access Management", 2010 https://cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf .[accessed on: March 2013.]
[16] Shen ,Yun ,and Siani Pearson" .Privacy Enhancing Technologies: A Review." HP Laboratories 2011.
[17] Pearson, Siani, Yun Shen, and Miranda Mowbray. "A privacy manager for cloud computing." *Cloud Computing* (2009): 90-106.
[18] Itani ,Wassim ,Ayman Kayssi ,and Ali Chehab" .Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures".Dependable ,Autonomic and Secure Computing , 2112 .DASC'09 .Eighth IEEE International Conference on .IEEE, 2009.
[19] Chadwick, David W., and Kaniz Fatema. "A privacy-preserving authorisation system for the cloud." Journal of Computer and System Sciences 78.5 (2012): 1359-1373.
[20] Kamara ,Seny ,and Kristin Lauter" .Cryptographic cloud storage ".Financial Cryptography and Data Security, 2010.
[21] Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010.
[22] Liu, Qin, Chiu C. Tan, Jie Wu, and Guojun Wang. "Reliable re-encryption in unreliable clouds." In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, pp. 1-5. IEEE, 2011
[23] Liu, Qin, Guojun Wang, and Jie Wu. "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment." Information Sciences (2012).
[24] Blaze, Matt, Gerrit Bleumer, and Martin Strauss. "Divertible protocols and atomic proxy cryptography." *Advances in Cryptology—EUROCRYPT'98* (1998): 127-144