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 9, September 2017

Revocation Methodologies Using Cloud Security

D. Deepika, Dr. Antony Selvadoss Thanamani

Research Scholar, Department of Computer Science, NGM College, Pollachi, India

Associate Professor and Head, Department of Computer Science, NGM College, Pollachi, India

ABSTRACT: The data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part o shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this article, we study about a novel public auditing mechanism for the integrity of shared data with efficient user revocation in cloud. This minimizes the computation cost and increase the reliability by means of proxy re-signature scheme**.** This mechanism is based on improved security. we also study about Attribute Based Encryption and access control using security. This method has a data confidentiality then forward and backward security process. This article shows some methodologies about cloud security.

KEYWORDS: Cloud Security, Revocable ABE, Public Auditing, Key Signature.

I.INTRODUCTION

Security and privacy represent major concerns in the adoption of cloud technologies for data storage. An approach to mitigate these concerns is the use of encryption. However, whereas encryption assures the confidentiality of the data against the cloud, the use of conventional encryption approaches is not sufficient to support the enforcement of fine-grained organizational Access control policies (ACPs). [1] Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using Access Control languages such as XACML. [1] Such an approach, referred to as Attribute-based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting Attribute based access control (ABAC) over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should thus is strongly protected from the cloud, very much as the data themselves. [2] Approaches based on encryption have been proposed for fine-grained access control over encrypted data. As shown in Figure 1, those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items [2]. Such approaches however have several limitations.

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 9, September 2017

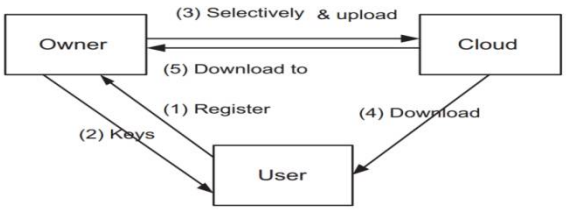

Fig.1. Public Auditing For Shared Data

II.IN HEALTH ORGANIZATION

A number of works used ABE to realize fine-grained access control for outsourced data. Especially, there has been an increasing interest in applying ABE to secure Electronic healthcare records (EHRs).[3] Recently, a proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In, a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs [4]. Applied Cipher Text Policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains. In investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline [6].

III. REVOCABLE ABE

It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally, this is often done by the authority broadcasting periodic key updates to unrevoked users frequently, which does not achieve complete backward/forward security and is less efficient. Recently, and proposed two CP-ABE schemes with immediate attribute revocation capability, instead of periodical revocation. However, they were not designed for Mulity authority (MA-ABE). In addition, another one has proposed an alternative solution for the same problem in our paper using Lewko and Waters's (LW) decentralized ABE scheme. The main advantage of their solution is, each user can obtain secret keys from any subset of the TAs in the system, in contrast to the CC MA-ABE. The LW ABE scheme enjoys better policy expressiveness, and it is extended by to support user revocation. On the downside, the communication overhead of key revocation is still high, as it requires a data owner to transmit an updated cipher text component to every non revoked user. They also do not differentiate personal and public domains. In this article, we bridge the above gaps by proposing a unified security framework for patient-centric sharing of PHRs in a multi domain, multi authority system with many users. The framework captures application-level requirements of both public and users details, and distributes users trust to multiple authorities that better reflects reality. We also propose a suite of access control mechanisms by uniquely combining the technical strengths of both CC MA-ABE and the YWRL ABE scheme. Using our scheme, patients can choose and enforce their own access policy for each PHR file, and can revoke a user without involving high overhead. We also implement part of our solution in a prototype system.In light of the above observations, it is very important that logging be provided in a secure manner and that the log records are adequately protected for a predetermined amount of time (maybe even indefinitely). Traditional logging proto-cols that are based on sys log have not been designed with such security features in mind. Security extensions that have been proposed, such as reliable delivery of sys log, forward integrity for audit logs, sys log-ng, and sys log-sign, often provide either partial protection, or do not protect the log records from end point attacks. In addition, log management requires substantial storage and processing capabilities. The log service must be able to store data in an organized manner and provide a fast and useful retrieval facility. Last, but not least, log records may often need to be made available to outside auditors who are not related to the organization.

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 9, September 2017

IV. RELIABILITY OF PUBLIC AUDITING

In our mechanism, it is very important for the cloud to securely store and manage the re-signing keys of the group, so that the cloud can correctly and successfully convert signatures from a revoked user to an existing user when it is necessary. However, due to the existence of internal attacks, simply storing these re-signing keys in the cloud with a single re-signing proxy may some-times allow inside attackers to disclose these re-signing keys and arbitrarily convert signatures on shared data, even no user is revoking from the group.

Eq. (1)

$$\begin{aligned}\prod_{l=1}^{t} {\sigma'_{k,l}}^{F_{j,l}(0)} &= \prod_{l=1}^{t} (H(id_k)w^{m_k})^{y_{j,l}F_{j,l}(0)} \\ &= (H(id_k)w^{m_k})^{\sum_{l=1}^{t} y_{j,l}F_{j,l}(0)} \\ &= (H(id_k)w^{m_k})^{f_j(0)} \\ &= (H(id_k)w^{m_k})^{\pi_j} = \sigma'_k.\end{aligned}$$

Obviously, the arbitrary misuse of re-signing keys will change the ownership of corresponding blocks in shared data without users' permission, and affect the integrity of shared data in the cloud. To prevent the arbitrary use of re-signing keys and enhance the reliability of our mechanism, we propose an extended version of our mechanism, denoted as Panda, in the multi-proxy model.By leveraging an(s, t)-Shamir Secret Sharing (s ≥2t−1) and s multiple proxies, each resigning key is divided into spices and each piece is distributed to one proxy. These multiple proxies belong to the same cloud, but store and manage each piece of a resigning key independently (Fig. 2). Since the cloud needs to store keys and data separately, the cloud also has another server to store shared data and corresponding signatures. In Panda, each proxy is able to convert signatures with its own piece, and as long as t or more proxies (the majority) are able to correctly convert signatures when user revocation happens, the cloud can successfully convert signatures from a revoked user to an existing user. Similar multi-proxy model was also recently used in the cloud to secure the privacy of data with re-encryption techniques. Compromised by an inside attacker, it is still not able to reveal a re-signing key or arbitrarily transform signatures on shared data.

V. KEY SIGNATURE

Rekey and re-assigning respectively. We use ∗to distinguish them from the corresponding algorithms in the single proxy model. Details of Algorithm Rekey and Resign are described. The correctness of the recovery and transformation of signature σ "k (i.e., Equation 1)can be explained.One of the most important advantages of batch auditing is that it is able to reduce the total number of pairing operations, which are the most time consuming operations during verification. According to Equation, batch auditing can reduce the total number of pairing operations for t auditingTasks totd+1, while verifying these t auditing tasks independently requires td +t pairing operations. Moreover, if all the t auditing tasks are all from the same group, where the size of the group is d and all the existing users' public keys for the group are(pk 1,...,pk d),then batch auditing on t auditing tasks can be further optimized.

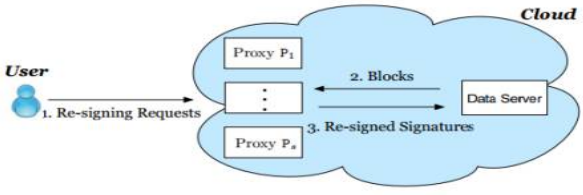

Fig.2. Re-signed Signature

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 9, September 2017

VI. COMPARISON

Global Data Vault provides three strategies for protecting data and systems. This chart will give you a high-level overview of the Data Protection Solution that is right for you – and offers links to further details and comparisons related to each option.

	Cloud Revocation	Cloud Backup	Cloud Archive
Protection	Full server and PC protection including operating systems, applications and data. Protection both locally and in the cloud.	Cloud based complete data protection.	Cloud and local data protection for large volumes of important but no longer critical data.
Recovery Options	Restore files, folders, or entire systems locally or in the cloud.	Restore files, folders, or entire databases.	Restore files, folders, or entire data sets.
Restore Time	Local restores down to one hour. Cloud restores down in each second	Dependent on connection speed.	Dependent on connection speed.
Restore Points	Restore points down to every 15 minutes.	Supports retention schedules including daily, weekly, monthly, annual, etc.	Most recent copies only.
Management	Fully managed solution including portal based view with SLA monitoring.	Fully managed solution including portal based view.	Fully managed solution including portal based view
Cost	Low cost.	Competitive and affordable.	High Cost

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 9, September 2017

VII. GLIMPSE OF LITERATURE

S.NO	Authors	Title	Year	Advantages	Disadvantages
1	B. Wang, B. Li, and H. Li,	Public Auditing for Shared Data with Efficient User Revocation in the Cloud	2015, pp.2904–2912.	1.Public audit ability 2.Storage accuracy	1.they may be potential reveal user data information to the auditors
2	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,"Communications of the ACM	2014, pp. 06-09.	1.drive down costs 2.improved security and compliance	1.downtime 2.security privacy 3.vulnerability to attack
3	Shashikumar, PuneethHegde,SiddarthGopinath, Zabiulla, Mrs.Sridevi, K N	Secure Data Sharing in Cloud computing Using Revocable data Using CP-ABE Techniques	2017,pp.2349-7009.	1.Data confidentiality 2.backward security 3.forward security	-
4	Kanya Devi	Efficient user Revocation for dynamic groups in the cloud	2014, pp.3938-3942.	1.access control 2.traceability	Require a public key infrastructure
5	YogeshBelekar, MadhukarVerma, PappuTormal	Efficient user Revocation in Cloud Using Proxy Server	2015,pp.2348-4853.	1.reduce costs 2.increasing flexibility 3.scalability	-
6	TejaswiniJaybhaye, Prog.D.H.Kulkari	Secure cloud Auditor for Efficient Data De-duplication with maintain shared data Integrity	2016 pp.3297:2007.	1.integrity auditing 2.cost effective 3.protection	-
7	MalaneelamBhaskar, G.Umadevi	Public Auditing for Shared Data with efficient user revocation	2015, pp.0976-1353.	1.identity privacy 2.support for large group 3.recovery options	-
8	Prof. Autade P.P, Prof.Gaikar M.R, Prof. Kharinar N.K	A Survey on Public Auditing For Shared data with efficient user revocation in the cloud	2016,pp.3297:2007	1.correctness 2.restore time 3.restore points	-

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 9, September 2017

VIII. CONCLUSION

In this article, survey has been done for a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.This article also study about Attribute based encryption and access control using security. Cloud revocation has a low cost and they have a recovery Option.

REFERENCES

1.B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2015,2015,pp. 2904–2912.
2. 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,"Communications of the ACM, 2014,pp. 06-09.
3.Shashikumar, PuneethHegde,SiddarthGopinath, Zabiulla,Mrs.Sridevi, K N,"Secure Data Sharing in Cloud computing Using Revocable data Using CP-ABE Techniques," Issue 05, Volume 04(May 2017)
4.Kanya Devi "Efficient user Revocation for dynamic groups in the cloud ," 2014, pp.3938-3942.
5. YogeshBelekar, MadhukarVerma, PappuTormal, "Efficient user Revocation in Cloud Using Proxy Server ," inthe 2015,pp.2348-4853.
6.TejaswiniJaybhaye, Prog.D.H.Kulkari, "Secure cloud Auditor for Efficient Data De-duplication with maintain shared data Integrity," inthe 2016 pp. 3297:2007.
7. MalaneelamBhaskar, G.Umadevi, "Public Auditing for Shared Data with efficient user revocation," in the 2015,pp.0976-1353.
8.Prof. Autade P.P,Prof.Gaikar M.R,Prof.Kharinar N.K., "A Survey on Public Auditing For Shared data with efficient user revocation in the cloud ," inthe 2016,pp.3297:2007
9.B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography, 2011, pp. 53–70.
10. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. EUROCRYPT, 2010, pp. 62–91.