Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study on Privacy and Security Methodologies in Cloud Storage

Nimi P Baby, Dr Salaja Silas
Department of Information Technology
Karunya University, India

Abstract – Cloud computing is an emerging environment where many advantages like ease of use and economical benefits are provided to the users. Where as the main issue is privacy and the security of the data stored .Even though cloud computing is providing many advantages, it cannot be used in many applications where privacy is an important concern. In this paper different methodologies that provide security and privacy are studied and compared based on the need for the cloud computing environment.

Keywords - Attribute Based Encryption, Privacy, Key distribution, PRE encryption

I. INTRODUCTION

At present various organizations are using cloud computing services. It is mainly because of the advantages such as cloud allows the users to access the contents and applications as that in the internet from anywhere any time in the cost effective manner and provides availability scalability and reliability. Cloud computing got this much attention because it helps to share all the resources as service so that this becomes more economical. Major cloud computing services are listed as software as a service, platform as a service, infrastructure as a service and anything as a service includes security, storage etc. On demand self service is another attracting property of cloud computing. Main deployment models in cloud are public cloud private cloud and hybrid cloud. Cloud computing faces many challenges such as security vulnerabilities, portability issues etc. The main research challenges are lack of security and privacy while using cloud computing services. [1].

Any cloud storage system must ensure that user's data must be always secure and it cannot be modified by unauthorized users and the data stored while accessing by the user must always at the latest versions. To ensure the security cryptographic methods are widely used. The data contents are encrypted before storing in the cloud system and then the key is made secured. While the user wanted to retrieve the data contents the user decrypts the cipher text with the encryption key. Only the users possessing the accurate matching key can decrypt and retrieve the contents.[9,12]

In this paper we have performed an extensive study on the various current researches being done to solve these issue related to the security and privacy of the contents stored in cloud storage system. The rest of the paper is organized as follows. In section 2 different methodologies are studied highlighting advantages and disadvantages within each of them. section 3 contains the conclusion of the paper.

II. STUDY ON CLOUD STORAGE SECURITY SCHEMES

A. *Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing[1]*

Yu S,Wang C, Ren K, LouW has proposed a methodology that helps the data owner to achieve fine-grained access control on files stored in Cloud Servers. This method supports user accountability it enables the data owner to delegate most of computation intensive tasks to cloud servers without disclosing data contents. The methodology combines three advanced cryptographic techniques such as KP-ABE, PRE and lazy re-encryption [1]. Here any data file is associate with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. A PRE scheme allows the proxy, given the proxy re-encryption key, to translate ciphertexts under one public key into ciphertexts under another public key and vice versa.

Main advantages in the method are the data owner can not only store data files but also run his own code on Cloud Servers to manage his data files. And achieve security goals like user accountability and support basic operations such as user grant/revocation. Disadvantage is that the Cloud Servers will try to find out as much secret information as possible based on their inputs.

B. *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data [8]*

] Goyal V, Pandey O, Sahai A,Waters B propose a new cryptosystem for fine-grained sharing of encrypted data that called Key-Policy Attribute-Based Encryption (KP-ABE)[2]. This scheme uses a set of attributes to describe the encrypted data and builds a access policy in user's private key. If attributes of the encrypted data can satisfy the access structure in user's private key, then the user can obtain the message through decrypt algorithm. In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy which is also called the access structure, that specifies which type of cipher texts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents.

This method helps to share stored data in the fine grained level. The limitation in KP-ABE system is that encryptors are not allowed to create the access policies and its dependency on the access control mechanism. On each user revocation, a new access policy is defined, which lead to a situation where it is not possible to construct further more access structure.

C. *Sirius: Securing Remote Untrusted Storage*

Design a security mechanism that improves the security of a networked file system without making any changes to the file system. SiRiUS[7] is layered over existing file systems such as NFS to provides end-to-end security. To achieve the access control, SiRiUS attaches each file with a meta data file which contains that file's access control list (ACL), containing each entry of which is the encryption of the file's file encryption key (FEK) using the public key of an authorized user. SiRiUS appears as a local file system with the standard hierarchical view of files and directories.

SiRiUS is defends against version rollback attacks and it reduce network traffic by providing random access within files. It supports granting read only or read-write access to files.

Disadvantages are

- Scalability: collaboration among bigger groups SiRiUS proves to be inefficient. Whenever, user is revoked, FEK and FSK are updated and new keys are encrypted with public key of the individual user, making it for dynamic user sets. Reads and writes to any location in a file should take comparable amounts of time.
- Key Management. The rapid increase of keys used by different applications creates a management and usability nightmare.

D. *Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records[5]*

Build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records. A centralized storage system with hierarchies was developed for sharing the PHR. Iis not possible to completely believe a certificate authority(CA) for managing the storage which guides to key escrow problem. To treat this problem, users in the system are classified as personal and public domains. Personal domain manages the personal information of the patient which is accessible by the data owner. Public domain comprises different types of information. An authority is assigned to each type of information. PHR uses ABE.[5]

Thus, personal domain is controlled by the Data Owner which uses KP-ABE and the public domain is controlled by multiple attribute authorities which use Multiple Authority - Attribute Based Encryption (MAABE). The attribute authority is responsible for granting and revoking access to the users. The attributes present in the cipher-text are modified to update the access policies. This method is approachable because the patient can easily grant access to a category, without knowing all the types included in it. Doctors can add subcategories with arbitrary names. Limitation of its hierarchy is like there is only one way to partition the record.

E. *Tcloud: A Multi – Factor Access Control Framework for Cloud Computing*

Framework of access control for cloud computing is introduced in this paper, which provides a multi - step and multifactor authentication of a user. [3]

The model proposed is well-organized and provably secure solution of access control for externally hosted applications. The authentication of the user is a multistep process, and after the successful authentication the user will only access the data file store by the owner, in a confidential manner by the implementation of the digital certificate. Advantages is that it Increase the confidentiality and integrity of the data using biometric data disadvantages are there associated with Key management Complexity and difficulty in revocation.

F. *Key Regression[4]*

Kevin Fu. U. Mass. Amherst. Seny Kamara introduces an efficient key distribution for Secure Distributed Storage and solves the limitations of key rotation. Here member states are given to the authorized users. Using key derivation function encryption key is generated for that particular member state. Encryption keys are separated from the member state so that the key is pseudorandom for any particular member state[4]. Lazy revocation method is used here which postpones the re-encryptions til the next write access is performed so that the extra re-encryptions are eliminated[13]

This method Significantly reduce the bandwidth requirements of a content publisher and reduces lack of pseudo randomness in key rotationThe main disadvantage is that after certain number of revocations Key derivation function will not be able to generate the new member states, thus reducing its practicability to a limited number of revocations.

G. *Crust: Cryptographic Remote Untrusted Storage Without Public Keys*

Geron E, Wool A propose a cryptographic remote storage system, which avoids the use of public key encryption for the purpose of speed and efficiency in cryptographic operations. Here for each new user, trusted agent generates an encryption key by using system master key stored locally on it. CRUST[6] maintains file in blocks each encrypted with a separate key. The major advantage of this method is that, Only the updated block of a file is re-encrypted to avoid unnecessary cryptographic operations. But it Uses trusted agent, thus making it highly dependent on the trusted third party. And it suffers from key management problem that is Separate encryption key for each block of a file increases key management burden on each user as well as on the trusted agent.

H. *K2C: Cryptographic Cloud Storage with Lazy Revocation and Anonymous Access*

Saman Zarandioon1, Danfeng (Daphne) Yao2, and Vinod Ganapathy presents a user-centric privacy preserving cryptographic access control protocol called K2C (Key To Cloud)[2] that enables end-users to securely store, share, and manage their sensitive data in an untrusted cloud storage anonymously. K2C is realized through our new cryptographic key-updating scheme, referred to as AB-HKU.

K2C is scalable and supports the lazy revocation. and it avoids trusted third party . But it requires guaranteed availability of the data owner until all of the legitimate users update their keys.

I. SAPDS: Self-Healing Attribute-Based Privacy Aware Data Sharing in Cloud

This method helps to achieve fine-grained access control to the outsourced data contents in the cloud. Key distribution and management process is done here without out analysing any confidential information about the secure data contents[1].so that it provides more privacy to the data contents stored. User revocation is achieved by changing one attribute associated with the key , here there is no need to modify the entire access control policy and this enables authorized users to update their decryption keys during each user revocation. These are made possible by combining ciphertext policy attribute based encryption[11] pre encryption and key distribution methods.

In this case the main advantage is that the owner should not remain always online to distribute new decryption key among the legitimate users and the legitimate users are allowed to update their secret key after each user revocation without interacting with the owner. Cloud server should not be able to learn any information about the contents of the outsourced data. Desired symmetric encryption methods can be used along in this method. But there is need for a secure channel to transfer the private key between the owner and the user.

The table below compares different methodologies for security in cloud storage based on the parameters revocation method used, complexity, scalability, need for third party, granularity and bandwidth.

TABLE 1
COMPARISON OF SECURITY MECHANISMS

METHOD	**REVOCATION**	**COMPLEXITY**	**SCALABILITY**	**THIRD PARTY**	**GRANULARITY**	**BANDWIDTH**
SiRiUs[7]	Simple	Less	Less	No	Coarse	Less
KEY REGRESSION[4]	Lazy	High	Less	No	Fine	Less
K2C[2]	Lazy	High	High	Yes	Fine	High
CRUST[6]	Lazy	No of user	High	Yes	Coarse	Less
PHR[5]	Hierarchical	No of user	Less	No	Fine	High
SECURE SCALABLE[9]	Re-encryption	No of user	High	Yes	Fine	High
KP-ABE[8]	Lazy	High	Less	No	Fine	High
SAPDS[1]	Proxy	Less	High	No	Fine	Less

III. CONCLUSION

One of the major issues in cloud computing is privacy and security of data. This paper survey on different mechanisms used to provide security and privacy for the data in cloud storage system. Cryptographic methods are widely used for security and along with that biometric and many other solutions are referred. The study and comparison of some methods based on the parameters such as revocation method,bandwidth,granularity, need for third party etc is done in this paper and listed with advantages and limitations of each of them.

REFERENCES

[1] Zeeshan Pervez, · Asad, Masood Khattak, · Sungyoung, Young-Koo Lee, · A M Khattak, · S Y Lee, · Y K Lee SAPDS: self-healing attribute-based privacy aware data sharing 2012. Yu S,Wang C, Ren K, LouW(2010) *, Issue 1, pp 431-460*

[2] Saman Zarandioon1, Danfeng (Daphne) Yao2, and Vinod Ganapathy K2C: Cryptographic Cloud Storage With Lazy Revocation Anonymous Access. *96, 2012, pp 59-76*

[3] Sultan Ullah, Zheng Xuefeng and Zhou Feng TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing. International Journal of Security & Its Applications;Mar2013, Vol. 7 Issue 2, p15

[4] Kevin Fu. U. Mass. Amherst. Seny Kamara. Johns Hopkins University.Key Regression: Enabling Efficient Key Distribution for Secure Distribute Storage.2005

[5] Benaloh J, Chase M, Horvitz E, Lauter K (2009) Patient controlled encryption: ensuring privacy of electronic medical records. In: Proceedings of the 2009 ACM workshop on cloud computing security, CCSW ’09. ACM, New York, pp 103–114

[6] Geron E, Wool A (2009) Crust: cryptographic remote untrusted storage without public keys. Int J Inf Secur 8:357–377

[7] Goh E-J, Shacham H, Modadugu N, Boneh D (2006) Sirius: Securing remote untrusted storage. In: Proceedings of the fifth workshop on the economics of information security (WEIS 2006)

[8] Goyal V, Pandey O, Sahai A,Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on computer and communications security, CCS ’06. ACM, New York, pp 89–98

[9] Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings of the 29th conference on information communications, INFOCOM’ 10. IEEE Press, Piscataway, pp 534–542

[10] Natarajan Meghanathan, Privacy In Cloud Computing: A Survey Sipm, Fcst, Itca, Wse, Acsit, Cs & It 06, Pp. 321–330, 2012.© Cs & It-Cscp 2012.

[11] John Bethencourt Carnegie Mellon University “Ciphertext-Policy Attribute-Based Encryption” *Security and Privacy, 2007. SP '07. IEEE Symposium 20-23 May 2007 321 - 334*

[12] Michael Armbrust, Armando Fox, Rean Griffith,Anthony D. Joseph, Randy Katz, Andy Konwinski,Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica,and Matei Zaharia “a view of cloud computing”

[13] Backes M, Oprea A “ Lazy revocation in cryptographic file systems. In: Proceedings of the third IEEE international security in storage workshop. IEEE Computer Society, Washington,2005 DC, pp 1–11