www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2, February 2014 Page No. 3924-3928

A Review of Various Trust Management Models for Cloud Computing Storage Systems

Mr. Anup R. Nimje[1], Prof. V.T.Gaikwad[2], Prof. H.N.Datir[3]

[1] M.E. Student, Computer Engineering
Sipna College Of Engineering and Technology, Amravati, India
anup.nimje@yahoo.com

[2]Associate Professor and Head , Information Technology
Sipna College Of Engineering and Technology, Amravati, India
vtgaikwad@rediffmaiI.com

[3]Assistant Professor, Computer Science and Engineering
Sipna College Of Engineering and Technology, Amravati, India
h_datir@rediffmail.com

Abstract: ***Computing has been widely used for data storage and computational purposes. When we discuss about the cloud storage services, the data must be outsourced, so, there may be serious concerns about the authorization and trust management for the cloud service provider (CSP). These concerns are about confidentiality, integrity and access control. In this paper we are going to discuss various models in brief such as Provable data possession (PDP), Proof of retrievability (POR), HAIL, Attribute Based Encryption Scheme, Plutus, SiRiUS, Third party auditor (TPA) etc that are introduced for addressing such issues about cloud storage systems. Also the mutual trust model given by Ayad Barsoum et al. This scheme supports dynamic data and trust in the cloud computing storage systems.***

Keywords: cloud storage, dynamic data, third party auditor, attribute based encryption, mutual trust model, broadcast encryption**.**

1. Introduction

While dealing with the cloud computing at corporate level, the confidential and expensive data is transmitted over the cloud systems to perform computational tasks. Managing such huge amount of data at local level is quite difficult and costly, because of requirements of high storage capacity and qualified personnel. Therefore, in modified cloud systems, the storage is offered by cloud service providers (CSPs) emerged as a solution to reduce the burden of large local data storage and maintenance cost by means of outsourcing data storage [1]-[2]. This can be called as Storage-as-a-Service. Because of the data owner physically releases sensitive data to a remote CSP, there may be some concerns regarding confidentiality, integrity, and access control of the data. Consider confidentiality, this feature can be provided by the owner by encrypting the data before outsourcing to remote servers. To verify the data integrity over cloud servers, provable data possession technique has been proposed. This validates the intactness of data stored on remote sites.[3]

2. Literature review

In traditional access control techniques it is assumed that the data exists that is of the data owner and the storage servers in the same trust domain. [4] But when the data is outsourced to a remote CSP, This assumption, however, no longer holds. [10]. It resides outside the trust domain of the data owner by taking the full access of the outsourced data management. The solution provided for it is to enable the owner to enforce access control of the data stored on a remote un-trusted CSP [7]. In this process, the data is encrypted by using a certain key, which is shared only with the authorized users. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. These approaches can prevent and detect malicious actions from the CSP side. On the other hand, the CSP needs to be safeguarded from a dishonest owner. And for verifying data integrity over cloud servers, there is provable data possession technique to validate the intactness of data stored on remote sites. A number of PDP protocols have been presented to efficiently validate the data integrity. [5]. The few models for cloud computing storage system with trust management point of view are discussed below.

3. Various schemes for trust management or trust enforcement in cloud computing storage system

3.1 Provable data possession (PDP)

A model for provable data possession (PDP) [4] that allows a client that has stored data at an un-trusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server. It reduces I/O costs. The client maintains a constant amount of metadata to verify the

proof. The response protocol transmits a small, constant amount of data, which reduces network traffic. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system.
The networking technology being advanced, is applied to the solution of computational problems, distributed computation as well. The model provided the data possession and authorized data transfer over the network. [6]

3.2 Proof of retrievability (POR), HAIL

It was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers. [7]

HAIL (High-Availability and Integrity Layer) [5] is a distributed cryptographic system. It guarantees the client that a stored file is intact and retrievable. It also improves approaches to the cryptographic and distributed-systems. Proofs in HAIL are efficiently computable by servers and highly compact. HAIL cryptographically verifies and reactively reallocates file shares. HAIL is robust and improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers.

In a proof-of-retrievability system, a data storage center provides that it is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any prover that passes a verification check. In this model, it gives the proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski [10].
In this scheme built from BLS signatures and secure in the random oracle model, has the shortest query and response of any proof-of-retrievability with public verifiability. In their second scheme, which involves pseudorandom functions (PRFs). It is secure in the standard model, has the shortest response of any proof-of-retrievability scheme with private verifiability.

3.3 Attribute Based Encryption

There are another solutions those utilize attribute-based encryption to achieve fine-grained access control [11].

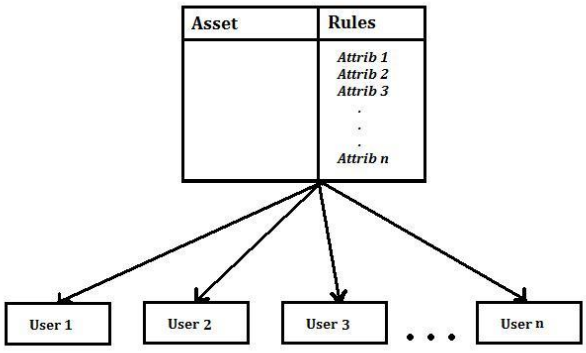

Figure 1 : Attribute Based Encryption scheme for data storage in cloud systems

In traditional system, user and server are assumed to be in a trusted domain. But what if their domains are not trusted or not same? So, the 'Attribute Based Encryption (ABE)' scheme was introduced.

In ABE scheme the user's secret key and the ciphertext are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a specified number of attributes overlap between the cipher-text and user's secret key. Attribute-Based Encryption (ABE) in which policies are specified and enforced in the encryption algorithm itself. As compared with traditional system, it provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered.

There are different approaches that have been clarified that encourage the owner to outsource the data, and offer some sort of guarantee related to the confidentiality, integrity, and access control of the outsourced data. Using these approach, malicious actions from the CSP side can be prevented as well as detected. Also, CSP needs to be protected from a dishonest owner, that can attempt to get illegal access and that can corrupt the data over cloud servers. and CSP can to go out of business.

3.4 Plutus:

It is a storage system, consisting cryptography by which file sharing without placing much trust on the file servers is carried out. Particularly, it makes good use of cryptographic primitives to protect and share files. Highly scalable key management is provided while allowing individual users to retain direct control over who gets access to their files. In Plutus, the number of cryptographic keys are reduced, that exchanged between users by using file-groups, file read and write (R/W) access. It also deals with handling user revocation efficiently, and allowing an untrusted server to authorize file writes.

A prototype of Plutus on OpenAFS has been built [12] that Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

3.5 SiRiUS:

A secure file system designed to be layered over insecure network and P2P file systems.[13]

It consists of network storage which is untrusted and provides its own read-write cryptographic access control for file level sharing. The mechanism of Key management and revocation is simple with minimal out-of-band communication. File systems are supported by SiRiUS using hash tree constructions. SiRiUS contains a method of performing file random access in a cryptographic file system without the use of a block server. When extensions is provided to SiRiUS that include large scale group sharing using the NNL key revocation construction. SiRiUS performs well relative to the file system despite using cryptographic operations.

Data outsourcing is allowing users and organizations to exploit external services for the distribution of resources. There is a crucial problem to be addressed in this context that the enforcement of selective authorization policies and updates in dynamic scenarios. A solution to the enforcement of access control and the management of its evolution is provided bt []. The authorization is implemented by selective encryption scheme.

Two layers of encryption are imposed on data: Inner layer is imposed by the owner for providing initial protection, Outer layer is imposed by the server to reflect policy modifications. The combination of the two layers provides an efficient and robust solution. An algorithm for managing the two layers, and an analysis is provided in the research.

3.6 Storage Service Provider:

The outsourcing their storage to a storage service provider (SSP) [14] by storing data at a remote SSP-managed site and accessing it over a high speed network. There are various concerns for a variety of reasons, it is unacceptable to fully trust the SSP at enterprise level and prefer to store data in an encrypted form.

3.7 Third Party Auditor:

There is also solution provided by introducing third party auditor (TPA), into the cloud system[3]. That is on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The TPA replaces the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be commercially important Cloud Computing.

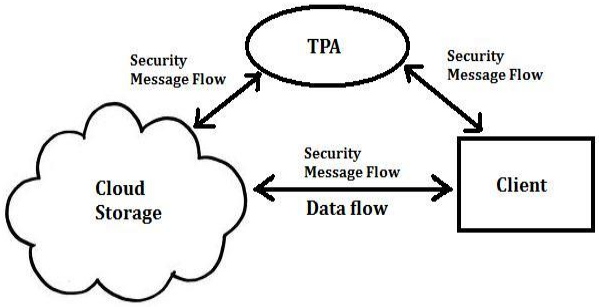

Figure 2 : Third party auditor model for data storage in cloud

The data operations such as block modification, insertion and deletion, is also a significant. The public verifiability and dynamic data operations are provided in this model of TPA. The proof of retrievability model is modified by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. The Extensive security and performance is proposed in TPA model and provably secure.

3.8 Hashing and Digital Certificates:

The digital signature scheme using self-certified public keys. It has provided the message recovery property. This scheme only allows a specified receiver to verify and recover the message with authenticated encryption. For transmission of large message or blocks, while providing the linkages among signature blocks, this scheme is suitable. [15] It described browser security in the Cloud computing context. It described the threat of flooding attacks on Cloud systems. Cloud Computing security concerns and analysis on their potential impact and relevance to real-world scenarios. [16]

4. Mutual Trust Model for Cloud Storage System

4.1 An overview of mutual trust Model:

In this model given by *Ayad Barsoum et al*, a scheme is proposed that provides solutions to the important issues and concerns related to outsourcing the storage of data, namely dynamic data, newness, mutual trust, and access control. [17] Data is stored remotely and that is accessed by authorized users. Also the data is updated, scaled and monitored by the owner. After updating, authorized users should receive the latest version of the data that is newness property.

The Mutual trust between the data owner and the CSP is another issue and that is addressed in this scheme. A mechanism is introduced to determine the dishonest party, from any side is detected and the responsible party is identified. Access control is also provided by the model which allows the owner to grant access or to revoke access rights to the outsourced data. In the existing schemes discussed, access control techniques assume the existence of the data owner and the storage servers in the same trust domain. Such system, no longer holds when the data is outsourced to a remote CSP. This scheme addresses important issues related to outsourcing the storage of data over the cloud storage systems. Especially these issues dynamic data, newness, mutual trust, and access control are addressed by this scheme. The cloud computing storage model considered in this scheme as shown in figure given by *Ayad Barsoum et al*.

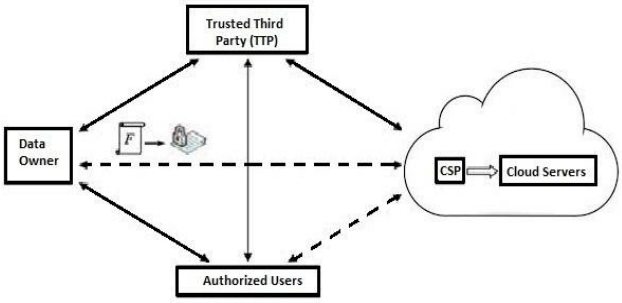

Figure 3 : Mutual trust model for cloud computing storage

The cloud computing storage model consists of four main components as shown in Fig. 1. Given by *Ayad Barsoum et al* [17] :

(i) A data owner (an individual or an organization) generating sensitive data to be stored in the cloud and made available for controlled external use;

(ii) A CSP manages the cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users;

(iii) Authorized users, a set of owner's clients who have the right to access the remote data; and

(iv) A trusted third party (TTP), This TTP is trusted by all other system components. It detects and specifies dishonest parties.

4.2 Algorithm used:

In this scheme, the data owner enforces access control for the outsourced data by combining three cryptographic techniques:, lazy revocation [18], and key rotation.[12][19] , broadcast encryption[20]. These can be given as below:

(i) Lazy Revocation

The lazy revocation technique was introduced [18]. In Lazy revocation allows revoked users to read unchanged data blocks. In other words, the lazy revocation is equivalent to accessing the blocks from cashed copies. Updated or new

blocks following a revocation are encrypted under new keys. Lazy revocation does re-encryption and data access cost depending upon a degree of security. However, it causes encryption keys fragmentation. The data blocks should have more than one key. Lazy revocation has been implemented into many cryptographic systems.

(ii) Key Rotation

In Key rotation,[12] [19] is a technique in which there is an initial key and a master secret key. A sequence of keys is generated from these keys.

The sequence of keys has two main properties:

(i) only the owner of the master secret key is able to generate the next key in the sequence from the current key, and

(ii) any authorized user knowing a key in the sequence is able to generate all previous versions of that key.

Given the i-th key Ki in the sequence, it is computationally infeasible to compute keys {Kl} for l > i without having the master secret key.

This scheme utilizes the key rotation technique [12], in which the authorized users can access both updated (new) blocks and unmodified blocks that are encrypted under older versions of the current key.

(iii) Broadcast Encryption

Broadcast encryption (bENC) [20] allows a broadcaster/data owner to encrypt a message for an arbitrary subset of a group of users. The proposed scheme uses bENC to enforce access control in outsourced data. The bENC is composed of three algorithms: SETUP, ENCRYPT, and DECRYPT.

(a) SETUP:

This algorithm takes system users n as input. It defines a bilinear group G of prime order p with a generator g, a cyclic multiplicative group GT , and a bilinear map ê : G×G →GT. The algorithm picks a random α∈Zp, computes gi = g(αi)∈G for i = 1, 2,..,n, n + 2 ,.., 2n, and sets v = gγ∈G for γ ∈R Zp.

The outputs of above operations are a public key PK = (g, g1,.., gn, gn+2,.., g2n, v)∈G2n+1, and n private keys {di}1≤i≤n, where di = gγi∈G.

(b) ENCRYPT:

This algorithm takes a subset S ⊆ {1, 2, . . . , n}, and a public key PK as input. And outputs a pair (Hdr, K), where Hdr is called the header (broadcast ciphertext), and K is a encryption key for message.

Hdr = (C0, C1) ∈ G2, where for t ∈R Zp, C0 = gt and C1 = (v · ∏j∈S gn+1−j)t. The key K = ê(g n+1, g) t is used to encrypt a message M (symmetric encryption) to be broadcast to the subset S.

(c) DECRYPT:

This algorithm takes as input a subset S⊆{1, 2,.., n}, a user-ID i ∈ {1, 2,...,n}, the private key di for user i, the header Hdr = (C0, C1), and the public key PK. If i ∈ S, the algorithm outputs the key K = ê(gi, C1)/ê(di · ∏ j∈S, j≠i gn+1−j+i, C0), which can be used to decrypt the encrypted version of M. [23]

Outsourced data validation requires metadata and block indices that provides modifications made by owner and hence newness of data is maintained. There is block status table (BST) in which combined hash values and a small data structure, indicating the status of blocks. The role of the Trusted Third Party is to establish the trust among different components. To enforce access control to the outsourced data, the proposed scheme uses three cryptographic techniques mentioned previously [17].

5. Conclusion

There is outsourcing of data over the cloud service provider. Thus there are serious concerns about the cloud storage systems, so there are various schemes have been introduced . These models are about trust and security for the cloud storage systems. In this paper, we have studied different models for cloud-based storage schemes. And finally model given by *Ayad Barsoum et al* which supports outsourcing of dynamic data. In this scheme, the owner is capable of archiving and accessing the data stored by the CSP and updating and scaling this data on the remote servers. This scheme enables newness of data.

The trusted third party has been introduced in this model which determines whether the storage is honest or not. It detects the party. Also the access control is provided by data owner. They provided the three techniques for cryptography i.e. broadcast encryption, lazy revocation, and key rotation. Thus, these schemes are reviewed. “Equation” markup style. Press the tab key and write the equation number in parentheses.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS ’07, 2007, pp. 598–609.

[2] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, “Efficient remote data possession checking in critical information infrastructures,” *IEEE Trans. on Knowl. And Data Eng.*, vol. 20, no. 8, 2008.

[3] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in *Proceedings of the 14th European Conference on Research in Computer Security*, 2009, pp. 355–370.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” ACM CCS ’07

[5] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” in *CCS ’09: Proceedings of the 16th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2009, pp. 187–198.

[6] D. L. G. Filho and P. S. L. M. Barreto, “Demonstrating data possession and uncheatable data transfer,” IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.

[7] Hovav Shacham and Brent Waters,” Compact Proofs of Retrievability ,” Cryptology ePrint Archive: Report 2008/073

[8] Kevin D. Bowers, Ari Juels, Alina Oprea, ”HAIL: A High-Availability and Integrity Layer for Cloud Storage” Proceedings of the 16th ACM conference on Computer and communications security Pages 187-198

[9] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing” Proceeding ESORICS'09 Proceedings of the 14th European conference on Research in computer security Pages 355-370

[10] A. Juels and B. S. Kaliski, “PORs: Proofs of Retrievability for large files,” in *CCS’07: Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 584–597.

[11] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.” Cryptology ePrint Archive: Report 2006/309

[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable secure file sharing on untrusted storage,” in Proceedings of the FAST 03: File and Storage Technologies, 2003.

[13] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in *Proceedings of the Network and Distributed System Security Symposium, NDSS*, 2003.

[14] A. Singh and L. Liu, "Sharoes: A data sharing platform for outsourced enterprise storage environments," Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference

[15] Digital signature with message recovery Using self-certified public keys and its variantsYuh-Min Tseng, Jinn-Ke Jan, Hung-Yu Chien

[16] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, ―On Technical Security Issues in Cloud Computing‖, 2009 IEEE International Conference on Cloud Computing

[17] Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems Ayad Barsoum and Anwar Hasan , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS-2013

[18] M. Backes, C. Cachin, and A. Oprea, "Secure key-updating for lazy revocation," in 11th European Symposium on Research in Computer Security, 2006, pp. 327–346.

[19] K. E. Fu, "Group sharing and random access in cryptographic storage file systems," Master's thesis, MIT, Tech. Rep., 1999.

[20] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Advances in Cryptology - CRYPTO*, 2005, pp. 258–275.