IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

An Automated Auditing and Verifiability in Cloud's Data Storage

Nisha Innola L X[1], Valarmathi P[2] and Ravi Maran S[3]

[1, 2, 3] **Computer Science & Engineering, M.A.M College of Engineering**
Siruganur, Trichy, Tamil Nadu, India

Abstract

There is a challenge that accompanies every technology being developed and Cloud Computing is not an exceptional prodigious. A real and perceived security threats to Cloud Computing still remain as a major slip to IT giants. One prime obstacle that stands in the way and must be circumvented is the secure data storage in cloud servers i.e. the cloud user (not the end user) does not have a direct control of auditing where their data resides, who has accessed their data & who has had accessed their data at present. Thus an automated Auditing & Verifiability is loosely adopted for cloud secure storage. In this paper, we discuss certain automated auditing Technique from three perspectives via through Cloud Service Provider, or through Third party auditing or directly by Cloud User. This benefits the Cloud User providing them with security assurance within the cloud Data Storage and helps to secure all other forms of Computing.

Keywords- *Cloud Computing, Cloud Auditing, Cloud Assurance, Storage Verifiability, Service Provider, Cloud Security.*

1. INTRODUCTION

The idea of Cloud computing was thrown into the minds of Technologists when they aspired as "Why don't Computing resource be offered as a Service?" .Cloud computing laid its foundation on 'Utility Computing' and 'Grid Computing'. One key Characteristic that makes this cloud service unique is the "Elasticity" and "Pay-Per-Use" basis. Cloud Computing continues to gain more attention as more and more companies move their data into Cloud environment.

Multitenancy -where a single instance of an applications used for many Customers; with each customer able to access their own data. This concept bound with Cloud computing makes the service available from anywhere, anytime for the cloud registered users. Widely deployed Cloud services like Storage, Application software, Hardware platform support for reduced cost & complexity and thus there is a shift from CAPEX (Capital Expenditure) - a tradition way to purchase IT equipments to OPEX (Operational Expenditure) with cost incurred for services making budgeting IT process simpler. Most prime service offered by Cloud technology is SAAS; which support for a huge Business profits.

Once decision is made to move our physically located resources into cloud storage, certain factors needs to be considered such as Reliability, Security & liability. The entire cloud user should pay keen attention in these areas. One Typical factor include the type of contracts we make with the Service provider i.e. contract like where the data resides and to whom the data should be made available (either public or confidential).

Backing up of our data in internet storage adds up a benefit of keeping our data online and accessing whenever & wherever needed. This makes companies & businessmen to collaborate in cloud-based scalable platform in an uncountable ways. Thus business process made easy by means of cloud workspace.

When the point of storage is being focused; in tradition data management, we are sure where the apps and data are; because the chances are they're near you. But in cloud the data is stored online; we may not know who is managing the application and who has the access to our data. Some data regulation and compliance require the physical

auditing of where a Customer's data and processes sit. Thus governance and management of cloud data is important because most of the data being stored is sensitive. It revolves around Cloud accountability and Cloud Privacy [1][2].

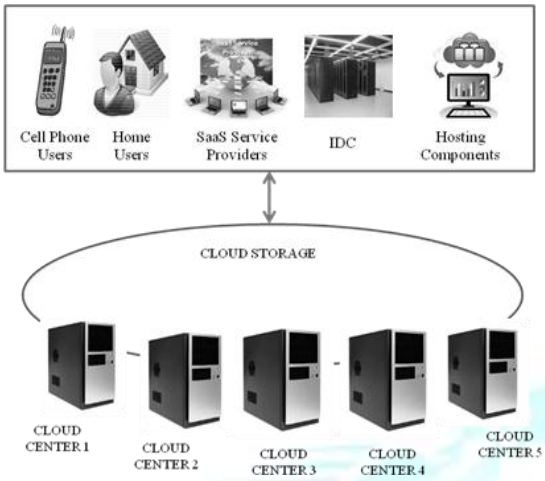

Fig .1 Cloud Data Storage

Hence there is a need for mechanism to ensure remote data integrity in cloud storage for IT & Business people around cloud environment. Because the risk associated with the data depends on the nature of the data being stored. And the cloud user's trust to put their data in cloud storage depends on these security aspects.

In this paper, the main contributions of the proposed system include:

1).Preserving the privacy of the user's data being stored in cloud storage by means of Predicate Encryption [3].At first level, the end-user's data(Customer's data) is being encrypted by the cloud user (eg.Bank Employee) by means of Predicate Encryption to secure against Untrusted servers & Third Party Verifiers [4].

2).Secondly, the remote integrity of the data is being verified by the concept of "Proof of Retrievability" in which the server proves to the client (Cloud user) that their target file is unbroken [5].

The research paper is ionized as Section 2 describing Related Works of this research. Section 3 outlines the problem being identified and Section 4 address the solution to the problem by a proposed

system with detailed functionality. Section 5 analyzes the performance of the proposed System. Finally Section 6 concludes the research with future Work.

2. RELATED WORKS

The work of Secure Data Storage was first analyzed by Cong Wang.et.al [6], in which an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. This construction drastically increased the communication and storage overhead as compared to the traditional replication-based file distribution techniques.

Hsiao-Ying Lin et.al in their paper [7] proposed threshold proxy re-encryption scheme and erasure codes over exponents. The threshold proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols in his system which results in huge Complexity.

Ryan K L Ko et.al in their research [8] used concepts from the Cloud Accountability Life Cycle and the abstraction layers of logs, they have identified the importance of both real-time and post-mortem approaches to address the nature of cloud computing at different levels of granularity. This conceptual model potentially can be used to give cloud users a single point of view for accountability of the CSP.

Shucheng Yu et.al in their writings [9] aimed at fine-grained data access control in cloud computing. One challenge in their context is to achieve fine grainedness data confidentiality, and scalability simultaneously, which is not provided by previous work. Moreover, their proposed writings can enable the data owner to delegate most of computation overhead to powerful cloud servers. Confidentiality of user access privilege and user secret key accountability can be achieved

Suhair Alshehri et.al in their scheme [10] designed a secure cloud-based EHR system using CP-ABE that provided effective solutions to some of the

issues related to standard encryption mechanisms.

It also investigated the feasibility of adopting the CP-ABE in terms of performance and storage overhead. The results suggest that the proposed design would provide reasonable performance and consume negligible storage, and thus it can be used as a replacement to standard encryption mechanisms in cloud-based EHR systems.

3. PROBLEM STATEMENT

The biggest Challenge when auditing cloud-based services can be done from Three perspectives i.e) by CSP, by TPA [11][12] or directly by Cloud User(not the end-user). The participants for Cloud Auditing include the end-user, System Integrators & Auditors. There are also folks from CSC, MS, VMware, Google, Amazon, Web Service, Rack space etc. These Companies work for the best to improve Privacy and Transparency of the User's data; what'll ultimately drive additional market opportunities for cloud Applications. But majority of Security breaches which occurred last year was mainly due to lapses in the security mechanism of CSP. Thus due to these step-down, the process of auditing the user's data was handled on to TPA [13]. But in case of TPA auditing, trusting the user's data security measures to the Auditor needs a full-fledged trust over the Auditor. Any possible leakage of user's outsourced data towards TPA through Auditing protocol should be prohibited. But what happens if the user's data is leaked to the TPA; who foresees the data stored in Data Centers during auditing.

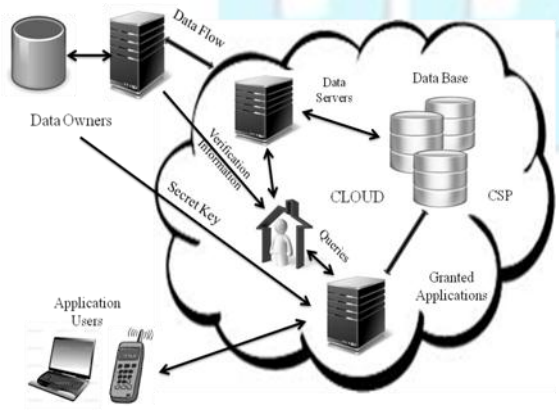

Fig. 2.Data Auditing in Cloud Environment

In such a case, the next higher level of auditing user's data is done by Cloud User itself. The Cloud user preserves the privacy of their end-user's data against Untrusted Servers & TPA; who is the intruder in this case.

4. PROPOSED SYSTEMS

In the proposed System, an automated auditing & verifiability scheme is adopted which support for verifying the integrity of the cloud user's data being stored remotely in Cloud Server (Figure.3).

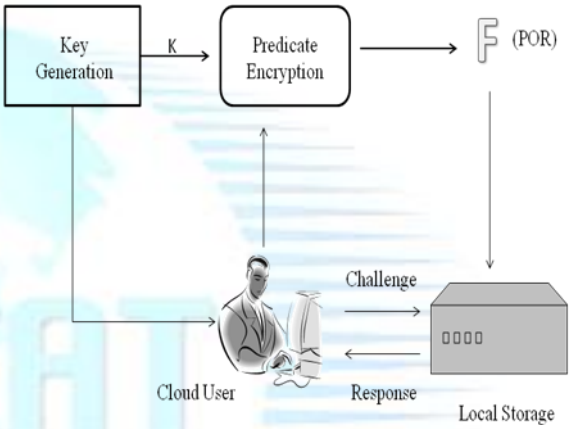

Fig. 3.Cloud Secure Storage Auditing Architecture

The system is based on Predicate Encryption & POR concept which benefits the Cloud user to have a direct Control over the data being stored. The Proposed Scheme will guarantee the following Security assurance: 1) Ultimate Control over the fate of their data. 2) Verify the integrity of the data being stored globally 3) Maintain Strong Storage Correctness even under condition like data dynamically changing; while saving the Computing cost & resource. Techniques we are investing for our research include Homomorphic Encryption, Predicate Encryption, Merkel Hash Type Encryption & their extensions.

4 a. CLOUD SECURE STORAGE SCHEME

A. Encryption Part

At first, the data stored in cloud is not stored just like that, it need to be encrypted before being stored in a Cloud Storage Services. Since the whole functionality is done from Cloud User side, their work should be made simple.

Hence the data stored in cloud storage is encrypted by means of Predicate Encryption [8].Predicate Encryption gives a master secret key owner fine-grained control access to encrypted data. The master secret key owner can generate secret key tokens corresponding to Tokens available.

An encryption of data x can be evaluated using a secret token corresponding to a predicate f; the user learns whether the data satisfies the predicate f(x) =1. A general PBE scheme consists of the four operations:

1.Setup: initializes the crypto-scheme and generates a master secret key MSK, used to generate decryption keys, and a set of public parameters MPK.

(MSK;MPK) = Setup()

2. KeyGen: generates a decryption key Dec(entity) based upon the master secret key and some entity supplied input.

Dec(entity) = KeyGen(MSK; input)

3. Encrypt: encrypts a plain-text message M using the public parameters and supplied encryption key for an entity.

CT = Enc(M;MPK; Enc(entity))

4. Decrypt: decrypts a cipher-text if and only if the attributes held by the entity can satisfy the access policy.

M= Dec(CT;MPK; Dec(entity))

This encryption benefits user by providing them, a simple method of Encryption & reduces burden on them. Roughly, Cipher texts reveal nothing about plaintexts beyond what is revealed by evaluation of Predicates on them.

B. Verification Part

Next, in order to verify the integrity of the data being stored remotely, we incorporate the POR (Proof of Retrievability) technique. This POR technique provides for verifying & prevents the Cloud Storage archives from misrepresenting or modifying the data stored at it without the consent of data owners by means of frequent checks on data archive [14].The Verification of integrity of the file can be either remotely or by downloading the file to a Local Server. The remote checking of file can be done as depicted in Fig 4.

Let the verifier V wants to verify the integrity of the file F. It throws a challenge to the archive and asks it to respond. The challenge and the response are compared and the verifier accepts or rejects the integrity proof.

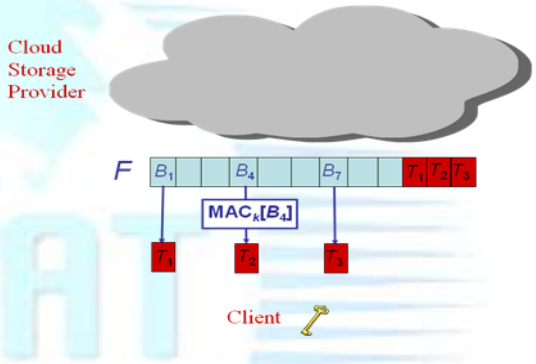

Fig.4.Remote Data Integrity Checking MAC Mechanism

Suppose the verifier wishes to check the integrity of nth block. A data block of the file F with random bits selected in it. The encrypted file F which will be stored in the cloud specifying the block number i and a bit number j generated by using the function MAC which only the verifier knows. The verifier also specifies the position at which the meta data corresponding the block i is appended. This Meta data will be a k-bit number.

The Meta data sent by the cloud is decrypted by using the number i and the corresponding bit in this decrypted metadata is compared with the bit that is sent by the cloud. Any mismatch between the two would mean a loss of the integrity of the client's data at the cloud storage.

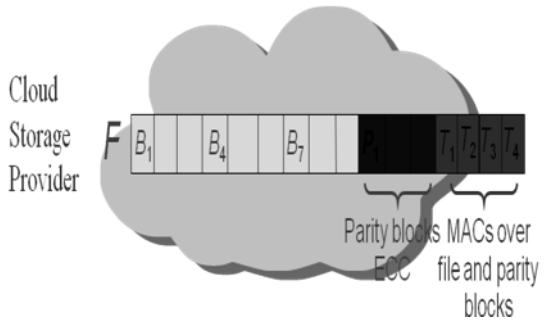

Fig.5 ECC+ MAC Mechanism

But the problem with this checking is that it does not detect small corruption to the file. Hence in order to overcome this drawback, ECC (Error Correcting Code) is combined with the MAC mechanism as in Fig.5

In this way, the Cloud user can examine their end user's outsourced data directly and verify its integrity. When this mechanism is being made automatic, it can reduce the burden on the cloud user side. Thus when an outsourced data is being broken, any message is being sent to the end user signifying that their outsourced data integrity is being altered. Our Proposed system does this functionality and provides for having a control over their stored data in cloud.

5. PERFORMANCE ANALYSIS

In this Section, we analyzed the performance of our proposed System in terms of Privacy, Secure Auditing and Complexity involved in it.

A. Privacy

By design, all PBE schemes are Payload Hiding (PH). This ensures that the payload cannot be accessed by a malevolent entity. A PBE scheme is Attribute Hiding (AH) if the scheme also hides knowledge of the encryption key i.e. attributes/access policies, used to encrypt the cipher-text.

During decryption when an entity attempts to access the plain-text they will only find out if the decryption procedure is unbeaten or not and will not learn anything else concerning the cipher-text and its attributes/access policy. While all schemes by default are payload hiding, attribute hiding schemes are dependent upon the underlying predicates used to realize the scheme.

B. Storage Auditing

Proofs of Retrievability(POR) protocols enable users to check that data outsourced to the cloud is stored in its entirety, untouched, and available on demand. PoRs are competent both in terms of bandwidth and computation usage. In an easy method, a user can verify that an entire archive is intact and retrievable.

In particular, this can be done without the client storing a local copy of the data and without it having to retrieve any of the data. In fact, the work for the client is negligible no matter how large the data is.

C. Computational Complexity

The computational complexity of PBE schemes is reliant upon the exact edifice of the scheme. Regardless, of exact construction some general observations over the complexity can be discerned. The size of the cryptographic keys and cipher-text within PBE schemes is inherently dependent on the number of attributes used during key construction. The size of the decryption keys and cipher-text is based upon the bit-length of the group elements involved, if the construction is based upon pairings.

6. CONCLUSION & FUTURE WORK

Although this problem of remote data storage integrity is being addressed before, in our proposed system both Encryption and Verification is done from Cloud User perspective (eg.Bank Employee). The use of PBE within the cloud appears to be concentrated at both the PaaS and SaaS service layers. Though some may be surprised at PBE's lack of use at the IaaS layer, this was not totally unexpected. In summation, the use of PBE in the Cloud is profitable, moreover recent papers supports these claims. PBE can aide in preventing the unwanted exposure, unwanted leakage and other unwanted breaches of confidentiality of cloud local data. Other guarantees such as integrity, non-repudiation and authenticity need additional security mechanisms.

In addition, the Cloud user is satisfied that their data being stored is unbroken (by POR). As a result, more users are confident to move their sensitive data in Cloud Storage. In Future, this scheme will be made practically applicable in huge Cloud environment.

REFERENCES

[1].Cloud Security Alliance "Cloud Consumer Advocacy Questionnaire and Information Survey", Cloud Data Governance Project, 2011.

[2].Harry Katzan Jr., "On The Privacy Of Cloud Computing, "International Journal of Management & Information System – Second Quarter 2010, Volume 14, No.2,2010,pp:1-12.

[3]. Kwangsu Lee, Intae Kim, Seong Oun Hwang, "Privacy Preserving Revocable Predicate Encryption Revisited", Department of Computer Science, Columbia University, NY, USA,2010.

[4].Vaishnavi Moorthy, S.Sivasubramanian, "Checking Protocol for Secure Storage Services with Data Dynamics and PublicVerifiability in Cloud Computing",IOSR Journal of Engineering, Vol.2(3), March 2012, pp:496-500.

[5].Kevin.D.Bowers, Ari Juels and Alina Opera, "Proofs of Retrievability: Theory and Implementation", RSA Laboratories Cambridge, MA, USA.

[6]. Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Department of ECE, Illinois Institute of Technology, April 2009.

[7].Hsiao-Ying Lin, Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", Member, IEEE;Ieee Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012; pp:1-9.

[8].Ryan K L Ko , Peter Jagadpraman, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, "Trust Cloud: A Framework for Accountability and Trust in Cloud Computing" 2nd IEEE Cloud Forum for Practitioners(IEEE ICFP 2011),Washington DC, USA, July 7-8, 2011, pp:1-9.

[9].Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing" Dept. of ECE, Worcester Polytechnic Institute; pp: 1-9.

[10].Stanisław Radziszowski, Rajendra K. Raj, "Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption" Golisano College of Computing & Information Sciences, Rochester Institute of Technology, Rochester,New York 14623, USA.

[11].K.Govinda,V.Gurunathaprasad, Sathiskumar, "Third Party auditing for secure data storage in cloud through Digital Signature using RSA", International Journal of advanced scientific and Technical research,Vol.4,No.2,2009,pp:1-9.

[12].Shuai Han,Jianchuen Xing, " Ensuring Data Storage through Novel Third Party Auditor Scheme in Cloud Computing", Proceedings of IEEE CCIS 2011,pp: 264-268.

[13].Giuseppe Persiano, " Predicate Encryption for Private and Searchable Remote Storage" Department of Information Technology,CSC'11, March 15-16, 2011; Zurich, Switzerland.

[14]. Sravan Kumar, Ashutosh Saxena, White Paper on "Data Integrity Proofs in Cloud Storage", Software Engineering & Technology Labs, IEEE Proceedings'2011, Hyderabad, India.