IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

THE ENCRYPTION AND AUDITING SCHEME OF CLOUD DATA BY A THIRD PARTY

[1] Prof Aman Kamble [2] Prof SnehalSarangi [3] Prof Geetanjali Sharma
[1]Assistant Professor ,[2] Assistant Professor,[3] Assistant Professor
[1] Department of Computer Engineering,
[1] D.Y Patil College Of Engineering,Akurdi Pune-44,India

Abstract : Confidentiality, integrity and auditability have been studied for long in cryptography, and to provide security is the foundation for all modern cryptographic research. In next generation of cloud computing client store data on centralized cloud server may some challenges. This work is focusing on honesty of data stored in cloud data servers. Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely andmade available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user’s data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of this work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data.The data integrity verification is done by using a TPA which is allow to check integrity of data periodically on rather than client. When data integrity is lost then client gets information from TPA. Not only checking of data purity also supports data dynamics. In this auditing task observes data insertions, deletions and modifications. This system is skillful of supporting both public auditability and data dynamics. Markel Hash Tree is used to improve block level authentication. In order to handle auditing tasks simultaneously, bilinear aggregate signature is used. This permits TPA to execute auditing simultaneously for many clients. In this dissertation the evaluation of multi user based TPA system is presented.

IndexTerms: **Cloud Storage; TPA; Privacy Preserving ; Public Auditing; Integrity, Third party Auditor (TPA), Cloud storage Server (CSS), Cloud service provider (CSP), Proof of Retrievability (PoR), Provable data Possession (PDP), Markel Hash Tree (MHT).**

I.INTRODUCTION

Cloud computing has been envisioned as next generation architecture of IT enterprise which use internet based computer technology for development [1]. Cloud computing is called on-demand computing . Cloud computing is a highly demanded service or utility today due to the positive points such as high computing power, low cost of services, high performance, scalability, accessibility and availability. Resources on cloud are shared by using network due to security issue. The service providers might behave unfaithful , try to cover information loss or corruption for status or economic explanations. Public auditing is the service which is used to ensure integrity of the data stored on the cloud as well as save the computation resources. TPA is able per-form the auditing task and it also verifies the correctness of the cloud data on demand without retrieving a copy of the whole data.The foremost issues in cloud data security include data privacy, data protection, data availability, data location,and secure transmission. Threats, data loss, service disruption, outside malicious attacks, and multi tenancy issuesare the securitychallenges included in the cloud. Data integrity in the cloud system means preserving the integrity of stored information. The data should not be lost or modified by unauthorized users. Cloud computing providers are trusted to maintain data integrity and accuracy of data. Data confidentiality is also important aspect from user's point of view because they store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality could be addressed by increasing the cloud reliability and trustworthiness in Cloud computing. Therefore security, integrity, privacy and confidentiality of the stored data on the cloud should be considered and are important requirements from user's point of view [4]. To achieve all of these requirements, new methods or techniques should be developed and implemented. Data auditing is introduced in Cloud computing to deal with secure data storage. Auditing is a process of verification of user data which can be carried out either by the user himself (data owner) or by a TPA. It helps to maintain the integrity of data stored on the cloud. The verifier's role are categorized into two: first one is private auditability, in which only user or data owner is allowed to check the integrity of the stored data. No other person has the authority to question the server regarding the data. But it tends to increases verification overhead of the user. Second is public auditability, which allows anyone, not just the client, to challenge the server and performs data verification check with the help of TPA. The TPA is an entity which is used so that it can act on behalf of the client. It has all the necessary expertise, capabilities, knowledge and professional skills which are required to handle the work of integrity verification and it also reduces the overhead of the client. It is necessary that TPA should efficiently audit the cloud data storage without requesting for the local copy of data. It should have zero knowledge about the data stored in the cloud server. It should not introduce any additional on-line burden to the cloud user [6].

The three network entities viz. the client, cloud server and TPA are present in the cloud environment. The client stores data on the storage server provided by the cloud service provider (CSP). TPA keeps a check on client's data by periodically verifying integrity of data on-demand and notifies client if any variation or fault is found in client'sdata.

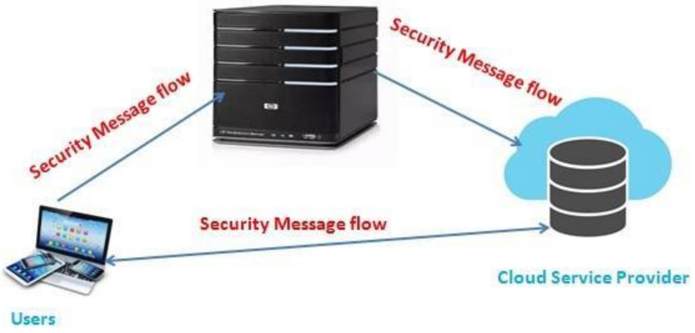


Figure 1 : Cloud data storage architecture

II Literature Survey :

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence it requires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud.Wang et al. [9] has proposed a privacy preserving public auditing protocol which makes use of an independent TPA to audit the data. It utilizes the public key based homomorphic linear authenticator (HLA) with random masking techniques. But this protocol is vulnerable to existential forgeries known as message attack from a malicious cloud server and an outside attacker. To overcome this problem, Wang et al. [6] proposed a new improved scheme which is more secure than the protocol proposed in [9]. It is a public auditing scheme with TPA, which performs data auditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn-Shacham short signature referred as BLS signatures. It also uses random masking for data hiding. For the sake of data binding, this new scheme involves computationally intensive pairing operation thus making it inefficient to use. This proposed scheme has been implemented practically on Amazon EC2 instance which demonstrates the fast performance of the design on both the cloud and the auditor side. But the full-fledged implementation of this mechanism on commercial public cloud is not been tested. So it is difficult to expect it to robustly cope with very large scale data [7]. Wang et al. [10] proposed another protocol that supports both public auditing and data dynamics by using BLS based HLA along with Merkle Hash Tree (MHT). It achieves the integrity of data but fails to provide confidentiality to the data stored on the cloud. Wang et al. [8] has also proposed a design to detect the modified blocks easily using homomorphic token pre-computation and later erasure coded technique is used to acquire the desired blocks from different servers. Solomon et al. [11] proposed protocol uses the same security level as Wang et al. [7] but with better efficiency. It generates a signature set which is an ordered collection of signatures on each file block, thus incurring computation and communication overhead. Meenakshi et al. [2] has proposed a protocol which uses TPA to audit the data of the users using Merkle Hash Tree algorithm. It supports data dynamics but fails to provide confidentiality to the data stored in the cloud.

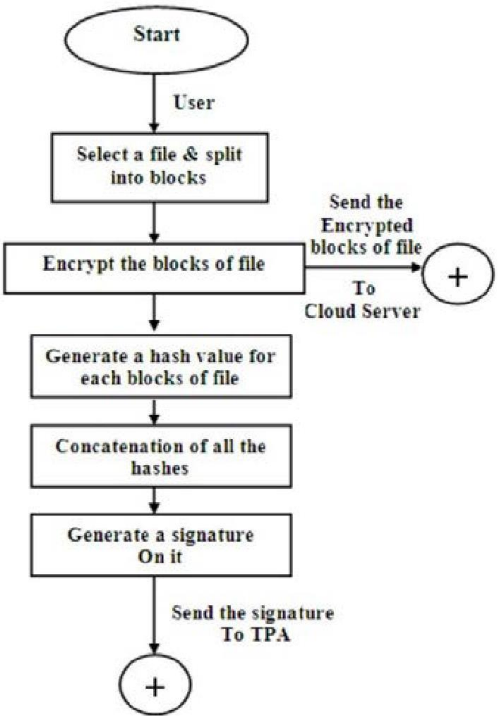
III Proposed System :

The proposed scheme consists of three basic entities; they are data owner, cloud server storage and TPA. Thedata owner or the user is responsible for splitting the file into blocks, encrypting those using AES algorithm, generating a SHA-2 hash value for each, concatenating the hashes and generates a RSA signature on it. The cloud server is used to store the encrypted blocks of files. When the client or data owner request for data auditing to the TPA, it immediately request for the encrypted data from the cloud server. After receiving the data, it generated the hash value for each block of encrypted files. It uses the same SHA-2 algorithm which was used by client. It later concatenate those hash values and generates a RSA signature for that file. In the Verification process, the signature generated by TPA and the one stored in the TPA which is provided by the data user are compared by the TPA. If they matches with each other it means that the data is intact and data is not been tampered by any outsider or attacker. If it does not matches then it indicates that the data integrity has been affected or tampered. The result for the data integrity check is provided to the data owner.

Advanced Encryption Standard algorithm (AES) to provide confidentiality to the data. The blocks which are split are now encrypted using AES algorithm by the data owner. Each blocks of file will be encrypted and stored on the client. A copy of the encrypted file will be transferred to cloud server for storage purpose. It encrypts data blocks of 128 bits using symmetric keys of size 128 bits. After encrypting the blocks, now a hash value for the blocks aregenerated separately. For this purpose a hashing algorithm SHA-2 is being used. After the hashes are generated, the

hashes for each blocks are concatenated and RSA digital signature is performed on it. Digital signatures are used to authenticate the source of messages. Later this signature is sent to the TPA, where it uses this signature to check the integrity of data stored in the cloud server storage is maintained or not. Data owner has the authority to request for data integrity check to the TPA.

Digital signatures are used to authenticate the source of messages. Later this signature is sent to the TPA, where it uses this signature to check the integrity of data stored in the cloud server storage is maintained or not. Data owner has the authority to request for data integrity check to the TPA. Figure 3.shows the working of the data owner in our proposed auditing scheme.


Start
User
Select a file & split into blocks
Encrypt the blocks of file
Send the Encrypted blocks of file
To Cloud Server
+
Generate a hash value for each blocks of file
Concatenation of all the hashes
Generate a signature On it
Send the signature To TPA
+

IV Algorithms

- KeyGen(): This algorithm is run by client and generate Public key pk& Se-crete Key sk.
- SignGen(sk,F) : It is used by client to generate verification metadata like sig-nature used for auditing . if file F is collection of Blocks(M1,M2,…. Mi)

Output Φ is collection of Signature σi on Mi compute σ we compute h=H(M)

- Genproof(F, Φ, chal) :This is run by server to generate proof of data storage correctness& gives output of data integrity proof P for file.
- Verify proof(pk,chal,P) :This algorithm can be run by Client /TPA to audit the proof of receipt P and generate output True or False
- Exec Update(F, Φ ,update): This algorithm can be run by server and generate output F' ,Φ'andPupdate for operation .
- Verify Update(pk, update, Pupdate): This algorithm can be run by Client gener-ate True/False

The Protocol for Provable Data Update (Modification and Inser-tion)

1. Generate σ'I=(H(m'i).u m'i)α
2. Update F and compute R( )
3. Compute R using { H(mi), Ωi};
4. Verify ( ) sigsk(H(R)), Output FALSE if fail.
5. Compute Rnew using {Ωi, H(m'i)}. verify update by checking sign R' is suc-ceed.
6. Update R' signature.

V Conclusion

Many recent challenges have appeared with the fast growth of adaptable cloud services. One of the most significant problems is how to securely delete the out-sourced data stored in the cloud severs. For ensuring security of cloud data stor-age, it is difficult for enabling a TPA for evaluating the quality of service from an objective and independent point of view. Public auditability is able to allow cli-ents for delegating the tasks of integrity verification to TPA while they are inde-pendently not reliable or cannot commit required resources of computation per forming verifications in a continuous manner. One more important concern is the procedure for construction of verification protocols which can be able to accommodate data files that are dynamic. In this dissertation, the problem of employing simultaneous public auditability and data dynamics for remote data integrity check in cloud computing is explored. The construction is designed for meeting these two main goals but efficiency is set as the main goal. For achieving data dynamics that are effective, the existing proof of storage models is enhanced through manipulation of the construction of classic Merkle Hash Tree for authen-tication of block tag . For supporting good handling of multiple numbers of audit-ing tasks, the method of bilinear aggregate signature is further explored for ex-tending the main result into a multiuser setting, where TPA is able to perform multiple auditing tasks in a simultaneous manner. This will reducing the cost required for personal auditing process conducted by users themselves.

References

[1] Q. Wang, C. Wang, K. Ren, W.J. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22(5), pp. 847-859, 2011.

[2] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc.14th European Symp. Research in Computer Security (ESORICS '09), pp.355-370, 2009.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), 2009.

[4] A. Juels and B.S. Kaliski Jr., "POR: Proofs of Retrievability for Large Files," Proceeding 14th ACM Conf. Computer and Communication Security (CCS'07), pp. 584-597, 2007.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-609, 2007.

[6] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Report 2008/175, Cryptology ePrint Archive, 2008