# AN EMPIRICAL MODEL OF AUDITING SERVICE OVER CLOUD DATA RESOURCES

**D.CHANDRIKA[1] (M.Tech),**
Computer Sci. & Engg.
Sanketika Vidya Parishad Engg. College
Pothina Mallayya Palem, Visakhapatnam 41

**N.SATYANARAYANA[2] M.S**
Asst. Professor, Computer Sci. & Engg.
Sanketika Vidya Parishad Engg. College
Pothina Mallayya Palem, Visakhapatnam 41

**B.PRAJITHA[3] (M.Tech),**
Computer Sci. & Engg.
Sanketika Vidya Parishad Engg. College
Pothina Mallayya Palem, Visakhapatnam 41

## ABSTRACT

Auditing over cloud data is an interesting research issue in the field of cloud computing. Data owner uploads data fragments after the segmentation of data component to cloud server and auditor monitors data component which is uploaded by the data owner, traditional approach completely depends on third party auditor. In this paper we are proposing an efficient auditing protocol with Meta data transfer to third party auditor instead of complete data component and dynamic updating when a block of data component corrupted.

## INTRODUCTION

Cloud computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of advantages in the IT history: on-demand service, location independent, resource pooling, rapid resource elasticity and usage -based pricing. From users' perspective, in clouding both individuals and enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with dependent geographical locations and avoidance of capital expenditure on hardware, software and personnel maintenances, etc.

Now a day's cloud service is a rapid growing technology due to its efficient features as a resource area, data storage area, it can be used as an application, used as operating system ,used as a virtual machine and so many advantages with cloud technology. Cloud service follows pay and use relationship with clients, data owner does not know where the actual data is located but he/she can access the stored information or application when required by validating themselves with their credentials.

Data Owner: In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider/ cloud server. Cloud user/Data Owner is a person who stores large amount of data on cloud server which is managed by the cloud service provider or The person who is uploading data or data component to the Cloud service. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services

to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud.

Third Party Auditor: Third party auditors will do the auditing on users request for storage correctness and integrity of data. This Auditor Communicates with Cloud Service Provider and monitors data components which are uploaded by the data owner.

The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

Batch Auditing: It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster.

Data Dynamics: It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Author of [2] proposed scheme which support simultaneous public audability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [3] uses MHT for

Cloud Service Provider: Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done. Organization or enterprises provide various services to cloud users. Confidentiality and integrity of cloud data should be maintained by CSP. The Provider should ensure that user's data and application are secured on a cloud. CSP may not leak the information or else cannot modify or access user's content. The attacker can log into network communication [9].The Cloud Service Provider allows the Data Owner to upload the data component and allows Third Party Auditor to monitor the data components if he/she is authenticated.

Cloud storage is an important service of cloud computing [4], which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud [5]. However, this new paradigm of data hosting service also introduces new security challenges [4]. Owners would worry that the data would be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take [6], [7], [8], [9], [10]. Sometimes, cloud service providers might be dishonest. They could discard the data that have not been accessed or rarely accessed to save the storage space

and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud.

In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. Thus, how to efficiently verify the correctness of outsourced cloud data without the local copy of data files becomes a big challenge for data storage security in Cloud Computing. Note that simply downloading the data for its integrity verification is not a practical solution due to the expensiveness in I/O cost and transmitting the file across the network. Besides, it is often insufficient to detect the data corruption when accessing the data, as it might be too late for recover the data loss or damage. Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users

## RELATED WORK

In the previous architectures data components can be uploaded by the data owners and same data component can be forwarded to auditor for monitoring of data which is uploaded to the server but leads to privacy issue when data owner transfer entire data component to the auditor, so in this protocol we are prosing an efficient auditing protocol with forwarding entire data component to the third party auditor.

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attacks.

The simplest Proof of retrivability (POR) scheme can be made using a keyed hash function hk(F). In this scheme the verifier, before archiving the data file F in the cloud storage, pre-computes the cryptographic hash of F using hk(F) and stores this hash as well as the secret key K. To check if the integrity of the file F is lost the verifier releases the secret key K to the cloud archive and asks it to compute and return the value of hk(F). By storing multiple hash values for different keys the verifier can check for the integrity of the file F for
Multiple times, each one being an independent proof.

A public auditing scheme consists of four algorithms(KeyGen,SigGen,GenProof,VerifyProof).
KeyGen is a key generation algorithm that is run by the user to setup the scheme.
SigGen is used by the user to generate verification metadata, which may consist of MAC,signatures, or other related information that will be used for auditing.
GenProof is run by the cloud

server to generate a proof of data storage. VerifyProof is run by the TPA to audit the proof from the cloud server.

Running a public auditing system consists of two phases, Setup and Audit.

Setup: The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata at the cloud server, and deletes its local copy. As part of preprocessing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response via VerifyProof[14].

## PROPOSED WORK

In this paper we are proposing an efficient auditing service with authentication, integrity of data and security as primary factors in the architecture. The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. We improved the traditional approach with efficient cryptographic approach and secure authentication approach. We also introduced dynamic block updating of corrupted block while intimated by the third party auditor.

Overview of three roles are as follows

Data owner(DO): who has data files to be stored in the cloud and relies on the cloud for data maintenance, can be an individual customer or an organization. Data owner uploads the data components, maintains monitored data components.

Cloud Storage Service Provider(CSP): who provides data storage service and has enough storage space to maintain clients data and updates blocks if any corrupted over database. Cloud service provider allows authorized auditor to monitor the data components and instant mails can be forwarded to Data owner.

Third Party Auditor(TPA): A trusted person who manage or monitor outsourced data under request of the data owner. Auditor details, forwards initiation and authentication parameters to auditor. Auditor receives authentication parameters and monitors data components.

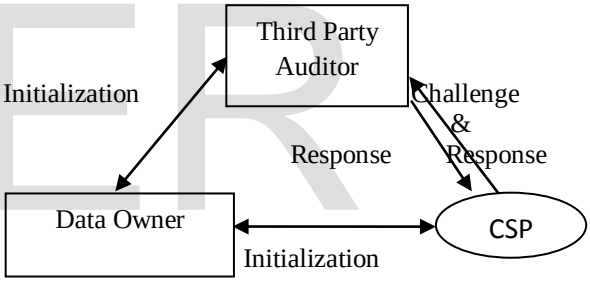


Fig 1: Auditing Architecture

In our approach data owner applies signature mechanism on individual blocks of the content and generates the hash code and encrypts the content with 3-DES algorithm and uploads in to the server, Data components divided into $m_1,m_2....m_n$ & generates random tag key set($t_1,t_2.....t_n$) , Individual block can be encrypted with tag keys and forward the file meta data information and key to the third party auditor ,there auditor performs same signature mechanism and generates signature on the blocks and then check the both signatures if any block code is mismatched that can be intimated to the data owner, then administrator can forward only the corrected information instead of total

content then User can access the service provider. information which is provided by the cloud

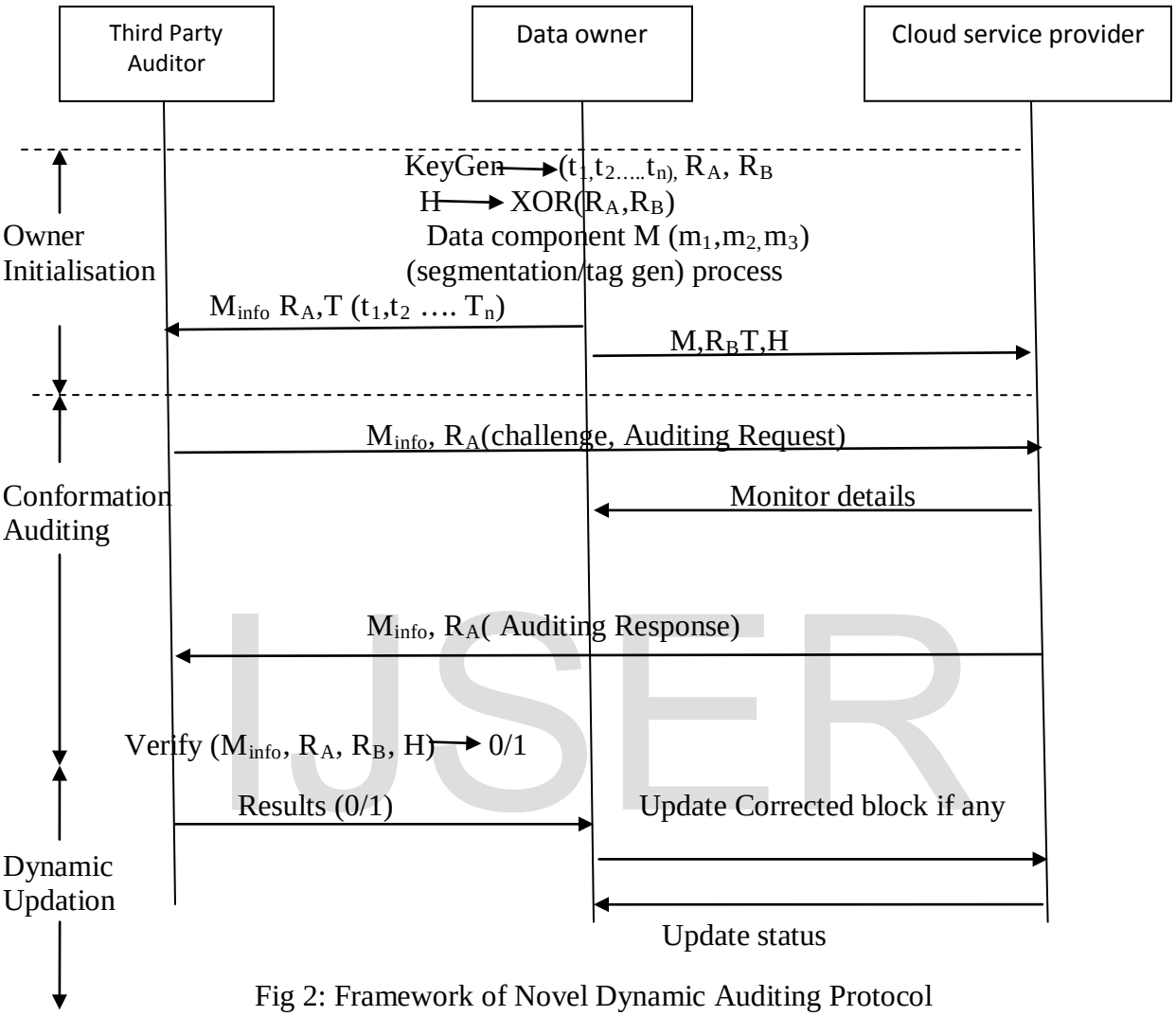


Fig 2: Framework of Novel Dynamic Auditing Protocol

Table 1

Notations

| Symbol | Meaning |
|---|---|
| M | Data component |
| T | Set of tag generation keys |
| $R_A$ | Random challenge to Auditor (Large Prime Number) |
| $R_B$ | Random Challenge to Cloud server (Large Prime Number) |
| $H(R_A,XOR, R_a)$ | Hash code after XOR Over $R_A$ and $R_B$ |
| $M_{info}$ | Meta or abstract informaton of M |
| N | Number of blocks in the each component |

The above Figure shows entire architecture of the protocol, initially data owner segments the data component or file into number of into number of blocks separated by a delimiter as space and generates a random tag key set which is required for encryption of individual blocks respectively. Data owner generates two random challenges for authentication of third party auditor at cloud service provider (CSP) while monitoring the data components of particular data owner. Data owner after encryption of data component uploads to the cloud storage area along with Tag key set and verification parameters and forwards initiation parameters to the auditor for monitoring of data component.

**Step by Step Process for protocol Implementation:**

Step1: Data owner fragments Data component D into n blocks ($m_1$,$m_2$….$m_n$).

Step2: Generates a random tag key set T (t1,t2…..tn) to encrypt the block with triple DES algorithm and finds signatures on encrypted blocks for authentication

Step3 : Generates random challenges $R_A$,$R_B$ and computes hash value of xor between $R_A$ and $R_B$.

x := hash ( $R_A$ XOR $R_B$ )

Step4 : Forward Data component, Tag key set and RB to service provider and meta data and authentication parameters ($M_{info}$ $R_A$,T ($t_1$,$t_2$ …. $T_n$) ) to Auditor

Step5 : data owner Checks authentication by recomputing hash code with auditor RA.

Step6 : Auditor again divides D in ti number of blocks at server end, encrypts and applies same signature and compares signatures of corresponding blocks

Step7 : Monitoring Status can be forwarded t Data owner through smtp implementation

Step8: Auditor updates Data cmponet status then Data owner updates blocks if corrupted

Auditor receives the initiation parameters and meta data for monitoring of data component and authenticate himself at cloud service provider by forwarding the random challenge ($R_A$).Cloud service provider validates the auditor by generating the hash code of XOR ($R_A$,$R_B$),if authentication is success, csp allows the author to monitor the data component and instantly forwards a mail response to the data owner. Data owner receives monitoring status from auditor, if uploaded data is same as monitored data then no issue otherwise data owner updates corrupted block which is informed by the auditor report.

## CONCLUSION

We conclude our research work with an efficient auditing protocol without losing its data integrity, In our approach we need not forward the data components to the auditor directly in our approach, but auditing can be done efficiently. We can enhance our approach by increasing the authentication approach rather than simple random challenges. Apart from the traditional approaches we are not completely rely on the third part auditors, So over protocol allows the auditor to monitors data component meta information only that provides the abstract information of data component. Data owner can receive the regular monitoring details.

## REFERENCES

[1] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, “Implementation of EAP with RSA for Enhancing The Security of Cloud

Computig",International Journal of Basic and Applied Science,vol 1, no. 3, pp. 177-183,2012.

[2] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li "Enabling Public Audatability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 859,2011.

[3] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29 -33, ISSN: 6602 3127, 2011

[4] P. Mell and T. Grance, "The NIST definition of cloud computing,"National Institute of Standards and Technology, Tech. Rep., 2009.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H.

[6] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, 1st ed. New York, NY, USA: McGraw-Hill, Inc., 2010, ch. 7. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM,

[7] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, "An analysis of latent sector errors in disk drives," in SIGMETRICS, L. Golubchik, M. H. Ammar, and M. Harchol-Balter, Eds. ACM, 2007, pp. 289–300.

[8] B. Schroeder and G. A. Gibson, "Disk failures in the real world: What does an mttf of 1, 000, 000 hours mean to you?" in FAST. USENIX, 2007, pp. 1–16.

[7] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A cooperative internet backup scheme," in USENIX Annual Technical Conference, General Track.USENIX, 2003, pp. 29–41.

[9] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote integrity checking," in The Sixth Working Conference on Integrity and Internal Control in Information Systems(IICIS). Springer Netherlands, November 2004.

[10] M. Naor and G. N. Rothblum, "The complexity of online memory checking," J. ACM, vol. 56, no. 1, 2009.

[11] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[12] T. J. E. Schwarz and E. L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage," in ICDCS. IEEE Computer Society, 2006, p. 12.

[13] 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.

[14] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking incritical information .

[15] Cong Wang, Sherman S.M, Qian Wang, Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage".