ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Resources Portions in Cloud Using Describe Data

Goda Srinivasa Rao
Research Scholar at JNTUA
Department of CSE
PNC & VIJAI Institute of Engineering & Technology, Repudi, Guntur, AP.

Dr.Rajeswara Rao Ramisetty
Associate Professor
Department of CSE
JNTUK University College of Engineering, Vizianagaram, AP.

Abstract:

The increasing popularity of cloud storage services has lead companies that handle critical data to think about using these services for their storage needs. The paper presents a way to implement Third Party Auditor which not only checks the reliability of Cloud Service Provider but also checks the consistency and accountability of data The architecture shifts data, applications and development environments to large data centers thereby providing storage software and platform services online Our design is based on Elliptic Curve Cryptography and Sobol Sequence in Our method allows third party auditor to periodically verify the data integrity stored at CSP without retrieving original data we make use of Public-Auditing. We propose a way in which the Merkle Hash Tree (MHT) used in a method called RSAS is made dynamic by using the concept of relative index to compute the index of leaf node quickly and a dynamic operation scheme based on this tree structure for cloud storage the proposed scheme aims at keeping the user data integrated and support data restore. The system also reduces the server computation time when compared with previous systems the use of homomorphism in multi-clouds due to its ability to reduce security risks using the enhanced modified festal technique.

Index Terms: ***data security, federated cloud, Privacy Preserved Data Storage, Third Party Auditor, Message Digest, Message Authentication Code.***

1. INTRODUCTION

Cloud computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware[1] Through the use of virtualization and resource time-sharing, clouds address with a single set of physical resources a large user base with different needs Data Security [4,5,6] is an important research topic in cloud computing. Security in cloud can only be remotely implemented by the client since they do not have access to data centers and protocols in the system Cloud storage becomes an increasing attraction in cloud computing paradigm, which enables users to store their data and access them wherever and whenever they need using any device in a pay-as-you-go manner[2]. Moving data into cloud offers great conveniences to the users since they do not have to care about the large capital investment in both the maintenance and management of the hardware infrastructures. Amazon's Elastic Compute Cloud [3]and Amazon Simple Storage Service The specification of deciding the key is based on the metadata attribute in the metadata server as well as the user key[7] Most of the existing cloud encryption schemes are constructed on the architecture where a single trusted (TPA) third party authority has the power to secure the secret data stored at the cloud servers The data owners therefore need to be convinced that the data are correctly stored in the cloud[8] In order to achieve data integrity and availability and enforce the quality of cloud storage

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

service, efficient methods that provide on-demand data correctness verification on behalf of the users are used. The data integrity problem is solved by many systems the server regarding the data integrity, whereas, Public Auditability is more convenient and preferred over Private Auditability because it allows a third party to perform integrity verification on behalf of client. The client is not solely responsible for it and so it largely reduces client's burden. We refer this third party as the Third Party Auditor (TPA)[9].

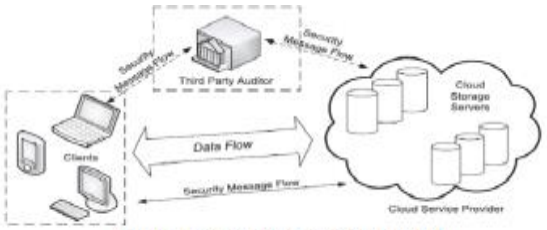

Fig 1: Cloud Storage Architecture [1]

2. RELATED WORKS

Data Privacy and Verification in cloud have been handled extensively in many existing works. On surveying the field of public audit ability it is evident that considering the third party auditor as the vulnerable component is not addressed anywhere the security of remote storage applications has been increasingly addressed in the recent years, which has resulted in various approaches to the design of storage verification primitives. The literature distinguishes two main categories of verification schemes [13]. Recently much work has been done in the area of cloud security. Majority of them focus on the integrity verification of data stored in the cloud. Descartes et al. in [10], use RSA based hash function for verification of the file stored at the remote server. Using this scheme, it is possible for the client to perform multiple challenges using the same metadata. The data stored in cloud is vulnerable to malicious attacks and it would bring irretrievable losses to the users, since their data is stored at an untrusted storage servers [15] have proposed a query based hiding schema information using a bloom filter. The query given is processed and the attributes of the query is used for key generation [11].

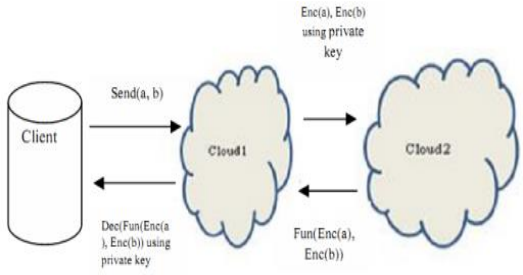

Fig.2 System model

Public Verifiability for Storage Security

This work [14] states that by data outsourcing, users can be relieved from the burden of local data storage and maintenance. It also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals [12].

Deterministic Secure Storage

Deterministic solutions are verifying the storage of the entire data at each server. Deswarte [18] and Filho.[19] are firstly proposed a solution to remote data integrity. Both use RSA-based functions to hash the whole data file for every verification challenge they require pre-computed results of challenges to be stored at verifier, where a challenge corresponds to the hashing of the data concatenated with a random number proposed a survey paper where they discussed about factors affecting cloud computing storage adoption, vulnerabilities and attacks. The authors have also identified relevant solution directives to strengthen security and privacy in the cloud environment [16].

3. SYSTEM MODEL

In cloud data storage model, the user stores his data in cloud through cloud service provider and if he wants to access the data back, sends a request to the CSP and receives the original data. If data is in encrypted form that can be decrypted using his secrete key [17] the data is stored in cloud is vulnerable to malicious attacks The data integrity problem is solved by many systems. Some make use of two-party auditing process [3] while some use third-party auditing. In two-party auditing, the client itself sends the challenge to the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

server and the server is supposed to respond to it with a proof to prove that it contains the data in integrated manner. In third-party auditing, however, the client delegates the right of auditing the data at the server to a third party called as the Third-Party Auditor it would bring irretrievable losses to the users, since their data is stored at an unfrosted storage servers The cloud storage model considering here is consists of three main components

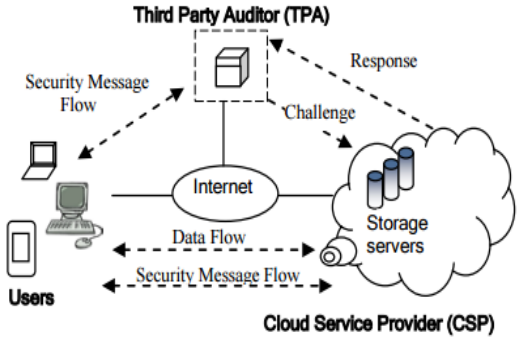

Fig.3 Cloud Data Storage Model

4. PROPOSED SYSTEM

In our scheme the client asks the CSP to provide service where CSP authenticate the client. RSA with Digital signature part will be done by the user to provide data authentication, data integrity and non-repudiation. This is done by first encrypting the user's data using symmetric encryption Client store[4] their data at the cloud, delete the local copy of that data and rely completely on the cloud server for data safety and maintenance auditing of the data is necessary to assure client safety of his data. To overcome this problem of data security, we introduce an AES based Storage integrated.

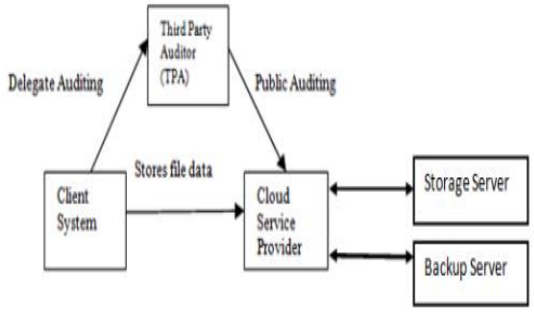

Fig.4 Block Diagram of AES based Storage Security System

A. Data Uploading and Downloading

When the file is uploaded to the cloud server, before storing it, AES algorithm is used to encrypt the data to protect the content from being displayed to the server Similarly at the time of download, the data is decrypted to plain text form The TPA generates a challenge, sends it to the CSP and in response, the server generates a proof for the corresponding challenge. In the proof, the server generates the proof [8] the proof contains the signature of the root and the root of the MHT generated for the respective file

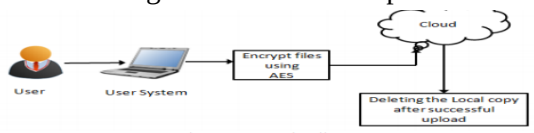

Fig. 4: Data Uploading

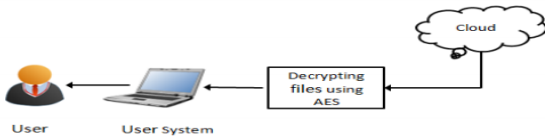

Fig. 5 Data Downloading

B. Enhanced modified matrix based Festal Network

Algorithm the below section describes the Festal Function F which plays a major role in the proposed encryption technique to specific types of computations to be carried out on the corresponding cipher text. The result is the cipher text of the result of the same operations performed on the plaintext That is homomorphism encryption allows computation of cipher text without knowing anything about the plaintext to get the correct encrypted result[6].

1 Read P, K
2. P_0 = Left half of P.
3. Q_0 = Right half of P.
4. for i = 1 to r
begin
P_{i-1} = Mix P_{i-1}
P_{i-1} = P_{i-1} K
Q_{i-1} = Shift (Q_{i-1})
Q_{i-1} = Mix Q_{i-1}
Q_{i-1} = Q_{i-1} K
(P_i, Q_i) = Shuffle (P_{i-1}, Q_{i-1})
End
5. C = P_r ||Q_r
/* || represents concatenation */

6. Write(C) Cipher key C = L_{mxn} || R_{mxn} / * || represents concatenation */
End

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

C. Metadata Verification Scheme

In Public auditing schemes have achieved the support for dynamic data updates which is a critical need in environments like cloud where huge volumes of data are updated frequently. These verification schemes do not consider the effects on data privacy in the hands of a third party auditor The scheme verifies metadata rather than the actual data. The model is divided into two fundamental blocks the cloud service provider on behalf of the client in order to check the data security at the cloud and the reliability of the server is presented [13]. Then, an efficient scheme for checking the data integrity between the client and the server is introduced

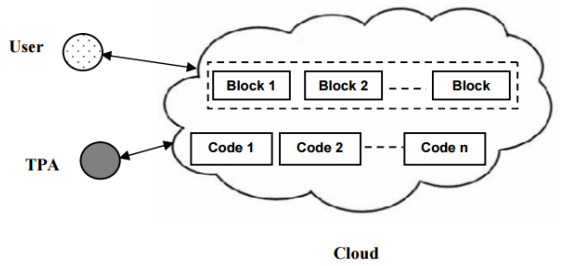

Fig. 6 Basic Verification Scheme

D. Merkle Hash Tree (MHT):

A Merkle Hash Tree is a well-studied structure used for authentication purpose [7], which is intended to prove efficiently that a set of elements are unaltered and undamaged. It is used for decreasing the server computation time [9] It is used by cryptographic methods to authenticate the file blocks. The tree is constructed as a binary tree where the leaf nodes are the hashes of the authentic data values i.e. the original file blocks Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system

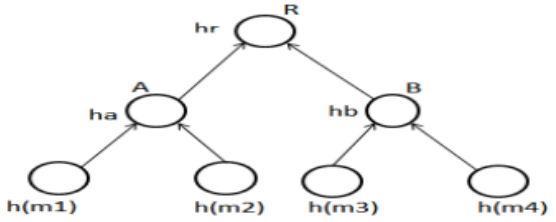

Fig.7 Merkle Hash Tree (MHT)

Advanced Encryption Standard (AES):

AES is a block cipher. The algorithm supports a variety of key sizes as 128,192 or 256. The default size is 256 bits. The encryption of data blocks is done in 10, 12 and 14 rounds depending on the size of the key used. It provides fast and flexible encryption and can be easily implemented on various platforms.

- AES has speedy key setup time and a good key agility.
- It is suitable for restricted-space environments as the memory requirement for its implementation is less.
- It makes efficient use of resources due to its inherent parallelism which results in a very good software performance.
- It does not have any serious weak keys.
- Any block size and key sizes are supported by AES that are multiples of 32 (greater than 128-bits)
- No linear and differential cryptanalysis attacks have yet been proven on AES.

5. IMPLEMENTATION

The proposed model is analyzed by executing set of experiments. The experiments are carried out in a cloud setup using eucalyptus which contains cloud controller and walrus as storage controller on a 5 node cluster

File ID	DES	AES	BlowFish	EFCA
3	0.2833	0.3833	0.53	0.77
4	0.3979	0.4979	0.69	0.87
5	0.527	0.627	0.727	0.927
7	0.477	0.577	0.57	0.897
12	0.3	0.4	0.59	0.8083
15	0.4	0.5	0.541	0.851
20	0.3	0.4	0.725	0.8125
28	0.5	0.6	0.66	0.866
39	0.4	0.5	0.75	0.9375
40	0.5	0.65	0.7	0.895
51	0.21	0.31	0.421	0.7721

Comparison of avalanche effect of cipher key

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

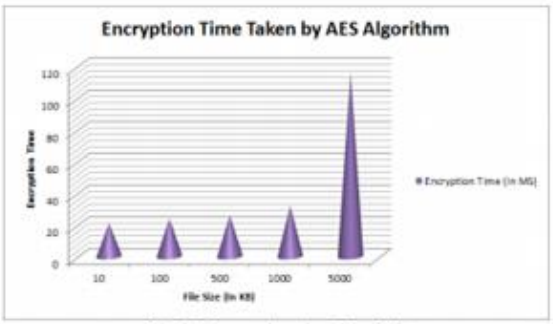

Fig 8: Encryption time by AES

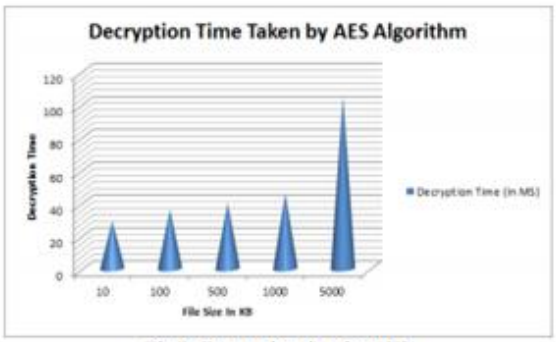

Fig 9: Decryption time by AES

6. CONCLUSION

Cloud Computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware As market grows the threat on data also grows To protect the data from unauthorized access and to ensure that our data are intact we proposed a scheme The verification scheme can further be specialized using security protocols to check the auditor's reliability and confidentiality in handling the data and also can be checked for biasing. Further the data stored in cloud can be encrypted and the code generated for individual files can be sent over using secured transmission protocols

7. FUTURE WORK

Our scheme also supports dynamic data operations which performed by the user on data stored in cloud while maintaining same security assurance We have proved that proposed scheme is secure in terms of integrity and confidentiality through security analysis In addition to that, the whole of the proposed security system is semantically secured against malicious users and also against the illegal activity of the trusted CSPs.

8. REFERENCES

[1] G. Michael Cammert, Jurgen Kramer, and Bernhard Seeger, "Dynamic Metadata Management for Scalable Stream Processing Systems", in Proc. IEEE International Conference on Data Engineering Workshop, 2007, pp.644-653

[2] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou ,‖ Privacy-Preserving Public Auditing for Secure Cloud Storage,‖ IEEE TRANSACTIONS ON COMPUTERS.

[3] Bo Chen, Reza Curtmola ,‖ Robust Dynamic Provable Data Possession,‖in 32nd International Conference on Distributed Computing Systems Workshops, 2012.

[4] Qi Zhang, Lu Cheng et al., "Cloud Computing: state-of-the-art and research challenges," Journal of Internet Services and Applications, Volume 1, Springer, 2010, pp.7-18.

[5] Daniele Catteddu, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," Communications in Computer and Information Science, Vol. 72, Springer 2010.

[6] N. Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/ articl/ 142549/amasons_down_for_sever_hours.html", 2008 .[7] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors",Online at http://www.techcrunch.com/2008/07/10/mediamaxthel ink up-closes-its-doors/, July 2008

[8] J. Heurix, M. Karlinger and T. Neubauer, "Perimeter – Pseudonymization and Personal Metadata Encryption for Privacy-Preserving Searchable Documents", Proc. of International Conference on Health Systems, vol. 1, no. 1, (2012), pp. 46-57.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[9] Y. Tang, P. P.C. Lee, J. C.S. Lui and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transacations On Dependable and Secure Computing, vol. 9, no. 6, (2012), pp. 903-916.

[10] Q. Wang, C. Wang, K. Ren, W. 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, no. 5, (2011), pp. 1-13

[11] D.G.Feng, M. Zang, Y. Zang and Z. Xu,"Study on cloud computing security", Journal of Software, vol.22 (1), pp. 71-83, 2011.

[12] L.M. Kunfam, "Data Security in the world of cloud computing", IEEE Security and Privacy, vol.7 (4),pp.61- 64,2009.

[13] B. Waters and H.Shacham, "Compact proofs of Retrievability", Proc.14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT' 08), pp.90-107, 2008.

[14] M. Venkatesh, Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing, ICRTIT-IEEE 2012

[15] Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security 8.12 (2008): 280-286.

[16] Simar Preet Singh, and Raman Maini, "COMPARISON OF DATA ENCRYPTION ALGORITHMS", International Journal of Computer Science and Communication (IJCSC), Vol. 2, No. 1, January-June 2011, pp. 125-127

[17] Dalia Attas and Omar Batrafi, "Efficient Integrity checking technique for or securing client data in Cloud computing," International Journal of Electrical & Computer Sciences, vol. 11, no 5, 2013 Scheme in cloud," Proc. of 2013 International Conference on Green High Performance Computing, Nagercoil, 2013

[18] Raju "Data Integrity using Encryption in Cloud Computing," Journal of Global Research in Computer Science, vol. 4, no. 5, 2013.

[19] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007.

Author Details

Dr. Rajeswara Rao Ramisetty presently working as a Associate professor in department CSE at JNTU Vizianagaram JNTUK University, Kakinada. He has 14 years of teaching experience. His research interested areas are speech processing, cloud computing, distributed computing and secure computing.

Goda Srinivasa Rao working as an Associate Professor & HOD in the department of CSE in PNC & VIJAI Institute of Engineering and Technology, Repudi, Guntur (Dist), AP., His research interested areas are cloud computing.