International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Enhancing Cloud Data Security and Integrity Using Third Party Auditing Service

Rakesh J. Wagh[1], Rajesh C. Dharmik[2]

[1, 2] Department of Information Technology, Yashwantrao Chavan College of Engineering, Nagpur, India

Abstract: ***Cloud Computing is called future generation architecture for computing. Generally cloud computing is a large scale and internet based computing paradigm in which pool of resources, shared software information is accessible to the world via internet. Now a day's data storage is important application of cloud where data owners put their data on cloud servers and users access their data from servers, Since Cloud Computing stores the resources and data in the cloud environment, security of stored data has become the main concern. Even though the Cloud computing is efficient and promising; there are several challenges for data security as there is no data proximity for the Cloud user. In proposed work the aim is to guarantee the data correctness, we consider the task of assigning multiple Third Party Auditor (TPA) on behalf of cloud client instead of existing schemes which uses single verifier (TPA). Also to ensure user authentication we extend our work by using the technique of digital signature and the Blowfish cryptographic algorithm together for better security of the cloud data and miscellaneous attacks. It provides good security with better data efficiency.***

Keywords: Cloud computing; Third Party Auditor; data security and integrity; Digital signature: cryptographic algorithm.

1. Introduction

Cloud computing is the emerging field in the digital era [7] where Cloud computing is a very important computing outline in which services to assign to software, Network Connection & also services over a network. This collectively known as the cloud [3]. The basic idea behind cloud computing is to proceed computing tasks from individual systems into the cloud, which provides resources over the Internet. By tapping into cloud architecture, cloud users can gain fast access to best applications and eventually boost computing resources in a easy and cost effective manner. The advantage of cloud is cost savings and so cloud storage is best business solution for data storage outsourcing as it gives infinite storage space in pay per use way. Many organizations reduce their financial overhead of data maintenance since they can achieve this by using remote backups from third party cloud storage providers.

The increasing of data storage in the cloud has gain a lot of attention over security issues of this cloud data. One of important and primary issue with cloud storage is verification of data integrity at non trusted cloud servers. Like Byzantine failures. To verify the integrity of data in cloud without having local copy of data files for large collection of outsourced data, here the main problem arises that how periodically user verifies integrity without having local copy of data[1].

Recently number of techniques of verification protocol have been developed using different systems and all those audit systems verifies integrity by single audit verifier (TPA). In that verification process metadata is stored related to file blocks and integrity of data get checked by challenge-response based[1]. The main disadvantage of this system is crash in system due to heavy challenge on single TPA and also the network traffic also getting high near the TPA system and it may create congestion in network therefore in this system the performance get degraded. Therefore we aim an efficient protocol which overcomes all problems related to single verifier.

2. Problem Statement

To design and implement a Protocol for Efficient Distribution Verification and authentication policy having following goals.

a) **Authentication:** Provide access to the authorized users and provide safety from unauthorized access.
b) **Integrity:** The data stored safely in cloud and maintain all the time in cloud without any alteration.
c) **Encryption:** Ensure the security of data by providing the encryption to our data.
d) **Low-Overhead:** The Scheme verifies the security of data stored in cloud with less overhead.

Design Goals:

1. Provide user authentication security by using digital signature to protect cloud data from a unauthorized users.
2. To construct a web application this verifies the integrity of data in distributed manner with support of multiple TPA.
3. Provide security to the data present at the cloud by using standard encryption algorithm

3. Existing Work

Syam Kumar et al.[1] introduced an efficient distributed Multiple third party auditor verification protocol to solve the problems of data integrity. In which author discuss about multiple TPA verifier and shows advantage of this method over single verifier TPA.
In proposed work of Syam Kumar et al. designed the protocol based on RSA-based Dynamic public Audit protocol which contains 3 phases as Key Distribution, Verification Process and last Validating Process. The main TPA validates integrity by observing report from subTPAs. Author observes better performance and smoothly found data corruptions efficiently compared to single verifier (TPA).

Wenjun Luo and Guojing Bai[2], proposed a remote data integrity protocol for cloud data which is based on HLAs and RSA signature which supports public verifiability in the

context of ensuring centrally stored data under different systems. According to them the data integrity is get highly improved, they also done the security analysis and result shows security against server and preserves privacy against TPA.

Arjun kumar, Byung Gook Lee HoonJae Lee and Anu Kumari[3] proposed a method that allows the user to store and access their data on cloud securely, they also provide provision that no one except the authenticated user can only access data and neither the cloud provider. In there work they uses ECC Encryption algorithm and they showed that the ECC is more efficient than the RSA.

Barsoum[4] et al proposed a Dynamic Multiple Data Copies on Cloud Servers which supports public verifiability of data integrity. This method achieves cloud data integrity which store on cloud. To verify the integrity of data, public verification process as third party auditor get enables behalf of public key of the data owner.

Wang et al.[5] designed an public auditability and data dynamics for data security storage in cloud computing using Merkle Hash Tree(MHT). There result shows the guarantee of achievement of data integrity with data dynamic operations.

Dr.NEDHAL A. AL SAIYD, NADA SAIL[6] proposed the cloud computing security development lifecycle model for gaining safety and enables the user for integrity to there data. They designed the integrity checking algorithm which eliminates the requirement of Third party auditing. They showed the analysis result for the algorithm. In order to protect cloud and data on it they discuss the vulnerabilities and risks related to it.

Rashmi Nigoti, Manoj Jhuriya, Dr.Shailendra Singh[7] Member IEEE discuss different security issues to cloud and different cryptographic algorithms which will be adoptable for better security to the cloud. Also they provide the comparative study of cryptographic algorithms used for cloud in there study.

4. Proposed Work

Our proposed work is based on multiple audit verifiers (Multiple TPAs) instead of using single audit Verifier (TPA) to verify the integrity of data in distributed way. In proposed protocol SHA-2 along with the digital signature is used for auditing the cloud data. Initially the user data get stored, on which the blowfish algorithm get applied while data sending to the cloud. In proposed protocol number of SUBTPA's concurrently works under single Main TPA, Main TPA assign some rows or blocks of file to the each SUBTPA for auditing. After completion of audit the result is collected by Main TPA from each SUBTPA and the final audit report is created which finally sent to the user. The comparison of data at the time of audit is done with help of digital signature which was generated at the time of storage itself.

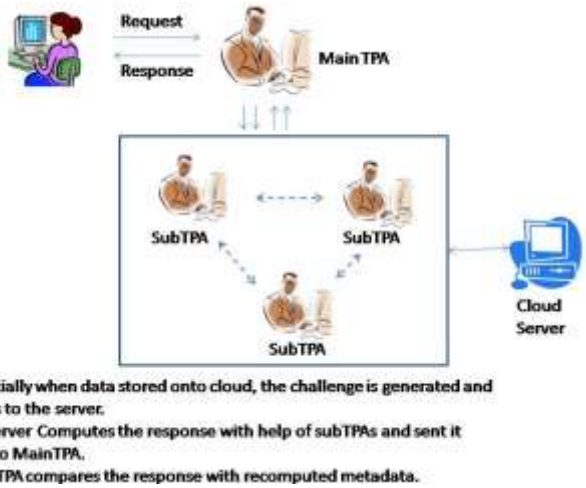

Figure 1: Multiple TPA Architecture[1].

For offer better security to the stored data the blowfish cryptographic algorithm used for encryption of data which comes in category of symmetric key encryption algorithm, which use same key for encryption and decryption. The block size it requires is 64 bits; so the cloud data that aren't a multiple of 64-bits in size have to be padded and get in the form of 64 bit blocks. It uses a variable –length key, from 32 bits to 448 bits. Data encryption happens via a 16-round Feistel network[7]. Therefore the data get store safe and processed securely.

5. FlowChart of Proposed Work

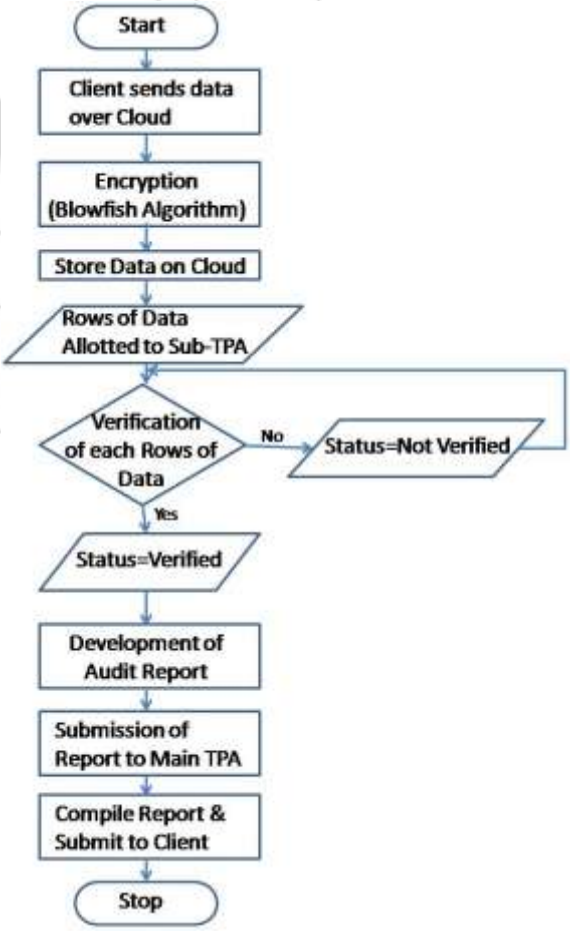

Figure 2: Flowchart of Proposed Model

6. Working Scheme

The proposed scheme is based on multiple audit verifiers (Multiple TPAs) instead of using single audit Verifier (TPA) to verify the integrity of data in distributed way.
Possible Overall Flow of ECC web application.

1) A web Application will be designed
2) There is following identified users
   a) Admin
   b) Main-TPA (Third Party Auditor)
   c) Sub-TPA's
   d) Client
3) The client send the data from his interface provided through web application to be stored on cloud.
4) The data then encrypted using BLOW FISH algorithm while sending to the cloud. The data is now stored at cloud.
5) A Digital Signature will be generated for each row of data and stored in the cloud along with the data.
6) The Main TPA will assign some rows of a database to multiple Sub-TPA's for auditing.
7) Each sub-TPA will get only those many number of rows assigned to him by Main-TPA.
8) For auditing SHA-3 along with Digital Signature is used.
9) Each Sub-TPA try to audit each row assigned to him.
10) While Auditing, a digital signature will be generated for each row and is compared with the one which is stored on the cloud. If the match is found the data in that row is considered to be integrated and is intact.
11) The Sub-TPA's after auditing all the rows assigned to them will generate a report informing about the integrity of rows audited by him. The sub-TPA's then send the report to Main-TPA.
12) The main TPA after receiving reports from all the sub-TPA's consolidate them to form a single report for the selected database and send it to Client.

7. Performance Analysis

We list the features of our proposed scheme in Table 1 and make a comparison of proposed scheme with other preexisting schemes.

Table 1: Comparison Table for Results Obtained with existing techniques

Method	*No. of Records*	*Time(ms)*	*% Data Success Rate*
EDVP	20	326.19	81.22
MD5	20	341.14	73.67
SHA1	20	329.15	67.12
	20	318.83	87.33

Figure 3: Performance chart

8. Conclusion

Use of Blowfish algorithm improves the security of data which store on cloud along digital signature improves performance. The proposed system uses multiple SubTPAs concurrently so the work get equally distributed and therefore the efficiency of Server get Increased.

Also in compare with the single verifier verification multiple TPA verification detect the more data corruptions. the region of non-interest that is area which does not contain much information (important information).

References

[1] Syam Kumar.P, Subramanian. R, Thamizh Selvam:" An Efficient Distributed Verification Protocol for Data Storage Security in Cloud Computing" Advance Computing, Networking and Security (ADCONS),2013 Second International Conference, page 214-219, December 2013
[2] Wenjon Luo, Guojing Bai "Ensuring The Data Integrity in Cloud Data Storage" Cloud Computing and Intelligence Systems (CCIS),2011 International Conference, Sept 2011, pp 240-243.
[3] Arjun kumar, Byung Gook Lee HoonJae Lee and Anu Kumari "Secure Storage and Access of Data in Cloud Computing" ICT Convergence (ICTC),2012 International Conference, page 336-339, October 2012.
[4] Hasan, M. A., Barsoum, A. F. "On Verifying Dynamic Multiple Data Copies over Cloud Servers", Technical Report, Department of Electrical and Computer Engineering University of Waterloo, Ontario, Canada, Aug 2011.
[5] Wang Q., Wang C., Li J., Ren K., and Lou W., "Enabling public verifiability and data dynamics for storage security in cloud computing", IEEE Trans. Parallel and Distributed Systems. VOL.22, NO.5. May, 2011,pp.
[6] Dr.NEDHAL A. AL SAIYD, NADA SAIL:"Data Integrity in Cloud Computing Security", Journal of Theoretical and Applied Information Technology.VOL58, NO.3,DECEMBER 2013.
[7] Rashmi Nigoti, Manoj Jhuriya, Dr.Shailendra Singh:" A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences,4(2), March-May 201,pp 141-146.
[8] Wang C., Wang Q., Ren K., cao N., and Lou W.,(2012) "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Trans. Service Computing. VOL. 5, NO. 2, APRIL -JUNE 2012, pp.220-232.
[9] Hao Z., Zhong S., Yu N.,(2011) "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability", IEEE Trans Knowledge and Data Engineering,Vol.23, Issue 9, pp.1432 –1437.
[10] P. Varalakshmi and Hamsavardhini Deventhrian "Integrity checking for Cloud Environment using Encryption Algorithm." Recent Trends in Information Technology (ICRTIT), Apr-2012, pp.228-232.
[11] Yang J., Wang H., Wang J., Tan C., and Yu D., (2011) "Provable Data Possession of Resource-constrained Mobile Devices in Cloud Computing", JOURNAL OF NETWORKS, VOL. 6, NO. 7, July,, 2011,pp.1033-1040