ISSN No. 0976-5697

Volume 8, No. 1, Jan-Feb 2017

International Journal of Advanced Research in Computer Science

RESEAECH PAPER

Available Online at www.ijarcs.info

Adaptive Model For Integrity Verification In Cloud Computing System

Shakti Arora
Department of Computer Science & Engineering,
SRM University, Haryana
Sonipat, Haryana, India

Surjeet Dalal
Department of Computer Science & Engineering,
SRM University, Haryana
Sonipat, Haryana, India

Abstract: In past years the usage of cloud data services has been widely increased as well the solution for assuring the data integrity has been extensively designed by different researchers. Some of the attempts started considering the multiple cloud users modifying the data and sharing the resources while maintaining the integrity of data. To ensure the level of user's confidence in the shared data, we proposed a one strong algorithm for integrity auditing by multiple users. Different solutions have been proposed to modify data and get integrity assurance, but far from the practical implementation and heavy cost of computation and communication. The proposed scheme can resist the attack and can find unwanted behaviour during transmission or on the server. The proposed technique is covering all the user's actions and generating time to time report to each and every user to maintain the trust and assuring the integrity of data.

Keywords: Cloud Computing; security; data integrity; integrity verification

I. INTRODUCTION

Public Cloud application and the requirement of cloud storage increased rapidly, and on the same pace number of users are accessing and modifying the data. Real world examples of cloud are drop box, Sugarsync, Dropbox in which multiple users are accessing the data and modifying the same file anywhere anytime on the cloud. For efficient implementation of this type of mutual applications, data integrity becomes the major challenge. Modifications done by different users must be authentic and data should be intact and up to date after the operations.

Cloud storage platforms may deal with the number of problems

1) Hardware / software failure
2) Malicious attack
3) Human errors/ intentional data leakage

As from the last observation done, we found out that the errors reported by the cloud service provider were very less than the actual errors occurred. Some of the data loss or data leakage was not reported by the server due to their reputation and financial constraints. Somehow we believed on external entity and assuring that it was providing the security of our data. That external entity could be called as Third party. TPA is giving the assurance of the data over the cloud[12].

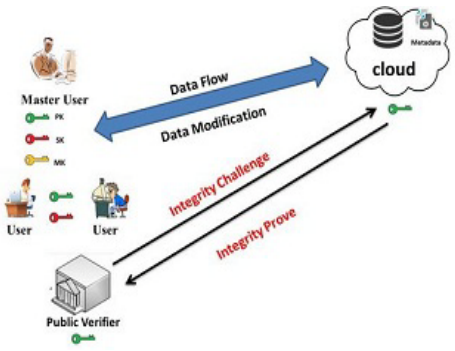

Figure 1. Integrity Basic Model

A number of private key algorithms were designed which provides the assurance that only the user having the private key was liable to modify the data. These solutions were working with the existence of the data owner, clients should be online for tracking the modification done by different users and maintain the logs of each. After commit of all adoptions, only the data owner will decide whether the data should be updated or not. So the results of this scheme were overburden and increasing the computation cost as well as have to make the record of each and every transaction in log file[15]. With multiple users the size of the log was increasing proportionally as their users were increasing day by day and dependency of users were also increased on the cloud resources.

II. RELATED WORK

This section deals with the works related to the cloud architecture and the security techniques adopted and used by cloud. As the higher availability of bandwidth and low cost network devices makes the increases the usage of internet at peak level. Depends on the centralized data over the network was increasing day by day. Hence, building of secure cloud storage was the major challenge in public cloud infrastructure.

The first proposed solution to remote data integrity was proposed by deswarate et al. [6] Uses RSA based hash function and applied it on the whole data for generating the verification challenge. For larger data files, this technique was inefficient. Carroni proposed another protocol where the server had to send the message authentication tag of the data as the response of challenge message and reduces the computation and storage overhead. For dynamic verification of data. Wang et al. [9] Discussed the problem of reliability and integrity of data and used the homomorphism and token based correcting codes for providing the security of data.

Yuan et al. [1] Allows multiple users to modify data with integrity assurance and worked on collusion attacks to provide an efficient integrity auditing scheme.

III. TPA MODEL USED FOR INTEGRITY VERIFICATION

The Third party auditor was a kind of supervisor. The TPA assured the client that the data stored in the cloud were under

his observation and client should not bother about the integrity of data. He knows the best practices and protocols that reduce the risk of keeping data in the cloud[2]. It generated a report in interval of times to help the user with analysis of data. Different protocols were designed by researchers time to time to make the TPA auditing more secure and reliable. We also tried to enhance the performance of TPA with the generation of few new initiatives and stronger algorithm that will reduce the storage and computational cost

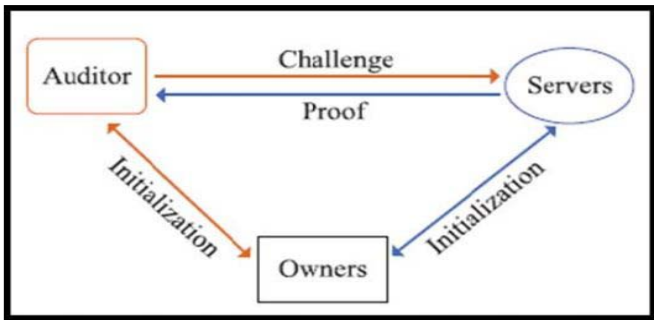

Figure 2. Role of Auditor

IV. ADOPTED SYSTEM MODEL

We considered the cloud system as the group of three different entities:-

1. Cloud server
2. Cloud client
3. Cloud certified channel

Cloud server will provide all the services and resources to users. Cloud clients are the users who are using the resources. The cloud client could be a single user or a group of users. Client is the owner of the data. With the proposed system, trying to resolve the multiuser modification of shared data in a group as well[14]. Cloud certified channel is the entity, which is dealing with assurance of server and client and do registration of all the clients who wants to access the services of cloud server[10]. Cloud certified channel will try to catch the a data corruption/ unwanted modification of data during auditing process and acknowledge to the data owner or group users.

Data can be uploaded by any of the client who is having the privileges. File processing algorithms will work on the client side or with the master user for calculation of tag values for individual file blocks[9]. Every time when the modifications done by the users associated tag value will be updated simultaneously. The log file is maintained by a cloud server, which is keeping the record of each and every transaction and updating the copy of log time to time with the updating.

Table I. Roles & Entities

CS	Cloud server
CU	Cloud user
CC	Certified Channel
H (.)	Hash function
F	A data file that will be split into blocks
Mi	Data block of file F
Mij	A block element ofmi

A. *Challenges*

1. To find the a secure and strong key for encryption and decryption as well as for generating the authentication tag
2. To update the log file with each of the operations done on the cloud server data
3. To reduce computation and communication overhead of file processing and key generation

B. *Scenario of the environment*

We assumed e P number of users Up where 0< p<n-1 in a group accessing data saved on the cloud and you is the master user and owns the data and handle the membership of the group. Every group member can access and edit the data saved over the cloud. The process is divided into a number of sections[5].

V. SETUP PHASE

This phase is divided into two parts. First is key generation and second is file processing. In key generation part proposed system will generate a secret key for the client and the owner of the data. Random generation of secret key will help the owner to make the system more secure[8]. In File processing phase an individual file will be divided into a number of blocks. Data owner also maintains a log file for keeping the record of the data stored in the block

In the case of updations performed on the shared data by the group users[9]. Users have to calculate the authentication tag value for each data block updated with his own secret key and upload the data block and tag value of the cloud. Now the main issues go with the size of log file how much space is required for storing the log file corresponding to complete file size.

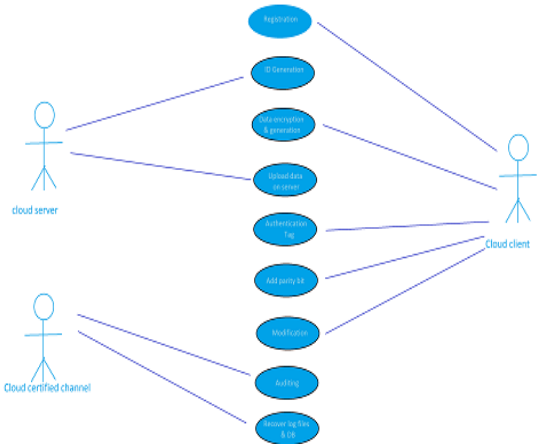

Figure 3. UML Diagram Of Setup Phase

Challenge: -Any of the group user or client can send the challenge message to the cloud by running the challenge algorithm. This challenge algorithm is used for auditing of data over the cloud

Proof: - On getting the challenged message, the cloud will execute a proof algorithm to generate the proof information, Which proves the validity of data that is actually stores the demanded data file correctly

Verify: - Works on the bases of information provided by proof algorithm, The certified channel or client can verify the integrity of data

The complete adopted the architecture of the proposed system

1) Cloud client will get registered with cloud server and one cloud id will be issued to the client. This is a random generated id [11](so random key generation algorithm will work in backend)
2) The unique id of the client will be submitted to cloud certified channel by a cloud server which ensures the client registration.
3) Encryption algorithm will be applied on the client side and file is divided into small blocks. With the setup phase discussed above,[7] Secret keys will be generated and used for calculation of authentication tag. That authentication tag will be added to each block with parity information.
4) Now the cloud server will only save the cipher text only on its disk to avoid any type of data leakage.
5) Any of the client and Certified channel can generate the challenge message to challenge the integrity of data over the cloud. . Challenge algorithm is run by the particular entity to generate a challenge message and passed to the server.
6) Updating if any of the users want to update the data over the cloud then the user should have privileges and the decryption key to decrypt the data once the data is decrypted at the local machine and modification are done. Users calculate the authentication tag value of the updated block and make the changes in the log file maintained by certified channel[6]. Step three will be repeated for the modification / updating process
7) On receiving the challenge message the verifies algorithms are run by the server to verify the integrity of data and prove algorithm to generate the proof message to the user or group of users

Factors affecting the performance are listed as tgiven below[13].

1) Size of log file
2) Communication cost
3) Computational cost

VI. COMPARATIVE ANALYSIS

Set up process having no influence on real time verification performance. Splitting of file into equal no of blocks and generating a security key for producing authentication tag for individual blocks. EXP and MUL operations are used to generate the public, master and secret key. And its performance depends upon the number of elements in the block and the number of users in the group

In updating process, every time user has to generate the authentication tag for updated file and do parallel modifications for the changes in the log file. Size of log file is also increasing as the changes done in authentication tag

A. Proposed system analysis

With implementation of the proposed system in real time cloud environment with Vsphere suite and results obtained are found more efficient than the previous one. Three different parameters are considered for results[4].

Less storage is required: - With the proposed methodology space required for storing the data is very less compared to previous one. Data is split into a number of shares so minimum size of cloud space can be used for storing heavier applications. Again, it depends on the data split ratio chosen by our system

Bandwidth utilization: - Instead of having the larger size, bandwidth, lower bandwidth with different channels can be utilized for transmissions. One third of the required bandwidth can be utilized efficiently[3].

VII. RESULTS

As proposed system is analyzed with different file size and number of parameters in different scenarios, proposed algorithms generating results which are presented in the graphs below

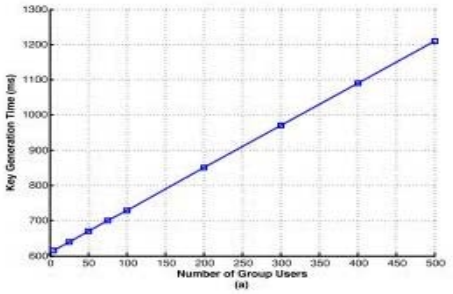

Figure 4. Key Generation Time

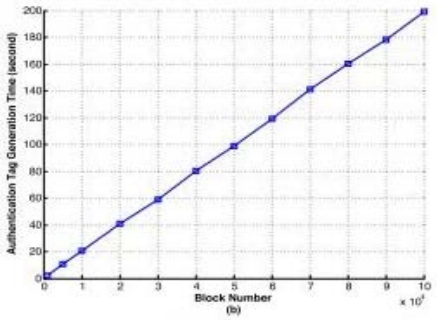

Figure 5. Authentication Tag Key Generation Time

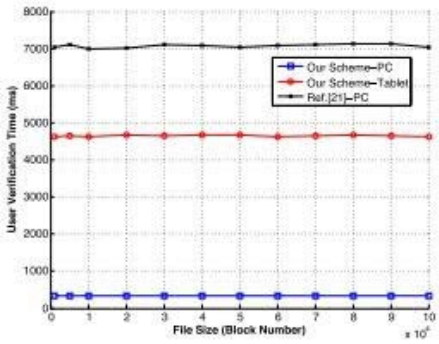

Figure 6. User Verification Time On Different File Size

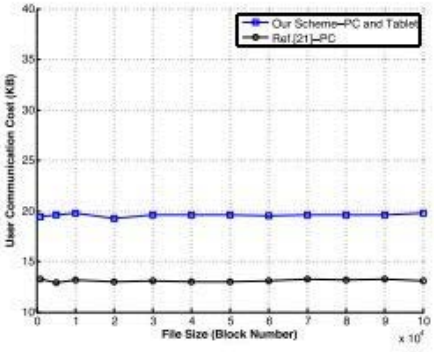

Figure 7. Communication Cost on Different File Size

According to our system model we calculated the cost of computation at different levels to calculate the different cost levels key generation time which is much stronger and taking very less time. Cost of calculating the authentication tag. The cost of updating the blocks by different client in a dynamic environment and how its affecting the authentication tag value which will be calculated every time. We also calculated the user verification cost at each level to make the system more secured and reliable

VIII. CONCLUSION

We adapted a new security system model to achieve security in term of integrity and enable the user to take advantage of this technology as much as possible. The proposed integrity checking algorithms eliminates the need of external party verification. The cloud client / user is dealing with the cloud server and all of the computation is done at the client level. The entity Certified channel managing the data integrity and evaluation using proposed algorithm. It provides a better protection approach in terms of filtering or risk management. The main advantages of the proposed model are that all the computation will be done at the client node and all the storage will be done at the server side. So the storage requirements and maintenance on the client side will be reduced.

IX. REFERENCES

[1] J. Yuan and S. Yu, " Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. 33rd Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM), Toronto, ON, Canada, Apr. /May 2014, pp. 2121–2129.

[2] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud computing research and development trend", in Second International Conferenceon Future Networks, January 2010, pp. 93-97.

[3] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition" ACM SIGCOMM Computer Communication Review. Vol. 39, no. 1, pp. 50-55, January 2009.

[4] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges", in the 24th IEEE International Conference on Advanced Information Networking and Applications, April 2010, pp. 27-33.

[5] Dropbox for Business. [Online]. Available: https://www.dropbox.com/business, accessed Apr. 24, 2015.

[6] DeswarteY.Quisquater j, saidane "A Remote Integrity Checking," Proc. Conference on Integrity and Internal Control in information system/////9IICIS '03') November 203, Switzerland.

[7] Caronni G. Waldvogel M. " Establishing Trust in Distributed Storage Provider", In Third IEEE P2P conference Linkoping03, 2003

[8] A. Behl, "Emerging security challenges in cloud computing: Aninsight to cloud security challenges and their mitigation", IEEEWorld Congress on Information and Communication Technologies,pp. 217-222, December 2011.

[9] Concurrent Versions System. [Online]. Available: http://cvs.nongnu.org,accessed Apr. 24, 2015.

[10] Amazon EC2 and Amazon RDS Service Disruption. [Online]. Available: message/65648 /, accessed Apr. 24,2015.

[11] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007,pp. 584–597.

[12] G. Ateniese et al., "Provable data possession at untrusted stores,"in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007,pp. 598–609.

[13] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. PrivacyCommun. Netw. SecureComm), 2008, Art. ID 9.

[14] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT),Melbourne, Vic., Australia, 2008, pp. 90–107.

[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in Proc. 17th IEEE Int. Workshop QualityService (IWQoS), Charleston, SC, USA, Jul. 2009, pp. 1–9.