Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.55 – 60

An Efficient Out Sourcing Computing System Using Cloud Storage

Shital Hemant Umale, Mahip M. Bartere
P.G. Student, Computer Science Department, GHRCE, Amravati University, India
Asst. Professor of Computer Science Department, GHRCE, Amravati University, India

Abstract: Cloud computing has become a very popular buzzword. Nowadays most of the business depends on the cloud, it realised as a pillar for IT industry. The most obvious advantage from the utilization of cloud computing systems and technologies is cloud computing is that the most value economical technique to use, maintain and upgrade. Because of this increasing economic condition with minimum maintenance & operational costs regarding IT software and infrastructure. By exploitation cloud storage, users store their information at remote location, information will delivered to the user on-demand for high-quality applications and services. Cloud storage is nothing but massive shared configurable computing resources, which will minimize the burden of native data storage and maintenance on the user. The cloud has modified the manner of application software and databases are stored has. Now days they are stored in cloud data centres by exploitation storage servers. The most important concern in cloud information storage is that the security of the information that is stored on cloud. The new phenomenon that is used to store and manage data without capital investment has brought several security challenges that don't seem to be completely understood. This paper focuses on the security and integrity of data keep in cloud data servers. The data integrity verification is completed by employing a third party auditor who is permitted to check integrity of data sporadically on behalf of client.

Keywords: data storage, privacy preserving, public auditability, cloud computing, cloud service provider (CSP),TPA(Third Party Auditor),CSS(Cloud Storage Server).

I. INTRODUCTION

Cloud computing is one among the most modern technical topics nowadays, it's broad-ranging effects across IT, information design, Business, software Engineering, and data Storage. Cloud Computing is a pioneering technology that is revolutionizing the approach we do computing. Cloud Computing is an internet based technology that uses distant servers to preserve data and applications. Cloud computing permits clients and businesses to use different applications while not installation and access their personal files at any location with internet access. This technology permits for more efficient computing by centralizing data storage, processing and bandwidth. This Cloud computing technology usually has 3 segments: "Application", "Data Storage Space" and "Connectivity." every section deserves a different a unique purpose and offers different products for businesses and

individuals around the world. These segments defined as cloud computing stack that is referred as software as a Service, Platform as a Service and Infrastructure as a Service. SaaS model is employed to deliver software applications above the web through that clients can use the software application. PaaS is the model that delivers hardware also the set of tools and services designed to enable coding and deploying those applications quickly and efficiently. IaaS provides various infrastructure elements like servers, storage, networks, and operating systems needed for the application Cloud computing has become a very common buzzword. Nowadays most of the business depends on the cloud, it realized as a pillar for IT industry due their essential characteristics like on-demand self-service provisioning, broad network access, fast elasticity i.e. scale in and scale out capabilities. Among the various services provided by the cloud is cloud data storage. This enables the client (Data Owner) to move the content on remote data store therefore relive the burden of local data storage on the client. Although this new data storage paradigm visualised as a promising service platform for the internet, it brings about several challenging design problems which have intense influence on the security and performance of the overall system. Data outsourcing in cloud has 2 vital problems security & integrity. Security is related to preserve the privacy of the data i.e. avoid unauthorized data access. While integrity maintains the data correctness. Our project has primarily concentrate on these 2 problems regarding cloud data.

The concept of public auditability used to check the data integrity. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is truly relinquishing user's ultimate control over the destiny of their data. As a result, the accuracy of the data within the cloud is being place at hazard because of the subsequent reasons. Firstly, although cloud infrastructures is much more powerful and consistent than personal computing devices, still they are facing the broad range of each internal and external threats for information integrity. Secondly, {there is chance that because of numerous motivations for CSP to behave unfaithfully toward the cloud users concerning their outsourced information status. For examples, CSP could rescue storage for economic reasons by discarding information that have not been or are seldom accessed, or maybe hide data loss incidents to maintain a reputation. Due to these reasons data owners would worry that the data could may be lost within the cloud. Thus, enabling public auditability for cloud storage is of important importance in order that users will resort to a third-party auditor (TPA) to examine the integrity of outsourced data and be worry free.

II. OBJECTIVES OF THE PROPOSE WORK

There are following objectives & motivations of the proposed work

1) Public verification for storage correctness assurance:

To There are following objectives & motivations of the planned work permit anyone to perform auditing, not just for the clients that have originally stored the file on cloud servers. Public auditing capability allowed on demand for verification of the correctness of keep in cloud.

2) Dynamic data operation support:

Clients will perform dynamic block level operations on the data files like insert, delete, update, whereas maintaining correctness of data files within the cloud .The design of system should be as effective as possible for assure the consistent integration of public verifiability and dynamic data operation support.

3) Blockless verification:

The challenged file blocks for data verification mustn't be retrieved by the verifier (e.g., TPA) throughout verification process for both efficiency and security considerations.

4) Stateless verification:

Verifier need not maintain the state information throughout the auditing process. Stateless verification will remove the need for state information maintenance at the verifier side between audits throughout the long term of data storage.

5) Batch Auditing:

Auditing will be perform for the batch of users i.e. Multi- User auditing will be supported by TPA in cloud environment.

III. EXISTING SYSTEM

In the existing system, outsourcing the data means user in fact relinquish important management over the fortune of their data & it is in hand of CSP. The traditional cryptographic technologies used for data integrity and accessibility, cannot work properly on the outsourced data. it is not a helpful solution .for data justification by downloading them due to the valuable communications, particularly for big size files. For securely establish an efficient third party auditor (TPA), there are following 2 basic needs need to be met:

1) TPA should be capable to with efficiency check (audit) the cloud data storage without demanding the local duplicate of data, and it will not place an extra on-line burden to the cloud user.

2) The third party auditing process mustn't bring any quite new vulnerabilities towards user data privacy.

The existing system, the information correctness within the cloud is being place in danger because of the following reasons. Though we expect that the infrastructures within the cloud are much more dominant and trustworthy than personal computing devices, they are facing broad range of both internal (loss or destruction of data) and external (disclosure of data to unofficial users) threats for data integrity.

Drawback of the existing system

1. Cloud Storage system provides the user for safe and consistent place to save important data and documents. However, in some cases user's files are not encrypted before store on some open source cloud storage systems. I.e. TPA demands retrieval of user data, here actual privacy is not preserved.

2. The storage service supplier i.e. storage server can effortlessly access the user's files. This brings a big anxiety concerning user's privacy. The user has no ultimate control over the software applications including secret data. User has to totally rely upon the suppliers for maintenance and administration.

IV. PROPOSED SYSTEM

This section presents the architecture of planned system that overcomes the drawbacks in the existing system. proposed system are able to do the public auditing that permit the TPA to verify accuracy of information without retrieving local duplicate of the data . It also conserve the privacy by applying encryption scheme. The auditing scheme also support batch auditing that permit the TPA to use the audit for multiple clients. To support expert handling of many auditing tasks, this work additional explore the technique of bilinear aggregate signature to extend the main result into a multiuser setting, wherever TPA will perform multiple auditing tasks at the same time. Wide security and performance examination show that the projected scheme is very efficient and provably secure. The subsequent figure shows the system design of planned system. The cloud storage consist of 3 different entities Cloud client, Cloud Storage Server & TPA (Third Party Auditor).

• Cloud Client: This entity has large quantity of data, which will store on cloud storage server.

• TPA (Third Party Auditor):-This entity will work on the behalf of the client, which is responsible for checking integrity of the outsourced data.

• Cloud Storage Server:-Cloud Storage Server is that the location wherever, user store their data.

V. METHODOLOGY OF PLANNED SYSTEM

The public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, and VerifyProof). KeyGen is a key generation algorithm that's run by the user to setup the scheme. SigGen is used by the user to get verification metadata, which can contains digital signatures. GenProof is run by the cloud server to get a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof. Running a public auditing system consists of {two|2} phases, Setup and Audit: {1|one}. Setup phase: The user initializes the public and secret parameters of the system by execution of KeyGen, and pre-processes the data file F by using SigGen to get the verification metadata. The user then stores the data file F and the verification metadata at the cloud server. The user might alter the data file F by performing updates on the keep data in cloud.

2. Audit phase: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has preserved the information file F properly at the time of the audit. The cloud server will produce a response message by

executing GenProof exploitation F and its verification metadata as inputs. The TPA then verifies the response by cloud server via VerifyProof.

VI. ALGORITHMS OF PROPOSED SYSTEM ALGORITHM

Algorithm 1: Key Generation (KeyGen)

Key Generation is a key generation algorithm running at the data owner side, which generates the secret key PKi upon getting input of some security parameter using AES algorithm. Input: File (F). Output: Private Key (PKi) [key is used for encryption and decryption mechanism.

1. Result = ValidateFormat (F);

ValidateFormat = {pdf .jpg ...}

2. If the format is valid then client want to secure the data using AES Algorithm.

CipherData (Fi) = AES (Fi);

Algorithm 2: Sign Generation (SigGen)

Sign Generation algorithm used to generate digital signature of the encrypted file partitions.

Input: File partitions (P1, P2, P3...Pn)

Output: Hash values of encrypted partitions (H1,H2...Hn)

1. MessageDigest md = MessageDigest.getInstance ("SHA");

MessageDigest is generic class used to provide the default functionality of the SHA-1 algorithm for the application. The getInstance () method generates the MessageDigest Object.

2. md.update (datArr, 0, datArr.length);

Updates method takes the input _le by appending a byte array at the end.

3. byte [] sha1hash = md.digest();

This method applied SHA-1 algorithm on current input message and returns the array of bytes.

4. Separate the first 4 bits of the particular byte i.e. MSB (Most Significant Bits) and convert then to character.

5. Separate the last 4 bits of the particular byte i.e LSB (Least Significant Bits) and convert then to character.

Algorithm 3: VerifyProof

Verify proof algorithm run by the TPA for performing the auditing task.

Input: Random File blocks

Output: Verification

Status 1. File Indices = getRandom ();

This method returns the random file indices and store in the vector array.

2. Result=updateLog ()

The updateLog method update the result of the verified partitions maintain the file status like file is safe or file is unsafe.

Algorithm4: Generation proof(GenProof)

This algorithm run by the cloud storage server for the possession of the data files.

Input: File

Output: Hash of the files

Result=GenProof (File, Chal) This method accept the challenge from TPA and send the proof of possession of the data files to the TPA.

VII. RESULT VERIFIED BLOCKS (BYTES)

Verified Blocks (bytes)	TPA Individual Audit time(ms)	TPA Batch Audit Time(ms)
3072	1014	921
3891	1154	1014
4096	1155	999
4505	1532	1045
5734	1632	1357

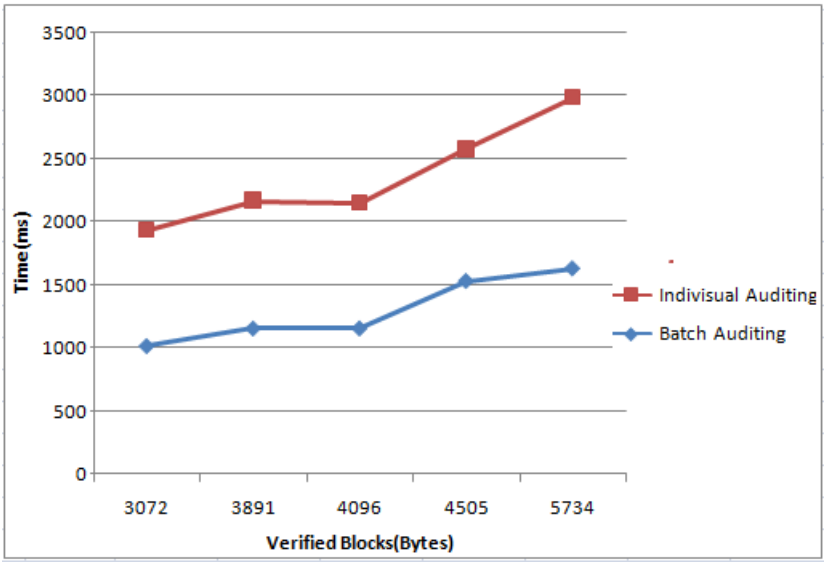

Figure 3: Comparison on auditing time between batch and individual auditing.

The Fig.3 shows the results for the auditing task. The number of auditing task & time required for auditing shown in the graph. The performance of the corresponding individual auditing is provided as a baseline for the measurement. Following the same settings for the data blocks of the file. The average per task auditing time, which is computed by dividing total auditing time by the number of tasks, is given for both batch and individual auditing. It can be shown that compared to individual auditing, batch auditing indeed helps reducing the TPA's computation cost, as more than 15 percent of per task auditing time is saved.

VIII. CONCLUSION

Use of third-party auditing service provides a cost-effective method for users to gain trust in cloud. We assume the TPA, who is in the business of auditing, is reliable and independent entity. In this paper, public auditing system is proposed for data storage security in cloud computing along with preserving privacy mechanism. It can utilizes the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage. Public auditing is able to allow clients for delegating the tasks of integrity verification to TPA while they are independently not reliable or cannot commit required

resources of computation performing 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. For achieving data dynamics that are effective, the existing proof of storage models is enhanced through manipulation of the construction of classic SHA-I for authentication of block tag. For supporting good handling of multiple numbers of auditing tasks, the method of bilinear aggregate signature is further explored for extending the main result into a multiuser setting, where TPA is able to perform multiple auditing tasks in a simultaneous manner. Huge security as well as performance analysis proves that the proposed scheme is efficient and secure to a greater extent. As the future work, efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor and also include the features to enable dynamic operations (e.g. inserting/deleting data block) in this system.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Comput- ing," technical report, Nat'l Inst. of Standards and Technology, 2009. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010K.
[3] Cloud Security Alliance, "Top Threats to Cloud Computing,"http://www.cloudsecurityalliance.org, 2010.
[4] 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.
[5] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[6] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.
[7] M.A. Shah, R. Swaminathan, and M. Baker, Privacy- Preserving Audit and Extraction of Digital Contents, Cryptology ePrint Archive, Report 2008/186, 2008.
[8] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, Auditing to Keep Online Storage Services Honest, Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS 07), pp. 1-6, 2007
[9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.
[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 Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847859, May 2011.
[11] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'01), pp. 514-532, 2001
[12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Storage Security in Cloud Computing," IEEE Transactions On Computers, vol. 62, no. 2, FEB 2013.
[13] Wang C, Wang Q et al. Privacy-Preserving Public Auditing for Storage Security in Cloud Computing, Proceedings IEEE INFOCOM'10.2010
[14] Wang B, Li B et al. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Conference on Cloud Computing, 295– 302.2012
[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.
[16] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

