International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 3 (March '2017)

DUAL CROSS VERIFICATION LAYER FOR CONTENT CONSISTENCY IN CLOUD COMPUTING

K.Ramiah Ilango,
Assistant professor,
Department of Computer Science and Engineering,
SBM College of Engineering & Technology,
Dindigul, Tamilnadu, India.

K.Jeya Aishwarya,
Student,
Department of Computer Science and Engineering,
SBM College of Engineering & Technology,
Dindigul, Tamilnadu, India.

N.Ananthi,
Student,
Department of Computer Science and Engineering,
SBM College of Engineering & Technology,
Dindigul, Tamilnadu, India.

M.Madhuvathani,
Student,
Department of Computer Science and Engineering,
SBM College of Engineering & Technology,
Dindigul, Tamilnadu, India.

Abstract: The U (User) sends the File F to Cloud server and disconnects the connection then U forms the META Data about F to PTV and SCV. The PTV and SCV manage the META data without the whole data storage to avoid the duplication. User demands the PTV and SCV to audit with correctness of Cloud server about F. The PTV and SCV starts with auditing by connecting with cloud using META Data. For cheating prevention META Data consists the Random Pin Approach. PTV and SCV use the thread fashion to manage the auditing for multi user demands with defined number of ways. Network Data computing involves three segments. They are user (U), who has large amount of data files to be stored in the Network Storage Server, the Network Cloud server (NCS), which is managed by cloud service provider (CSP) to provide data storage service. The system adds the fourth layer the PTV and SCV, who has expertise and capabilities that maintain the stability between cloud users, cloud data and cloud system.

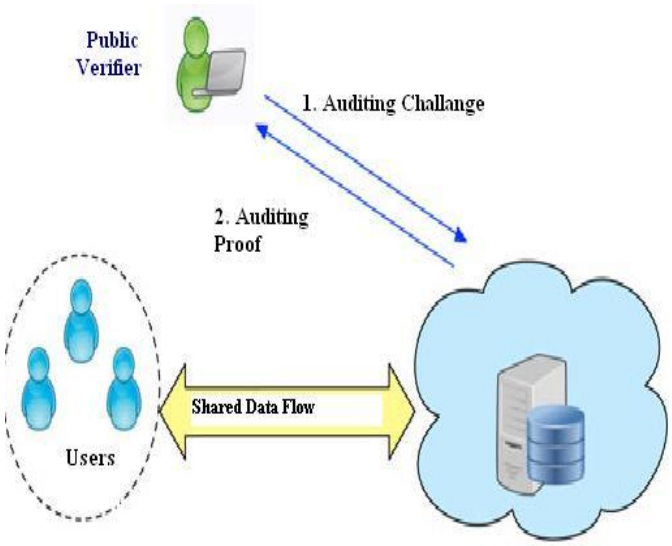
Keywords: PTV,SCV,META Data, RMI,RBA,GUI.

I.INTRODUCTION

Cloud computing and storage allow users are to access and share resources offered by cloud service providers at a lower marginal cost. It is routine for users to have cloud storage services to use data with others in a group as data sharing is unique feature in many cloud storage offerings. The integrity of data in cloud storage, subject to doubt and challenge, as data stored in the cloud can easily be lost or corrupted due to the inevitable hardware/software failures and human errors. The traditional approach for checking data correctness is to retrieve the entire data from the cloud and then check data integrity by checking the correctness of the entire data.

Cloud computing makes many advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Cloud service providers (CSP) are separate administrative entities where the data outsourcing is actually relinquishing user's ultimate control over the fate of their data. So in result, the correctness of the data in the cloud is being put at risk due to the following reasons. Even though the infrastructures under the cloud are more powerful and reliable than personal computing devices, still they are facing the broad range of both internal and external threats for data integrity.

The outages and security breaches of noteworthy cloud services are the best examples which appear from time to time. Second, there exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed, or even hide data loss incidents to maintain a reputation [8], [9], [10]. In short outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. If this problem is not properly addressed it may impede the success of cloud architecture [2], [4],[7],[12]. For managing easily, it is desirable that cloud only entertains verification request from a single designated party.



If the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and response protocol between a public verifier and the
cloud server [9].

The TPA, who has expertise and capabilities that users do not, it can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. In addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes [11]. Most of the existing schemes do not consider the privacy protection of user's data against external auditors [15], [16]. To solve the privacy issue on shared data, this paper discusses novel privacy retaining public auditing mechanism so that to verify the integrity of shared data by a public verifier without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier [1].

II.EXISTING SYSTEM

Cloud user sends the data to cloud, Cloud returns the confirmation message to user. But the user doesn't know whether the file is fully stored or not. Because sometimes the file does not send properly due to many reasons. As a disruptive technology with profound implications. Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc

Drawbacks: 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 network environment can be formidable and expensive for the users.

III. PROPOSED SYSTEM

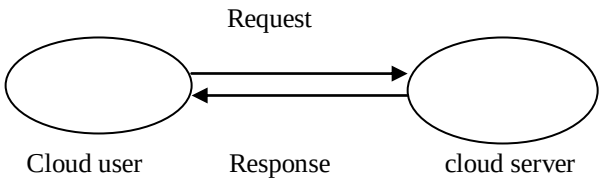
How to efficiently verify the correctness of outsourced cloud data without the local copy of data files becomes a big challenge for data storage security in network Computing. Therefore, to fully ensure the data security and save the users' computation resources, it is of critical importance to enable public audit ability for data storage so that the users may resort to a PTV and SCV , who has expertise and capabilities that the users do not, to audit the outsourced data when needed. Based on the audit result, PTV and SCV releases an audit report, which would not only help users to evaluate the risk of their subscribed data services, but also be beneficial for the service provider to improve their storage based service platform.

The U (User) sends the File F to Cloud server and disconnects the connection then U forms the META Data about F to PTV and SCV. The PTV and SCV manages the META data without the whole data storage to avoid the duplication. User demands the PTV and SCV to audit with correctness of Cloud server about F. The PTV and SCV starts with auditing by connecting with cloud using META Data. For Cheating prevention META Data consists the Random Pin Approach. PTV and SCV uses the thread fashion to manage the auditing for multi user demands with defined number of ways.

Benefits Of Proposed System: Network Data computing involves three segments. They are user (U), who has large amount of data files to be stored in the Network Storage Server, the Network Cloud server (NCS), which is managed by cloud service provider (CSP) to provide data storage service. The system adds the fourth layer the PTV and SCV, who has expertise and capabilities that maintain the stability between cloud users, cloud data and cloud system.

III.CLIENT SERVER IMPLEMENTATIONS

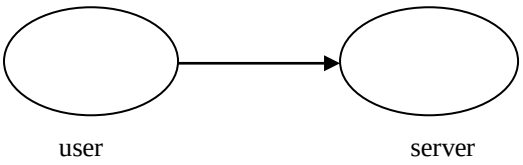
PTV and SCV has default validation setup and the PTV and SCV starts after the admin name and admin password verification. Cloud also have the default password setup, after the cloud startup, the user can upload the data to cloud. User should register with PTV and SCV to upload the file with Cloud after the login process with PTV and SCV. There are three segments available in this system. The segments are started using proper authentication. Each one startup provides the appropriate home page. Validations are involved in the setup to control the admin in null and invalid values. Swing based GUI designs are developed to accomplish this scenario.



Server Data Communication by User In Network: The system has been divided into four segments. One of the segments is Cloud. In our system Cloud Server is the RMI server with the defined functionalities. When the system starts Cloud Server, the server can be known as Cloud server. After the startup, the Cloud Server Listener listens the client request at specified portno. Client can send the files to Cloud System then The CS receive the file information and store in its persistence and file storage. Data will be sent to CS as byte array format by RMI network connectivity. The byte array format is the collection of bytes of file content in sequence file stream. The CS manages the byte array as the

file. After that storage, The server shows the report about the file storage. Te system connects PTV and SCV to provide the META data about file. The cloud accepts the files from user. Only registered users can upload the files. This is Gen Proof for this purpose Cloud communicates with PTV and SCV for the user validation. User system automatically generates the Meta info about the uploaded file to PTV and SCV. CS by default manages the Service list to share the files to clients.

User and server communicated with RMI



Meta Verification Management With (Rpa) Random Pin Approach: Meta data is a data about uploaded file. The user system automatically generates Meta data with Word Bytes Sequence Logic. The logic creates the random walk in file to generate the pin with place in byte order. This is the keygen process The Meta data will be stored in PTV and SCV without store the full content in PTV and SCV. PTV and SCV acknowledges the user about the received Meta data, means Meta data matching with user info. It is SigGen. The data is the random walk of file data developed and passed to PTV and SCV. The data are the byte values with key pair segments. Key is the place of data and value is the data. The PTV and SCV collects the data and manages in its persistence for future comparisons.

Parallel Connectivity by Ptv And Scv To Cloud: PTV and SCV makes the parallel approach to cloud to verify the user uploaded data with Meta Data. To do this we make three level parallel approaches. It can increase in future. It means the three different processes are started and each process has the Meta data to compare with Cloud data. First PTV and SCV finds how many users are found in file group to accomplish the parallel connectivity instead of single way finder. Based on parallel approach, the PTV and SCV starts multiple threads means each one user segment will have each one thread. PTV and SCV collects user files as file map. Each one thread sends File Map Meta data to cloud and verifies the cloud storage to get the data storage reliability and accuracy.

Verification Process Implementations: After the successful verification, the PTV and SCV alerts the user about verification report. If successful result, The PTV and SCV signal deletes the user file automatically with the confirmation of user. The invalid results protect the file from user side with the safe message to user. This is the verify proof. PTV and SCV collects the file storage information and maintains the success list and failure list. The success list contains the information about successful storage files list and failure list contains the information about failure files. The list will be maintained for each one user level. After the user demand the list will be sent to user and user can delete the file in its memory if successful storage is done

IV.PUBLIC AUDITING SCHEME ALGORITHMS

Public auditing scheme provides a complete outsourcing solution of data with data integrity check. A public auditing scheme consists of four algorithms(KeyGen, SigGen, GenProof, VerifyProof).

1. KeyGen – It is a key generation algorithm that is run by the user to setup the scheme.
2. SigGen- It is used by the user to generate verification metadata, which may consist of digital signatures.
3. GenProof- It is run by the cloud server to generate a proof of data storage correctness.
4. VerifyProof – It is run by the TPA to audit the roof.

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. Then user stores the data file F and the verification metadata at the cloud server, and deletes its local copy. In the preprocessing part 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. By executing GenProof using F and its verification metadata as inputs the cloud server will derive a response message. Then TPA verifies the response via VerifyProof.

V.CONCLUSION

This paper discusses a Dual cross verification layer for content consistency in cloud computing. There are two techniques are used this method PTV AND SCV. It is mainly used to reduce the server work burden. The PTV and SCV mange the META data without the whole data storage to avoid the duplication. This paper also discusses the different security and performance challenges such as the dual cross verification layer, batch auditing.

VI.REFERENCES

[1]. Cong Wang, Sherman S.M. Chow, Qian Wang,Kui Ren, Wenjing Lou," Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS VOL. 62, NO. 2, FEBRUARY 2013

[2]. 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.

[3]. 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. 847-859, May 2011.

[4]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[5]. Cloud Security Alliance, "Top Threats to Cloud Computing,"http://www.cloudsecurityalliance.org, 2010.

[6]. C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[7]. P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," 30Thttp: //csrc.nist.gov/ groups/SNS/cloud computing /30T index.html, June 2009.

[8]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc. 15th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT), pp. 319-333, 2009.

[9]. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," 30TUhttp://www.cloudsecurityallianceU30T. org, 2009.

[10]. 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, "Above the Clouds: A Berkeley View of Cloud Computing, "Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[11]. K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High- Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009.

[12]. Amazon.com, "Amazon s3 Availability Event: July 20, 2008

[13]. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy- Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[14]. 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.

[15]. 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