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

Flexible and lightweight Storage Auditing Mechanism in Cloud Computing for dynamic operations

Suresh Arangi
M.Tech(Computer Science and Engineering),
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

Jayanthi Rao Madina
Head of the Department,
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and Mangement, Srikakulam.

Abstract:

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

To maintain the data securely in distributed environment i.e., on clouds we propose an effective and flexible distributed scheme with Token Generation algorithm for data files checking as a secure and dependable cloud storage service. A new scheme was introduced to encrypt with the user specified key parameters to make the resource more robust. We are also proposing allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of hacker information. And securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing.

We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

Keywords:

Cloud, Private Cloud, Security, Secure data Transmission, dependable distributed storage, error localization, data dynamics.

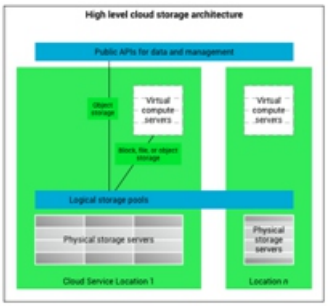
Introduction:

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service (Amazon S3) or deployed on-premises (ViON Capacity Services) Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Cloud storage is:

- Made up of many distributed resources, but still acts as one - often referred to as federated storage clouds.
- Highly fault tolerant through redundancy and distribution of data.
- Highly durable through the creation of versioned copies.
- Typically eventually consistent with regard to data replicas

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



Advantages:

• Companies need only pay for the storage they actually use, typically an average of consumption during a month. This does not mean that cloud storage is less expensive, only that it incurs operating expenses rather than capital expenses.

• Organizations can choose between off-premises and on-premises cloud storage options, or a mixture of the two options, depending on relevant decision criteria that is complementary to initial direct cost savings potential; for instance, continuity of operations (COOP), disaster recovery (DR), security (PII, HIPAA, SARBOX, IA/CND), and records retention laws, regulations, and policies.

• Storage availability and data protection is intrinsic to object storage architecture, so depending on the application, the additional technology, effort and cost to add availability and protection can be eliminated.

• Storage maintenance tasks, such as purchasing additional storage capacity, are offloaded to the responsibility of a service provider.

• Cloud storage provides users with immediate access to a broad range of resources and applications hosted in the infrastructure of another organization via a web service interface.

• Cloud storage can be used for copying virtual machine images from the cloud to on-premises locations or to import a virtual machine image from an on-premises location to the cloud image library. In addition, cloud storage can be used to move virtual machine images between user accounts or between data centers.

• Cloud storage can be used as natural disaster proof backup, as normally there are 2 or 3 different backup servers located in different places around the globe.

EXISTING SYSTEM:

In existing system, the importance of ensuring the remote data integrity has been highlighted by the following research works under different system and security models. These techniques, while can be useful to ensure the storage correctness without having users possessing local data, are all focusing on single server scenario. They may be useful for quality-of-service testing, but does not guarantee the data availability in case of server failures. Although direct applying these techniques to distributed storage (multiple servers) could be straightforward, the resulted storage verification overhead would be linear to the number of servers.

PROBLEMS IN EXISTING SYSTEM:

• However, while providing efficient cross server storage verification and data availability insurance, these schemes are all focusing on static or archival data.

• As a result, their capability of handling dynamic data remains unclear, which inevitably limits their full applicability in Server storage scenarios.

Proposed System:

In our proposed work the framework contains safe upload and retrieving of data upload. In our framework there are four main features such as file encryption, file upload, file decryption, and file download. There are three types of users such as data owner, Auditor and user. Data owner initially selects file and generates transformation key to encrypt selected file.

After that data owner encrypts the selected file and generates signature for encrypted file. He sends Meta data to auditor such as file index, file name, and signature. Auditor is the trusted authority of the cloud service provider. He frequently verifies files in the cloud service using the Meta data sent by the data owner.

He can send status of the verification such as auditing to data owner using simple mail transfer protocol. In this verification auditor again generates signature to the file in the cloud and compares with the signature sent by the data owner. If the signatures are same the file in the cloud service is secure otherwise he decides that file was corrupted.

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

User view list of files and request to cloud service, cloud service checks authentication and sends decrypted file to download the requested file. In our work we introduced a block based signature algorithm to generate signatures. In we divide the encrypted file into equal number of blocks. And generate signature to each and every block of the divided file. A novel algorithm for signature generation.

Algorithm: Generate file with Signatures

Input: User File in ASCII (Fo)

Output: User File with Signature appended at end of (Fn)

Method:

In order to apply hash function on each n byte block of file we perform the following steps to make (m mod n)= 0 of Fo:

M – Calculate length of uploaded file

n -- length of block such as 128/256/512/1024

Divide Lo into the given block length BL
Block=Lo/BL
If there any remaining bits append zeros rounded to block length BL
Then For each block B={b1,b2...bn}
Encrypt block
Benc=DES(b)

Then for each Encrypted Block generate signature

For j - I to count

S <- 0
S+ = reverse[ΣnA=1 ((A + B) || (A- B))]

B *- to_Integer (to_Char (A))
Signature ---- Signature+ to-Binary (S)
Fn ----- F1+Signature

In order to accomplish this task we have devised an algorithm which uses file signature method to identify the exact location of error. A new file signature strategy is proposed in this paper to know the exact location of error. We call this file technique is block based signature algorithm.

The above algorithm generates signatures against the data in file and appends those generated sign9atures at the end of file. It is very obvious from the algorithm that this algorithm generates signatures for every block separately and then those signatures are appended at the end of file as well. Block size in this algorithm (n) is dependent upon the preference of users. We have performed testing of our technique represented later, in order to identify the best suitable block size for our technique. The method of identifying corruption at the receiving site uses the similar technique. The algorithm at receiving site first identifies the actual size of the file received. Then it separates the signatures from the received file. Then it separates the signatures from the original data with appended zeros and 16 reserved bytes

One very strong point about the proposed algorithm is that it first divides the whole file into blocks of equal and stored in the servers. It means that the number of blocks in the file is exactly equal to the number of the unique block of data. The receiving site generates signatures of the file received after removing sending site signatures from the file. The signatures generated at sending site are then matched against the signature match is found, it means that the block is received accurately. Otherwise the block is not received accurately. This technique makes up capable of identifying the exact blocks which are received corrupted. After the identification of corrupted block the third party auditor will store the corrupted block into the cloud server.

Related Discussion:

Before file is distributed to the cloud, TPA will generate token key with required parameters passed by user. once the token key has been generated, TPA will send the file by dividing the file into equal sized blocks and generate a small token signature for each block along with initial key file token .This file Token was generated based on mathematical calculations with hash based technique, It is fully randomized we are not explore the operations present in it and just given the function split(X). Before sending the block it stores the computed signatures obtained from bit permutations on both file Token and block data .The resultant token was stored in its database or at clients place. Each block is send along with short signature and each block is treated as encrypted block.

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

Cloud will perform the same operation and checks whether the given block is same or not when computed and checks with the signature. If it matches the same, cloud server store each block and acknowledges the newly generated signature to TPA.TPA verifies the signature with the existing signature, if it matches TPA will send next block otherwise it assumes that block was not saved successfully or it may effect to attacks and resend the same block.

The tokens of each block which we were generated using precomputation algorithm has been stored in the database. Now we are using homomorphic technique to retrieve entire file or required blocks dynamically. Once user has been sent the requested file to TPA. TPA monitors whether he is authenticated user or not for accessing the file. TPA maintains the file details and tokens (if TPA is not present user will have the details) but not an entire file, TPA requests the file by passing the pre-computed token stored in the database for each block. If this token is same as it is present in cloud server, cloud server will send the requested blocks.

We can easily check whether the file blocks were damaged or not by computing tokens dynamically as follows: When TPA challenges or requests a block with block indices, cloud server receives this input and it computes the token of that particular block and sends the short signature to TPA. Upon receiving the signature TPA verifies it with the existing token signature. The result of two tokens are same means the block remains same without any effect, otherwise TPA assumes block was modified and it generates a message to cloud server to perform block recovery operation using distributed schemes and erasure coded techniques.

CONCLUSION :

In this paper, we ensure that the data which was sent to the cloud servers(CSP) are acknowledged by generating the token dynamically . We will combine the data file with file tokens to send the file from cloud client to TPA. Block storage on clouds will give better performance and we can easily distribute the blocks to different cloud servers for more data availability . Block modifications can be easily done simply by calling each block with indices along with the token

REFERENCES:

[1] Cong Wang; Qian Wang; KuiRen; Ning Cao; Wenjing Lou; , "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220-232, April-June 2012.

[2] Towards Secure and dependable storage service in cloud computing by congwang , Qianwang, KuiRen , Ning Cao, Winjing Lou,2011 .

[3] "Ensuring Data Storage security in cloud computing" by C Wang , Q Wang 4.) "Auditing to keep online storage service honest " by M.A. Shah , R Swaminathan.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[5] 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.

[6] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, http://eprint.iacr.org, 2008.

[7] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (Secure Comm '08), pp. 1-10, 2008.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf.Theory and Application of Cryptology and Information Security:

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

Advances in Cryptology (Asiacrypt '08), pp. 90-107, 2008.

[11] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 20

BIOGRAPHIES:

Suresh Arangi

student in M.Tech(Computer Science and Engineering) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his MCA-Aditya Institute of Technology & Management,K.Kotturu ,Tekkali. His interesting areas are Data Mining, Networking.

Madina Jayanthi Rao

working as a HOD of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He is pursuing Ph.d at KRISHNA UNIVERSITY Machilipatnam in computer science. He received his M.Tech (CSE) from Aditya Institute of Technology And Management (AITAM), Tekkali. Andhra Pradesh. His interest research areas are Data mining, Image Processing, Computer Networks, Distributed Systems. He published 12 international journals and he was attended number of conferences and workshops.