IJCSEC- International Journal of Computer Science and Engineering Communications.
Vol.3, Issue 3, 2015, Page.1013-1020, ISSN: 2347–8586

Auditing Protocol for Secured Data Storage in Cloud

[1]B. Sunitha, [2]K. Suresh Babu
[1]PG Scholar, [2]Assistant Professor
Department of Computer Science, St. Peter's University, Chennai, India,
[1] sunithababu04@googlemail.com, [2] sureshstudy2010@gmail.com

Abstract

On cloud servers the data are hosted by the data owners and the data are accessed by the users from the cloud servers in cloud computing. As the data are outsourced, there are new security challenges been introduced by the new data hosting service that requires an independent auditing service in cloud to check the data integrity. There exist few remote integrity methods used for checking which can only serve for static archive data and hence cannot be applied to the auditing service as the data in the cloud can be updated dynamically. Thus, a new dynamic protocol which is secure and efficient is designed in order to make data owners believe that in cloud, the data are stored correctly. In this paper, first design a framework which would audit the data stored on the cloud servers and then a protocol which would be efficient in preserving the private data of the data owners.. The auditing protocol is extended to support the dynamic data operations, which is provable secure and efficient in the random oracle model. Also, the auditing protocol is extended to support batch auditing for multiple owners, without using any trusted organizer. The simulation and analysis results show that the proposed auditing protocols are efficient and secure, especially it reduces the computation cost of the auditor.

Keywords*: Auditing Service, Remote Integrity, Dynamic Auditing Protocol, Batch Auditing, Data Dynamic Operations, Privacy, Cloud Computing, Access Control.*

1. Introduction

The important service of cloud computing is cloud storage wherein the owners of data can move data to cloud from the local computing device. Day by day more owners started to store the important data in the cloud. However, this is a new paradigm in which the data hosting service introduces new challenges in data security. There is a chance of losing data which worry the owners of data. The loss of data would happen in any infra structure even there are very high reliable measures in place by the cloud service providers, can be due to dishonest service providers. The cloud service providers could remove the data from the cloud which are very rarely accessed in order to save the cloud storage space, however the data owners would still believe that their data are in cloud. Owners need to be convinced that in cloud, their private data are stored correctly.

In cloud storage, it is inappropriate for the auditing to be performed either by cloud service providers or owners of the data to perform any auditing as both of them could be biased in providing auditing result. In such situation, were the data owners and service providers are not trustable, the choice would be third party auditing which assures the confidentiality of the data. A third party auditor can be more efficient as the TPA has the necessary expertise and capabilities in order to convince the owners and cloud service providers.

Fig. 1: Storage structure in cloud

The cloud storage service (CSS) mitigates the load of maintenance and storage management. However, if such a significant service is weak to attacks or failures, it would take permanent losses to users since their data or records are stored into an unsure storage space pool outside the enterprises. These security risks move about in the direction of from the following reasons: the cloud infrastructures are much more authoritative and reliable than personal computing devices. If they are still susceptible to security threats both from inside and outside the cloud for the benefits of their control, there exist various motivations for cloud service providers (CSP) to behave falsely toward the cloud users in addition, the dispute infrequently suffers from the lack of trust on cloud service provider.

As a result, their behaviours may not be known by the cloud users. Therefore, it is necessary for cloud service providers to offer a scalable audit service to check the integrity and accessibility of the stored data. While Cloud Computing makes these advantages more appealing than ever, it also brings new challenging security threats towards users' outsourced data. Since cloud service provider is separate administrative units, outsourcing the data is actually resigning user's control over the destiny of their data. The correctness of the data in the cloud is being put at risk due to the subsequent reasons. First of all, although the infrastructures beneath the cloud are much more powerful and reliable than private computing devices, they are silent facing the broad range of both internal and external threats for data integrity.

A protocol which is secure, efficient and dynamic, which can be used in auditing is proposed, which can meet the data owners need. To solve the data privacy problem, a new method is defined which would generate a proof with a challenge stamp in an encrypted form by using the Rijndael Managed object, which would not allow the auditor to decrypt and view the data, however, the auditor can only verify the correctness of the proof. Without using the mask technique, the method does not require any trusted organizer during the batch auditing for multiple clouds. On the other hand, in the method, let the server compute the proof as an intermediate value of the verification wherein the auditor can directly use this intermediate value to verify the correctness of the proof. Therefore, the method can greatly reduce the computing loads of the auditor by moving it to the cloud server.

The aim of this paper is to design a framework and a protocol which would audit the private data stored by the data owners on the cloud servers.. Auditing protocol ensures the data privacy by using cryptography method and the Rijndael Managed object, instead of using the mask technique. Auditing protocol incurs less communication cost between the auditor and the server. By moving it to the server, it also reduces the computing loads of the auditor. Extend the protocol which is used to perform auditing on the private data to also perform the data dynamic operations, which would be secure and efficient. Extend auditing protocol to support batch auditing for not only multiple clouds but also multiple owners. The multi cloud batch auditing does not require any additional trusted organizer. The auditing performance can be improved by the multi owner batch auditing, especially in large-scale cloud storage systems.

2. Literature Review

To support the dynamic auditing, a dynamic provable data possession protocol [3] was developed based on symmetric key encryption and cryptographic hash function. Their idea is to precompute a certain number of metadata during the setup period, such that the number of updates and challenges is limited and fixed beforehand. In their protocol, each update operation requires recreating all the metadata remaining, which is problematic for large files. Moreover, their protocol cannot perform block insertions anywhere (only append-type insertions are allowed). Also [4] extended the PDP model to support dynamic updates on the data and proposed two dynamic provable data possession scheme, using a new version of authenticated dictionaries based on the rank information. However, their schemes may cause heavy computation burden to the server as they relied on the PDP scheme proposed by Ateniese. In [12], the authors proposed a dynamic auditing protocol which can support the dynamic operations of the data on the cloud servers, but this method may leak the content of the data to the auditor as it requires the server to send the linear combinations of the data blocks to the auditor. In [14], the authors also extended their dynamic auditing scheme to be privacy preserving and supports the batch auditing for multiple owners. However, due to the large number of data tags, their auditing protocols will incur a heavy storage overhead on the server. In [19], Zhu proposed a cooperative provable scheme for data possession which supports the batch auditing for multiple clouds and also extend it to support the dynamic auditing in [20]. However, it is not possible for their scheme to support the batch auditing for multiple owners as the parameters used for generation of the data tags by each owner are different, and thus, the data tags from different data owners cannot be combined in order to perform batch auditing. The other drawback is their scheme also requires an additional trusted organizer to send the auditor, a commitment during the batch auditing for multiple clouds, because their scheme applies the mask technique to ensure the data privacy.

3. Proposed System

The system proposed in this paper uses an efficient and secure dynamic auditing protocol to enable privacy-preserving public auditing for cloud data storage under the aforementioned model, protocol design should achieve the following security and performance guarantees.

1) Public auditability: To allow the third party auditor to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.
2) Storage correctness: To ensure there exists no cheating cloud server that can pass the third party auditor's audit without indeed storing users' data intact.
3) Privacy-preserving: To ensure that the third party auditor cannot derive users' data content from the information collected during the auditing process.
4) Batch auditing: To enable third party auditor with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.
5) Lightweight: To allow third party auditor to perform auditing with minimum communication and computation overhead.

4. Storage Auditing Protocol

To solve the data privacy problem, a new method is defined which would generate a proof with a challenge stamp in an encrypted form by using the Rijndael Managed object, which would not allow the auditor to decrypt and view the data, however, the auditor can only verify the correctness of the proof. On the other hand, in the method, let the server compute the proof as an intermediate value of the verification, which the auditor can directly use as intermediate value to verify the correctness of the proof.

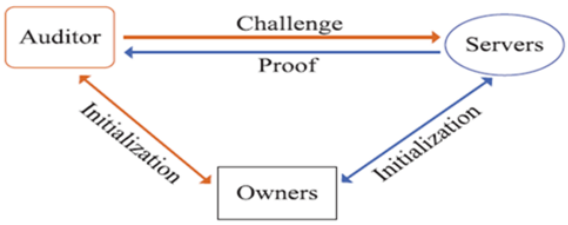


Fig. 2: System model of the Data Storage Auditing

The newly designed protocol used to audit the data stored on the cloud servers should protect the private data to be accessed and viewed by the auditor. By recovering the data blocks from the proof of the encrypted data, the auditor could obtain the data by decrypting the data. To solve the problem in preserving the private data, a new method is defined which would generate a proof with a challenge stamp in an encrypted form by using the Rijndael Managed object, which would not allow the auditor to decrypt and view the data, however, the auditor can only verify the correctness of the proof. Rijndael Managed object used to encrypt the data. The shared key to decrypt the password would be sent to the user's provided mail id. The shared key needs to be passed in the system to get the user key which would be used to upload the files. Symmetric algorithms break clear text into blocks of a fixed size which would be of size 16, 24, or 32 bytes and perform iterative rearrangement and substitution on successive blocks. Rijndael is used for the Crypto Utility as it offers the longest key length of the algorithms available natively from .NET—256 bits. There are difference modes available, out of which the cipher mode is used. In Rijndael, there are two possible ways, which are Cipher Block Chaining (CBC) or Electronic Code Book (CB). CBC, is the default and the most desired methods in cipher mode. The operation performed in XOR operations in CBC, the operation is performed on each block of clear text with the previous cipher block before enciphering it. CBC requires a random block of the same length as the block size and also an Initialization Vector (IV). When there are previous blocks, the IV is used as a stand-in to perform Cipher Block Chaining on the first block of clear text. The IV ensures that there are no repetitions in the first block of clear text.
Although the auditor has sufficient expertise and capabilities in conducting the auditing service, the computing ability of an auditor will not be as strong as cloud servers. Since the auditor would need to audit for many cloud servers and a large number of data owners, the auditor could have performance bottleneck. In the method, let the server compute the proof as an intermediate value of the verification (calculated by the challenge stamp and the linear combinations of data blocks), the auditor may use this intermediate value to verify the proof. Therefore, the method can greatly reduce the computing loads of the auditor by moving it to the cloud server. Storage auditing protocol ensures the data privacy by using the following five steps:

- Key Generation (λ): The key generation step takes no input other than the implicit security parameter. It outputs a secret hash key.
- Tag Generation (M): The tag generation step takes as inputs the file M and generates a tag for each and every file uploaded.
- Challenge: The challenge step challenges the user every time the file is accessed.
- Prove: The prove step takes as inputs the file M, the tags T, and the password to open the file.
- Verify. The verification step takes as inputs the password and if matches download the file to the users local.

Algorithm

1.Retrieve the file tag t, verify the signature and quit if the verification step fails.
2.Generate a random challenge and send to the cloud server.
3.The server generates the response proof
4.The third party auditor runs the verification to validate the response.

Flow Diagram to explain the activities of the cloud admin

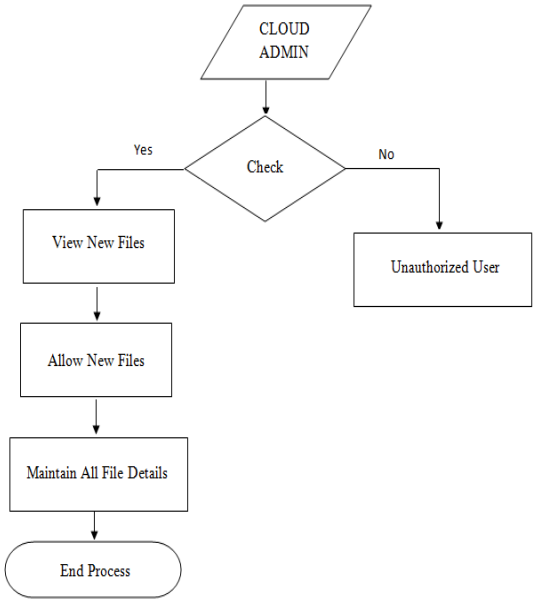


Fig. 3: Data flow diagram of a cloud admin

Flow Diagram to explain the activities of the TPA

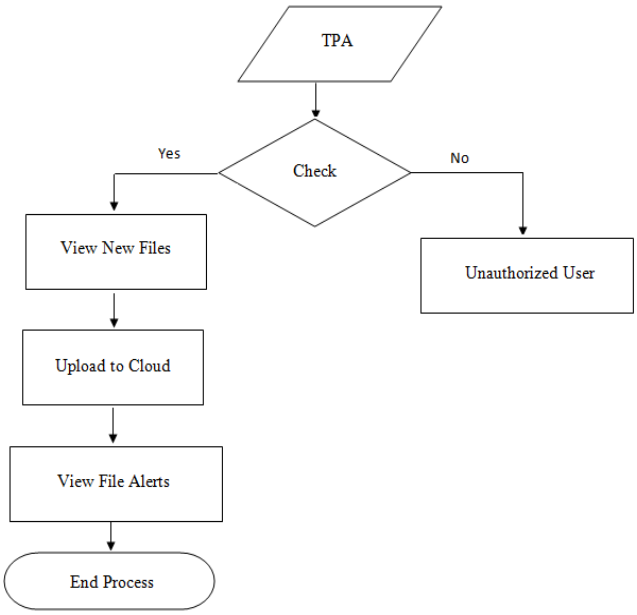


Fig. 4: Data flow diagram of a third party auditor

The storage auditing protocol consists of three phases: initialisation of owner, confirmation of the auditing, and the sampling auditing. During the initialization process, the owner for the entered data generates the keys and the tags. Once the data is stored on the server, the owner would ask the auditor to conduct the confirmation auditing to make sure that their data is correctly stored on the server. On confirmation, the owner may choose to delete the data which resides on their local end. The auditor then conducts the sampling auditing periodically to check the data integrity. Data storage auditing is an important service to check the data integrity on the data present in cloud servers by the data owners. There would be a number of requests to perform auditing on the data saved on cloud servers by multiple data owners, to improve the performance rather than handling the different request individually, it would be good to combine the requests handling by the auditor.

4. Batch Auditing for Multiowner

Data storage auditing is a vital service in cloud computing which helps the data owners to maintain data integrity on the data in the cloud servers. There would be a number of requests to perform auditing on the data saved on cloud servers by multiple data owners, to improve the performance rather than handling the different request individually, it would be good to combine the requests handling by the auditor. Previously, the auditor could not support the batch auditing for multiple owners as the parameters used for generating the data tags were different and hence the auditor could not combine the tags generated from the data by the multiple owners. To ensure the data integrity of the data owners, the auditing challenges needs to be sent to each cloud that hosts the data and need to verify the proofs from all of them. To reduce the cost in performing all these steps individually for every request, it is desirable to combine all the responses and do the batch verification together.

Algorithm

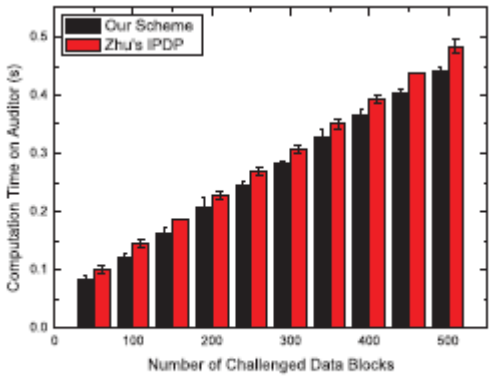
1.The owners perform the key generation step to generate the secrete key, this secret key would be different for each cloud servers.
2.The data owners perform the tag generation in order to get the data tags.
3.The data tags and the secret key needs to be sent to the corresponding server.
4.In case of batch auditing, the auditor performs batch challenge for a set of challenged owners.
5.On receiving the challenge, the cloud server generates a proof and sends it back to the auditor.
6.The auditor on receiving all the proofs, perform batch verification.
7.Retrieve the file tag t, verify the signature and quit if the verification step fails.
8.Generate a random challenge and send to the cloud server.
9.The server generates the response proof. The third party auditor runs the verification to validate the response.

5. Experimental Results and Analysis

Communication cost between the auditor and the server is considered which consist of the challenge and proof. Consider a batch auditing with K owners and C cloud servers. The number of challenged data block from each owner on different cloud servers is the same, denoted as t, and the data blocks are split into s sectors.

5.1 Computation Cost of the Auditor

Fig. 5 shows the computation time of the auditor versus the number of challenged data blocks in the single cloud and single owner case. In this figure, the number of data blocks goes to 500 (i.e., the challenged data size equals to 500 KByte), but it can illustrate the linear relationship between the computation cost of the auditor versus the challenged data size. From Fig. 5, the scheme incurs less computation cost of the auditor.

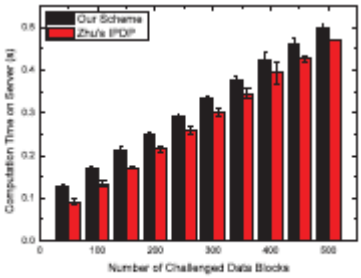


Single Owner, Single Cloud

Fig. 5: Computation cost of Auditor

5.3 Computation Cost of the Server

The scheme moves the computing loads of the auditing from the auditor to the server, such that it can greatly reduce the computation cost of the auditor. By estimating the cost in terms of basic cryptographic operations, suppose there are c random blocks specified in the challenge message during the Audit phase. Under this setting, quantify the cost introduced of the privacy preserving auditing in terms of server computation, auditor computation as well as communication overhead.



Single Owner, Single Cloud

Fig. 6: Computation cost on the Server

However, on the practical side, there are additional less expensive operations required for batching, such as modular exponentiations and multiplications. Meanwhile, different number of sampled blocks c, are also a variable factor that affects the batching efficiency. Thus, the benefits of removing pairings significantly outweigh these additional operations.

6. Results

In this section, the proposed system results have been presented. Fig. 7 shows the screen which displays the key generated

Fig. 7: Registered data owner key generated

Fig. 8 is used as the screen to select the file, upload the file and send a request to the cloud server.

Fig. 8: File upload

Fig. 9 is used as the screen to accept the request from the data owners to upload the files to cloud.

Fig. 9: Grant access for the file to be uploaded

Fig. 10 is used as the screen to share the data by the data owners to other users who can access the data.

Fig. 10: Data Sharing

Conclusion

In this paper, a secure, dynamic and an efficient protocol for auditing is designed which protects the private data of the data owners by using cryptography against the auditor. Furthermore, in this design the computing loads of the auditor are performed on the server rather than on the auditor end which incurs less communication cost and less computation cost and can be applied to large-scale cloud storage systems. Hence, there is no need for a separate organizer in case of batch auditing. To support the multiple requests from multiple data owners, batch auditing protocol is used. In cloud computing, establishment of privacy-preserving public auditing, TPA may concurrently handle multiple auditing delegations upon different users' requests. Individual auditing of these tasks for TPA can be tedious and inefficient while batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, also greatly reduces the computation cost on the TPA side. The support to perform data dynamics for privacy-preserving public risk auditing is also of paramount importance. The main concept is used to build on top of the existing work to support data dynamics which includes block level operations of insertion, deletion and modification.

References

[1] 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, 2010.

[2] G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, M. Matsui, ed., pp. 319-333, 2009.

[3] Ateniese et al. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," IACR Cryptology ePrint Archive, vol. 2008, p. 114, 2008.

[4] C.C. Erway, A. Kupcu , C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security, E. Al-Shaer, S. Jha, and A.D. Keromytis, eds., pp. 213-222, 2009.

[5] Kan Yang, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Sep. 2013.
[6] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," technical report, Nat'l Inst. of Standards and Technology,2009.
[7] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking," J. ACM, vol. 56, no. 1, article 2, 2009.
[8] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security (CCS '07), P. Ning, S.D.C. di Vimercati, andP.F. Syverson, eds., Oct. 2007.
[9] F. Sebe´, J. Domingo-Ferrer, A. Martı´nez-Balleste´, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.
[10] 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), G.C. Hunt, ed., 2007.
[11] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010.
[12] C. Wang, S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEECS Log Number TC-2010-11-0627, 2013.
[13] C. Wang, Q. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
[15] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[16] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.
[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.
[18] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012.
[19] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
[20] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing, W.C. Chu, W.E. Wong, M.J. Palakal, and C.-C. Hung, eds., pp. 1550-1557, 2011.