International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Optimized Secure Auditing Protocol for Storage of Data Dynamically in Cloud Computing

Preeti Wadhera[1], Dr. Rajdev Tiwari[2]

Research Scholar, Noida International University, Noida

Director (MCA) at Noida Institute of Engineering and Technology, Greater Noida

Abstract: ***Cloud computing is growing nowadays , the one of the most efficient use of cloud is data storage on cloud server. In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Cloud Computing is a type of distributed computing whereby resources and applications are shared over the internet. These applications a restored in one location and can be accessed in different location by any authorized users where the user does not need any infrastructure. But due to the data outsourcing, there are some challenging aspects behind this cloud data storage as per end users perspective, this new paradigm of data hosting service introduces new security challenges, how end users know their data is secure on cloud server? How they satisfied that the data is not tampered and successfully updated after performing some operation over it? Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing services in the cloud can be dynamically updated.Thus,anoptimizedandsecuredynamicauditingprotocolisdesiredtoconvince data owners that the data are correctly stored in the cloud. Here the Trusted Third Party auditor comes in picture and using auditing framework he satisfy end users that there data is secure over server and successfully updated. So in this paper optimized secure auditing algorithm is designed and also extended to dynamic auditing. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds.***

Keywords: Cloud computing, Storage auditing, Cloud storage, Privacy Preserving Auditing, Secure Dynamic Auditing.

1. Introduction

In recent times, the Cloud Computing is gaining more and more success , from both industrial and academic community. Cloud computing is a model for enabling on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, applications, and services). Cloud computing is being driven by many which includes Google, Amazon and Yahoo as well as traditional vendors including IBM, Intel and Microsoft.

Sometimes, cloud service suppliers can be dishonest. They might discard the data that has not been accessed or rarely accessed and claim that the data area unit still properly hold on inside the cloud. Therefore, owners have to be convinced that the data are properly hold on inside the cloud. Traditionally, owners can check the data integrity based on two-party storage auditing protocols [3], [4], [5], [6],[7], [8], [9], [10], [11]. In cloud storage system, however, it is inappropriate to let either side of cloud service providers or owners conduct such auditing, because none of them could be guaranteed to provide unbiased auditing result. In this situation, third-party auditing is a natural choice for the storage auditing in cloud computing. A third-party auditor (auditor) that has expertise and capabilities can do a more efficient work and convince both cloud service providers and owners.

2. Proposed Work

In this paper, we propose an optimized and secure dynamic auditing protocol, which can meet the above-listed requirements. To solve the data privacy problem, our method is to generate an encrypted proof with the challenge stamp by using the Elliptic curve in integrated mode and secure asymmetric key distribution scheme will be processed for security parameters, such that the auditor cannot decrypt it but can verify the correctness of the proof. On the other hand, in our method, we let the server compute the proof as an intermediate value of the verification, such that the auditor can directly use this intermediate value to verify the correctness of the proof. Therefore, our method can greatly reduce the computing loads of the auditor by moving it to the cloud server.

Definition of a system model

We consider an auditing system for cloud storage as shown in Fig. 1, which involves data owners (owner), the cloud server (server), and the third-party auditor (auditor). The owners create the data and host their data in the cloud. The cloud server stores the owners' data and provides the data access to users (data consumers). The auditor is a trusted third-party that has expertise and capabilities to provide data storage auditing service for both the owners and servers. The auditor can be a trusted organization managed by the government, which can provide unbiased auditing result for both data owners and cloud servers.

Basic Concepts

Three main entities in cloud environment include:

- Cloud Service Provider: It provides data storage service as well as cloud servers with significant resources.
- Data Owner: Owners keep their own data to the cloud server and access them when needed. They rely on the cloud for data computation.
- Third party auditor: An optional TPA is trusted to assess and expose risk of cloud storage services on behalf of the user's open request. It has expertise capabilities to convince both CSP as well as Data Owner.

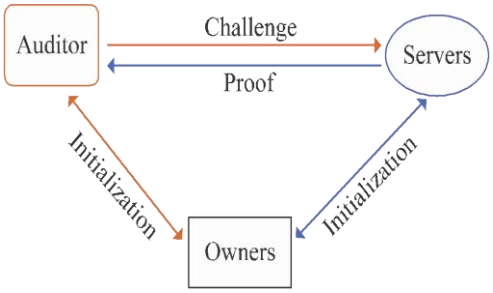

Figure 1: shows the basics of cloud computing

Characteristics of auditing protocols:
While designing this data integrity checking protocol, they must satisfy some requirements:

- Highly private: The TPA should not gain knowledge of the original user data during the auditing process. Data dynamic: The clients must be able to perform operations on data files like insert, alter and delete while maintaining data correctness.
- Open verifiability: Anyone, not just the clients, must be allowed to verify the integrity of data.
- Block free verification: Challenged file blocks should not be retrieved by the verifier during verification process.
- No restriction of queries: The verifier may be allowed to use unlimited number of queries in the challenge-response protocol for data verification.

3. Main Contribution

- To provide optimized conditional message communication which will provide solution for storage while auditing process for number of transactions which will provide good level of privacy preservation. (This process is done by runtime asking from user in simulation for authentication of the user. Four way handshake authentication algorithms will be used for better security in between user and server resources.)
- To provide optimal storage solutions required for storing Pseudonyms by introducing traces with local reference in PDU exchange. Malicious traffic prevention will lead to huge amount of storage while processing prevention measures so, we are cutting that storage issue by providing trace information in header processing so that there will be no need for extra storage of counter measures. We are using an auditor, owner and server based protocols which will work on conditional message forwarding. (This process is done by providing optional message transfer from server to user dependent on the role of the server and user. For better management in cloud structure, we will implement parallel computing structure in network simulator. This structure will run in relative to cloud resource shuffling in between servers. Random proportional resource assignment will be done for checking initial resources assignment to cloud structure. Header of the messages considered with each transaction will carry various traces of KeyGen for authentication filtering.)
- Measurement of effectiveness of our proposed by comparing it with already existing auditing operation communication.

The terms used in our work:

- KeyGen: key generation algorithm that is run by the user to setup the scheme by generating the set of keys.
- TagGen: used by the user to generate verification metadata, which may consist of signatures or other information used for auditing
- Challenge: run by the auditor on the CSP to check the verifiability of the file stores on the server as per owner order.
- Proof: run by the cloud server to generate a proof of data storage correctness
- Verify: run by the TPA to audit the proof from the cloud server by checking the actual hash and calculated hash by server.
- ITable: ITable is created by the owner during the owner initialization and managed by the auditor.

Our process is also started with auditor initialization phase which exchange KeyGen including secret key with secret hash function and public tag key for providing synchronized security locally at auditor end and globally at owner and server ends. Similarly to previous process Keygen is treated along with TagGen which includes tag key as synchronized with keyGen to fetch the secret key generated through Elliptic Curve in integrated mode and secure asymmetric key distribution scheme will be processed for security parameters. But instead of processing it through challenging algorithm which utilize huge space at auditor, owner and server end for processing and storing of in between data, we processed header's 2 bit information for storing traces of data blocks for challenge algorithm. Server checks the KeyGen and TagGen and provides a feedback with tiny trace update in header bits which further update the challenge algorithm information on auditor side with information of successful transaction. Once auditor verifies the challenge info, it starts process without Checking KeyGen and Tag hash function on each transaction. ITable is created for future references of process and it is stored on auditor end.

4. Related Work

To support the dynamic auditing, Ateniese et al. [22] developed a dynamic provable data possession protocol based on cryptographic hash function and symmetric key encryption. Their idea is to precompute a certain number of metadata during the setup period, so that the number of updates and challenges is limited and fixed beforehand. In their protocol, each update operation requires recreating all the remaining metadata, which is problematic for large files. Moreover, their protocol cannot perform block insertions anywhere (only append-type insertions are allowed). Erway et al. [16] also extended the PDP model to support dynamic updates on the stored data and proposed two dynamic provable data possession scheme by using a new version of authenticated dictionaries based on rank information. However, their schemes may cause heavy computation burden to the server because they relied on the PDP scheme proposed by Ateniese.

In [17], the authors proposed a dynamic auditingprotocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the

auditor because it requires the server to send the linear combinations of data blocks to the auditor. In [18], the authors extended their dynamic auditing scheme to be privacy preserving and support 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 et al. proposed a cooperative provable data possession scheme that can support the batch auditing for multiple clouds and also extend it to support the dynamic auditing in [20]. However, it is impossible for their scheme to support the batch auditing for multiple owners. That is because parameters for generating the data tags used by each owner are different, and thus, they cannot combine the data tags from multiple owners to conduct the batch auditing. Another drawback is that their scheme requires an additional trusted organizer to send a commitment to the auditor during the batch auditing for multiple clouds, because their scheme applies the mask technique to ensure the data privacy. However, such additional organizer is not practical in cloud storage systems. Furthermore, both Wang's schemes and Zhu's schemes incur heavy computation cost of the auditor, which makes the auditing system inefficient.

5. Conclusion

In this paper, we proposed an optimized and secure dynamic auditing protocol for storage of data. It protects the data privacy against the auditor by using the elliptic curve cryptographic scheme rather than using the other schemes. Our batch auditing protocol can also support the batch auditing for multiple owners. Furthermore, our auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the auditing performance and can be applied to large-scale cloud storage systems.

References

[1] Amazon elastic compute cloud (Amazon EC2), http://aws.amazon.com/ec2/.
[2] Kan Yang, Student Member, IEEE, and XiaohuaJia, Fellow, IEEE "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" IEEE transactions on parallel and distributed systems, vol. 24, no. 9, September 2013
[3] M. Lillibridge , S. Elnikety , A. Birrell , M. Burrows, and M. Isard ,"A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf., pp. 29-41, 2003.
[4] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote Integrity Checking,"Proc. Sixth Working Conf. Integrity and Internal Control in Information Systems (IICIS), Nov. 2004.
[5] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking,"J. ACM,vol. 56, no. 1, article 2, 2009.
[6] A. Juels and B.S. Kaliski Jr., "Pors: Proofs of Retrievability for Large Files,"Proc. ACM Conf. Computer and Comm. Security,P. Ning, S.D.C. di Vimercati, and P.F. Syverson, eds., pp. 584-597, 2007.
[7] T.J.E. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems,p. 12, 2006.
[8] D.L.G. Filho and P.S.L.M. Barreto, "Demonstrating Data Posses-sion and Uncheatable Data Transfer," IACR Cryptology e Print Archive,vol. 2006, p. 150, 2006.
[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] G. Yamamoto, S. Oda, and K. Aoki, "Fast Integrity for Large Data,"Proc. ECRYPT Workshop Software Performance Enhancement for Encryption and Decryption, pp. 21-32, June 2007.
[11] 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.
[12] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services,"IEEENetwork,vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[13] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities,"World Wide Web,vol. 15, no. 4, pp. 409428, 2012.
[14] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores,"Proc. ACM Conf. Computer and Comm. Security,P. Ning, S.D.C. di Vimercati, and P.F. Syverson, eds., pp. 598-609, 2007.
[15] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, J. Pieprzyk, ed., pp. 90-107, 2008.
[16] C.C. Erway, A. Ku¨pc¸u ¨, 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.
[17] 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 Distributed Systems,vol. 22, no. 5, pp. 847-859, May 2011.
[18] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM,pp. 525533, 2010.
[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.
[21] K. Zeng, "Publicly Verifiable Remote Data Integrity,"Proc. 10th Int'l Conf. Information and Comm.

Security,L. Chen, M.D. Ryan, and G. Wang, eds., pp. 419-434, 2008.

[22] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient ProvableData Possession," IACR Cryptology ePrint Archive, vol. 2008, p. 114, 2008.

Author Profile

PreetiWadhera is Research Scholar at NIU, Noida. She did M.Tech , B. Tech (Computer Science).

Dr Rajdev Tiwari Director (MCA) at NIET, Greater Noida.UGC NET (Computer Science),Ph. D(Computer Science) , MCA, Post Graduate Diploma in Advance Software Design & Development, M Sc., B Sc.