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

Framework for Secure and Dynamic Auditing Of Data Storage in Cloud Platforms

G.Jyothsna
M.Tech Student
Department of CSE
B V Raju Institute of Technology
Narsapur, India.

Mrs.P.M.Jyothsna
AssistantProfessor
Department of CSE
B V Raju Institute of Technology
Narsapur, India.

Abstract:
Cloud Computing is a type of distributed computing whereby resources and applications are shared over the internet. These applications are stored in one location and can be accessed in different location by any authorized users where the user does not need any infrastructure. In cloud storage, while outsourcing trust worthiness of the data is a scary task in cloud. To ensure the integrity of dynamic data stored in the cloud, external Third Party Auditor (TPA) is acquainted in a cloud infrastructure. For enabling public auditing in cloud data storage security, users can resort to an external auditor to check integrity of an outsourced data. The third party auditor (TPA) should met the following fundamental requirements: 1) TPA should be able to efficiently audit the cloud data without revealing the original data, and it should not add burden to the cloud user; 2) Auditing process should not bring no new vulnerabilities towards the user data. 3) Integrity of the data is protected against TPA by invoking some cryptographic techniques to ensure the storage correctness in cloud. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users, can be performed by the TPA and further enables TPA to perform data dynamics operations. Thus, the performance analysis depicts that the proposed schemes are more sheltered and highly competent.

Index Terms--Cloud Computing, Data Storage, Integrity, Availability, Public Auditing.

INTRODUCTION

Cloud Computing is the use of Internet for the tasks performed on the local machine, with the hardware and software demands maintained elsewhere. It represents a different way to architect and remotely manage computing resources. Cloud is widely used everywhere owing to its convenience, be it in simple data analytic program or composite web and mobile applications. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Cloud computing is being driven by many which includes Google, Amazon and Yahoo as well as traditional vendors including IBM, Intel and Microsoft.

Fig 1 General Representation of cloud

Fig 1 shows the representation of client access the data on the cloud server with the help of internet. In this cloud computing paradigm data integrity is a big issue when storing data in the cloud. Because data owners store there data in the cloud server but there is no assurance for data correctness. So there are some auditing protocols available to provide data integrity.

The auditing protocol should have the following properties 1) Confidentiality. The auditing protocol should keep owner's data confidential against the auditor. 2) Dynamic auditing. The auditing protocol should support the dynamic updates of the data in the

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

cloud. 3) Batch auditing. The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds. Recently, several remote integrity checking protocols were proposed to allow the auditor to check the data integrity on the remote server. Fig 1.2 shows the simple auditing process between auditor and the cloud server.

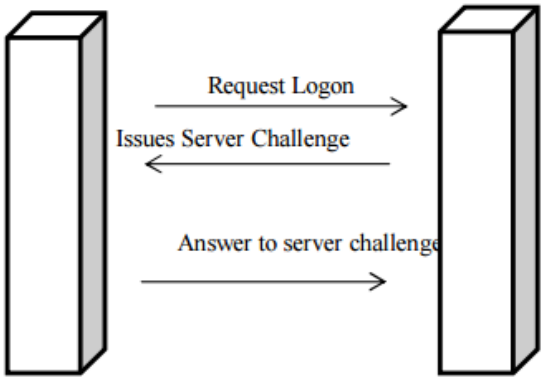

Fig 2 Auditing Query via the Challenge-response Protocol

EXISTING SYSTEM

To solve the data privacy problem, existing method is to generate an encrypted proof with the challenge stamp by using the Bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it but can verify the correctness of the proof. Without using the mask technique, this method does not require any trusted organizer during the batch auditing for multiple clouds. On the other hand, in this method, server computes 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, existing method can greatly reduce the computing loads of the auditor by moving it to the cloud server. Fig 1.2 shows the overall work flow of the existing auditing protocol. To improve the performance of an auditing system, apply the data fragment technique and homomorphic verifiable tags in our method. The data fragment technique can reduce number of data tags, such that it can reduce the storage overhead and improve the system performance. By using the homomorphic verifiable tags, no matter how many data blocks are challenged, the server only responses the sum of data blocks and the product of tags to the auditor, whose size is constant and equal to only one data block. Thus, it reduces the communication cost.

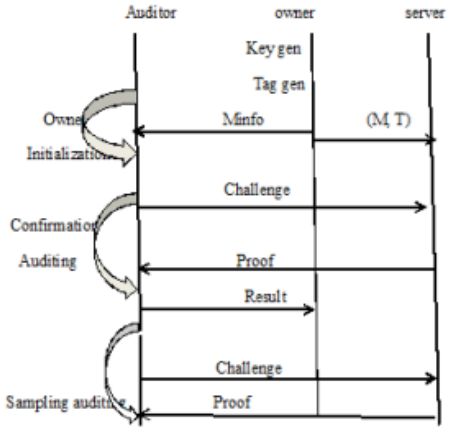

Fig 3 Framework of our privacy-preserving auditing protocol

Advantage:

1. Auditing protocol ensures the data privacy by using cryptography method and the Bilinearity property of the bilinear pairing, instead of using the mask technique .This protocol incurs less communication cost between the auditor and the server. It also reduces the computing loads of the auditor by moving it to the server.
2. Also it supports data dynamic operations, which is efficient and provably secure in the random oracle model.

3. We further extend our auditing protocol to support batch auditing for not only multiple clouds but also multiple owners, multicloud batch auditing does not require any additional trusted organizer. The multiowner batch auditing can greatly improve the auditing performance, especially in large-scale.

Disadvantage:

1. This protocol is not suitable when data loss occur during auditing process. Especially when sending encrypted challenge stamp to the auditor and to the cloud server.
2. Also it can't be solving the situation when multiple owners periodically updated.

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

PROPOSED SYSTEM

To improve the draw backs of existing system we introduce a modified dynamic auditing protocol, This protocol contains 1.Time stamp value to verify the validity of data 2.Index table for dynamic owner as well as data.

This system includes 4 modules

1. Multi cloud storages

2. Modified dynamic auditing

3. Data Integrity and Third Party Auditor

4. Dynamic auditing

Multi cloud storage

First we should create storage space for client to host there data in the cloud server. When storing the encrypted data in cloud server client fragment there data to reduce storage overhead. Fragmentation technique is the first process done by modified dynamic auditing protocol. During this fragmentation process we have to mention the fragmentation size of the data blocks. We further split the data blocks in to sectors. Sector size is restricted by the security parameter. Next step is to generate one data tag for each data block that consists of s sectors.

Modified Dynamic Auditing:

Using key generation and tag generation algorithm we generate a computed data component.

KeyGen (λ) → (skh, skt , pkt). This key generation algorithm takes no input other than the implicit security parameter λ. It outputs a secret hash key skh and a pair of secret-public tag key (skt , pkt).

TagGen(M, skt , skh) → T. The tag generation algorithm takes as inputs an encrypted file M, the secret tag key skt and the secret hash key skh. For each data block mi, it computes a data tag ti based on skh and skt . It outputs a set of data tags T = {ti}i∈[1,n].

$$t_i = \left(h(sk_h, W_i) \cdot \prod_{j=1}^{s} u_j^{m_{ij}} \right)^{sk_t},$$

Data integrity and third party auditing:

Chall (Minfo) → C. The challenge algorithm takes as input the abstract information of the data Minfo (e.g., file identity, total number of blocks, version number and timestamp etc.). It outputs a challenge C.

Prove (M, T, C,Ti) → P. The prove algorithm takes as inputs the file M, the tags T and the challenge from the auditor C. It outputs a proof P.when sending proof we should include the time stamp to verify the validity of the data.

Verify (C, P, skh, pkt ,Minfo) → 0/1. The verification algorithm takes as inputs the P from the server, the secret hash key skh, the public tag key pkt and the abstract information of the data Minfo. It outputs the auditing result as 0 or 1.

Dynamic Auditing:

Data update:

There are three types of data update operation is takes place 1.modify 2.insert 3.update.We Propose an auditing protocol that include a time stamp field for each operation.

Modify:

The modification algorithm takes as inputs the new version of data ,secret hash key skh , secret tag key skt. It generates new version number for the data and it again generate tag key.

Insert:

Insert (m∗i , skt , skh) → (Msginsert , t∗i)

The insertion algorithm takes as inputs the new data block m∗i , the secret tag key skt and the secret hash key skh. It inserts a new data block m∗ i before the ith position. It generates an original number B∗i ,a new version number V∗i and a new timestamp T∗i . Then, it calls the TagGen to generate a new data tag t∗ i for the new data block m∗i . It outputs the new tag t∗ i and the update message Msginsert = (i, B∗ i , V∗i , T∗i). Then, it inserts the new pair of Data block and tag (m∗i

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

, t∗i) on the server and sends the update message Msginsert to the auditor.

Delete (mi) → Msgdelete.

The deletion algorithm takes as input the data block mi. It outputs the update message Msgdelete = (i, Bi, Vi, Ti). It then deletes the pair of data block and its tag (mi, ti) from the server and sends the update message Msgdelete to the auditor.

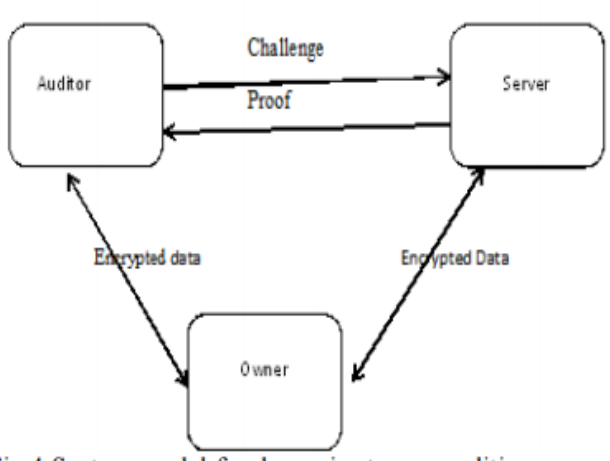

Fig 4 System model for dynamic storage auditing

CONCLUSION

Cloud-based mechanisms are required to ensure data security and privacy, and to fulfill the regulatory and audit requirements of enterprises. Economical and inherently secure dynamic auditing protocol is proposed which protects the information privacy against the auditor and data loss by combining the cryptography method with the additive property of bilinear paring with time stamp, rather than using simple bilinear pairing without timestamp value. Thus, multicloud batch auditing protocol does not need any extra organizer. Batch auditing protocol can even support the batch auditing for multiple owners. Also, it reduces the computation time compared to the previous auditing scheme. It uses the best fragmentation technique so that the data tag generation is reduced. Thus, the storage space is preserved. In this technique, even the auditor is not aware about the actual form of data that is stored in the cloud.

REFERENCES

1. Kang Yang, (2013) "An Efficient and secure dynamic auditing protocol for data storage in cloud computing", vol.24,no9.

2. Armbrust.M, Fox.A, Griffith.R, Joseph A.D, Katz R.H, Konwinski .A, Lee.G, Patterson D.A, Rabkin.A, Stoica.I, and Zaharia.M,(2010) "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58.

3. Ateniese.G, Pietro R.D, Mancini.L, and Tsudik.G,(2008) "Scalable and Efficient Provable Data Possession," IACR Cryptology ePrint Archive, vol. 2008, pp. 114.

4. Bairavasundaram L.N,Goodson, Pasupathy.S, and J. Schindler,(2007) "An Analysis of Latent Sector Errors in Disk Drives," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, Golubchik.L, Ammar L.N., and Harchol- Balter L.N, eds, pp. 289-300.

5. C. Wang, Q. Wang, K. Ren, and W. Lou,(2010) "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533.

6. Kher.V and Kim.Y,(2005), "Securing Distributed Storage: Challenges, Techniques, and Systems," Proc. ACM Workshop Storage Security and Survivability (StorageSS), pp. 9-25.

7. Li.J, Krohn M.N , Mazieres.D, and Shasha.D ,(2004) "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth Conf. Symp. Operating Systems Design Implementation, pXp. 121-136,

8. Lillibridge.M, Elnikety.S Birrell.A, M. Burrows, and Isard.M,(2003) "A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf., pp. 29-41.

9. Schroeder .B and Gibson G.A,(2007), "Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You?" Proc. USENIX Conf. File and Storage Technologies, pp. 1-16.

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

10. Sebe.F, Domingo-Ferrer.J, Martı nez-Balleste.A, Deswarte.Y, and Quisquater.J,(2008) "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034-1038.

11. Shah.A, Baker.B, MogulJ.C, and Swaminathan.R,(2007) "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HOTOS), G.C. Hunt, ed.

12. Velte.T, Velte.V, and Elsenpeter.R,(2010), Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill.

13. Wang C., Ren .K, W. Lou, and J. Li,(July/Aug2010), "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24.

14. Yang.K and Jia.,(2010) "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428.