ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Detecting And Eliminating Fraudulence Using Cloud Storage

V. Kalaiarasi[1], R. Gugapriya @ Saruga[2], K. Nirmaladevi[3], Mr. P. Anandhajayam[4]

Final Year, Dept. of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry[1, 2, 3]

Assistant Professor, Dept. of Computer Science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry [4]

Abstract—In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.

Key Terms—Storage auditing, dynamic auditing, privacy-preserving auditing, batch auditing, cloud computing.

I. INTRODUCTION

CLOUD computing - "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet. It is the infrastructure provided by the service provider to build the Internet applications. Cloud storage is an important service of cloud computing[1], which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud [2].However, this new paradigm of data hosting service also introduces new security challenges [3]. Owners would worry that the data could be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take [4], [5], [6], [7], [8]. Sometimes, cloud service providers might be dishonest. They could discard the data that have not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud. Traditionally, owners can check the data integrity based on two-party storage auditing protocols [9], [10], [11], [12], [13], [14], [15], [16], [17]. 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. For the third-party auditing in cloud storage systems, there are several important requirements that have been proposed in some previous works [18], [19]. 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 cloud. 3) Batch auditing. The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Recently, several remote integrity checking protocols were proposed to allow the auditor to check the data integrity on the remote server [20], [21], [22], [23], [24], [25],[26], [27], [28]. In [23], the authors proposed a dynamic auditing protocol 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 [24], 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 may incur a heavy storage overhead on the server. In [25], 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 [26]. However, their scheme cannot 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 multicloud batch auditing, because their scheme applies the mask technique to ensure the data privacy.

We design an auditing framework for cloud storage systems and propose a privacy-preserving and efficient storage auditing protocol. Our auditing protocol ensures the data privacy by using cryptography method and the Bilinearity property of the bilinear pairing, instead of using the mask technique. Our auditing 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. We extend our auditing protocol to support the 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. Our multicloud batch auditing does not require any additional trusted organizer. The multiowner batch auditing can greatly improve the auditing performance, especially in large-scale cloud storage systems.

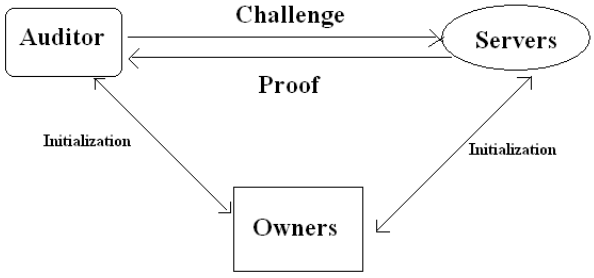

Fig: System Model Of DAta Storage Auditing

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.

II. FORMAL APPROACH

We consider a Joint Threshold Administrative Tool (JTAM) which is used to detect the fraudulence to check similar details stored in the cloud. The cloud servers store the data and provide the data access to the users.

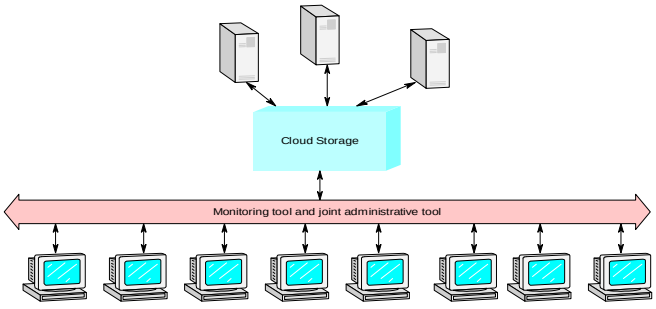

Fig: System Architecture

Our study is in the case where the auditing service is used to check the integrity of data in the cloud. These are critical problems such that 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. Although the

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

auditor has sufficient expertise and capabilities to conduct the auditing service, the computing ability of an auditor is not as strong as cloud servers. Therefore, our method can greatly reduce the computing loads of the auditor by moving it to the cloud server.

III. EXISTING SYSTEM

The data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. Auditing protocol is used to support the data dynamic operations, which is efficient and provably secure in the random oracle model. In dynamic auditing protocol cloud server have threat for security for data storage. When any system is suspected that will be under tracked only under complaint. There is no link between all the databases where an individual have different accounts.

IV. PROPOSED SYSTEM

A monitoring tool that detects fraudulent using link analysis and checks for similar details among multiple databases will be created. As there is no interlinking between different bank database an individual can create many accounts with different identity proofs So that they can do malicious activities in the network. To avoid this we use link analysis for finding similarity link in all the combined cloud stored database. It uses Joint Threshold Administrative Model (JTAM) for authenticating database storage and handles fault tolerance effectively using the monitoring tool. Creating monitoring tool that tracks fraudulent account creation using link analysis. It is used to handle all the suspected system involved in malicious activities Joint Threshold Administrative Tool (JTAM) is used for permitting privileges for data storage. It also handles fault tolerance effectively. The data will be stored securely in the cloud.

PRIVACY PRESERVING AUDITING PROTOCOL

To improve the performance of an auditing system, we 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.
Our storage auditing protocol consists of three phases: owner initialization, confirmation auditing, and sampling auditing. During the system initialization, the owner generates the keys and the tags for the data. After storing the data on the server, the owner asks the auditor to conduct the confirmation auditing to make sure that their data is correctly stored on the server. Once confirmed, the owner can choose to delete the local copy of the data. Then, the auditor conducts the sampling auditing periodically to check the data integrity.

Phase 1: Owner initialization. The owner runs the key generation algorithm KeyGen to generate the secret hash key secret hash key, the pair of secret-public tag key skt; pkt. Then, it runs the tag generation algorithm TagGen to compute the data tags. After all the data tags are generated, the owner sends each data component and its corresponding data tags to the server together with the set of parameters fujgj2½1;s_. The owner then sends the public tag key pkt, the secret hash key skh, and the abstract information of the data Minfo to the auditor, which includes the data identifier FID, the total number of data blocks n.

Phase 2: Confirmation auditing. In our auditing construction, the auditing protocol only involves two-way communication:
Challenge and Proof. During the confirmation auditing phase, the owner requires the auditor to check whether the owner's data are correctly stored on the server.

Phase 3: Sampling auditing. The auditor will carry out the sampling auditing periodically by challenging a sample set of data blocks. The frequency of taking auditing operation depends on the service agreement between the data owner and the auditor (and also depends on how

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

much trust the data owner has over the server). Similar to the confirmation auditing in Phase 2, the sampling auditing procedure also contains two-way communication.

SECURE DYNAMIC AUDITING

In cloud storage systems, the data owners will dynamically update their data. As an auditing service, the auditing protocol should be designed to support the dynamic data, as well as the static archive data. However, the dynamic operations may make the auditing protocols insecure. Specifically, the server may conduct two following attacks:

1) Replay attack.

The server may not update correctly the owner's data on the server and may use the previous version of the data to pass the auditing.

2) Forge attack.

When the data owner updates the data to the current version, the server may get enough information from the dynamic operations to forge the data tag. If the server could forge the data tag, it can use any data and its forged data tag to pass the auditing.

To prevent the replay attack, we introduce an index table (ITable) to record the abstract information of the data. The ITable consists of four components: Index, Bi, Vi, and Ti. The Index denotes the current block number of data block mi in the data component M. Bi denotes the original block number of data block mi, and Vi denotes the current version number of data block mi. Ti is the time stamp used for generating the data tag. This ITable is created by the owner during the owner initialization and managed by the auditor. When the owner completes the data dynamic operations, it sends an update message to the auditor for updating the ITable that is stored on the auditor. After the confirmation auditing, the auditor sends the result to the owner for the confirmation that the owner's data on the server and the abstraction information on the auditor are both up-to-date. This completes the data dynamic operation. To deal with the forge attack, we can modify the tag generation algorithm.

V. CONCLUSION

In this paper, we introduced a we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor. We create server & client systems and different databases. Creating network between server, client and database system.

We also create monitoring tool which tracks the stored data in different databases for its similarity interlinking details. Joint administrative tool is created with different administrators implied in different databases. Admin gives authentication for storage of data and subsequently analyze similarity details in cloud storage database. Using link analysis algorithm database details are compared and checked also implies JTAM thus handling fault tolerance mechanism. This tool implies authenticated and secured database management.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing,"technical report, Nat'l Inst. of Standards and Technology,2009.
[2] 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.
[3] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010.
[4] J. Li, M.N. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Operating Systems Design Implementation, pp. 121-136, 2004.
[5] G.R. Goodson, J.J. Wylie, G.R. Ganger, and M.K. Reiter, "Efficient Byzantine-Tolerant Erasure-Coded Storage," Proc. Int'l Conf. Dependable Systems and Networks, pp. 135-144, 2004.
[6] V. Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," Proc. ACM Workshop Storage Security and Survivability (StorageSS), V. Atluri, P. Samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, eds., pp. 9-25, 2005.
[7] L.N. Bairavasundaram, G.R. Goodson, S. Pasupathy, and J. Schindler, "An Analysis of Latent Sector Errors in Disk Drives," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, L. Golubchik, M.H. Ammar, and M. Harchol-Balter, eds., pp. 289-300, 2007.
[8] B. Schroeder and G.A. Gibson, "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, 2007.
[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. USENIX Ann.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Technical Conf., pp. 29-41, 2003.
[10] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote Integrity Checking," Proc. Sixth Working Conf. Integrity and Internal Control in Information Systems (IICIS), Nov. 2004.
[11] M. Naor and G.N. Rothblum, "The Complexity of Online Memory Checking," J. ACM, vol. 56, no. 1, article 2, 2009.
[12] 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.
[13] 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.
[14] D.L.G. Filho and P.S.L.M. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," IACR Cryptology ePrint Archive, vol. 2006, p. 150, 2006.
[15] 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.
[16] 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.
[17] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," G.C. Hunt, ed., 2007.
[18] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditableecure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[19] 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.
[20] 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," P.F. Syverson, eds., pp. 598-609, 2007.
[21] 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.
[22] C.C. Erway, A. Ku¨ pc¸u¨ , C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security, A.D. Keromytis, eds., pp. 213-222, 2009.
[23] 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.
[24] 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.
[25] 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.
[26] 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.
[27] 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.
[28] 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.