INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY ON ENABLING EXTERNAL AUDITING FOR STORAGE SECURITY IN CLOUD COMPUTING

Suganya S[1] , Roshni Thanka M[2]

[1] Post-Graduate Student, Department of Computer Science and Engineering, Karunya University, India
[2] Assistant professor, Department of Computer science and Engineering, Karunya University, India

Abstract - Cloud computing is a model for enabling on-demand high quality applications and services from shared pool of configurable computing resources. Using cloud storage users can be able to store their data without bothering about its storage correctness. So, the user will not have any confirmation about the outsourced data. The cloud data storage should have some mechanism to verify storage correctness and its integrity. All the existing technique can verify the integrity of outsourced data only if the data is static. In this paper we propose a privacy preserving public auditing for secure cloud storage which supports dynamic data and batch auditing.
.

Keywords: Data Security, Public Audit ability, Batch Auditing, Data Dynamics

I. INTRODUCTION

A cloud computing is a distributed computing system which provides delivery of computing services over the internet. Some of the examples of cloud storage are online data storage, social networking, online business application sites and webmail. The essential characteristics of cloud computing are on-demand service, broad network access, resource pooling, rapid elasticity and measured service [18]. There are three service models in cloud computing which include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service(IaaS) [18]. The deployment models of cloud computing are private cloud, community cloud and public cloud [18].

Cloud computing provides almost unlimited storage capacity. So, user need not worry about increasing their current storage space availability. And also backup and recovery is much simpler than other data storage techniques. In cloud computing one of the field to be considered is security. While storing information to the cloud , the user should be aware of external hack attacks. And cloud server may sometimes leak users sensitive information to Third Party Auditor (TPA). Because the Third Party Auditor (TPA) can be able to download entire data for its integrity verification.

The Provable Data Possession (PDP) allows a client to efficiently, frequently and securely verify the server who stores users outsourced data and is not cheating them [2]. The client have to verify that the server has retained data file without retrieving the data from the server and without the server need to access the entire file [1]. Using public cloud, the user need to check the data from each cloud one by one and it may cause communication and computation overhead [17]. Public auditability [6], [12] allows external auditor on behalf of user to verify the correctness of remotely stored data. The client sends the challenge request to the server by specifying the positions of a collection of sentinels and asking the server to return the associated sentinel value [7].

In this paper, public key based homomorphic linear authentication with random masking technique is proposed to audit user's outsourced data without learning the data content. As the individual auditing of different task can be tedious, the third party auditor performs multiple task from different users at a time. And the user can perform updates dynamically whenever they want to make any changes in their outsourced data. The three different entities involved in cloud data storage are cloud user, cloud server and third party auditor. Cloud user is the one who can store their huge amount of data in the cloud; cloud server is the one who has significant storage space and computation resources to provide data storage service. The TPA is the one who can be able to audit the outsourced data on behalf of the user.

I. COMPARATIVE STUDY

A) Symmetric Key Cryptography

The provable data possession technique is used to allow a client to efficiently, frequently and securely verify the server who stores client potentially very large amount of data [2]. That is the server might delete some part of the data or it might not store all data in cloud storage. PDP is a public key based technique which allows any verifier to query the server and POR verifies the integrity of cloud data using special blocks called sentinels [2]. The client will ask the server for randomly picked sentinels and checks whether they are intact. If the server modifies or deletes some parts of the outsourced data then sentinels will also be changed with certain probability.

Setup phase

During setup phase, the owner generates t random challenges and the corresponding answers called tokens. When the client gives a challenge request to server on data blocks D[1] ,……,D[r] ,it has to get back corresponding token. Each token is the output of a hash function. The owner can store the tokens in encrypted format at the cloud server.

Verification phase

The owner sends challenge request to server which consist of set of blocks D[1],…,D[r]. The server computes hash function of this block z = H(D[1],…..,D[r]). The server returns [z,v_i'] to owner. The owner decrypts the value v_i' and compares the value of v_i and z. If the results are same then we can easily identify that the data is not modified.

B) Probabilistic Proof

The probabilistic proof [1] allows a client to store their data at an cloud server and to verify that the server has the original data without retrieving it. The client maintains some amount of data to verify the proof. This technique uses homomorphic verifiable tags. In that tags from multiple file blocks will be combined into a single value. The client pre-computes tags for each file blocks and then stores the verification metadata with the server. The verification metadata refers the file and its tag. After receiving the challenge request from client the server generates proof of possession. Then the client will be convinced with the data without retrieving the data from server.

C) Homomorphic Verifiable Responses and Hash Index Hierarchy

Cooperative provable data possession scheme is proposed in hybrid cloud to provide dynamic data support on multiple storage servers. In this technique multiple cloud service providers can cooperatively store and maintain the client's outsourced data. The homomorphic verifiable responses and hash index hierarchy [17] provides an effective construction of cooperative provable data possession which supports any kind of updation on the client's outsourced data. Using homomorphic property, the response collected from multiple cloud service provider can be combined into a single response as a result of hybrid cloud. Hash index hierarchy is mainly proposed to store and manage the client's data in hybrid clouds.

D) Integration of Forward Error Correction Code with Spot Checking

The integration of forward error-correcting codes with remote data checking can be used to prove the possession of data which is stored in cloud. Remote data checking allows a client to periodically challenge the server in order to prove that the server possesses the exact data that was initially stored by client. The file F is encoded into F' using forward error correction code (Reed-Solomon code) [13] .

E) Sentinel based Proof of Retrievability Protocol

Proof of retrievability protocol encrypts file F and embeds a set of random check blocks called sentinels. F' denotes the file F with its associated sentinels [7]. The verifier sends the challenge request to the prover by specifying the positions of a collection of sentinels and asking the prover to return the associated sentinel value. If the prover deletes or modifies some portion of file F then the sentinel also will gets changed. The verifier can easily identify whether the portion of data has been deleted or modified.

F) Challenge Response Protocol for Multiple-Replica Provable Data Possession

This technique is used to store n number of replicas of a file in different locations of the cloud server. The client can store equal sized replicas F1,….,Fn and later it can recover the exact file from any of these replicas [14] . The data availability and reliability will be improved using this technique. If some copies of data are deleted then the original data can still be available in any of these replicas. There are three phases in multiple replica provable data possession.

-Setup: During setup phase, the client preprocesses the data file F using KeyGen and generates n number of replicas using ReplicaGen. After that the client will store these replicas and its corresponding file tag at the server

-Challenge: The client will send either individual challenge or entire challenge request to the cloud server. Then the server will send the response back to the client.

-Replicate: Using ReplicaGen the client can create and maintain n number of replicas.

TABLE 1
PERFORMANCE PARAMETERS

Parameters	Availability	Reliability	Security	Public auditability	Batch auditing	Dynamic data	Computation overhead
Symmetric Key Cryptography	√	√	√	-	-	√	Low
Probabilistic Proof	-	-	√	√	-	-	Low
Homomorphic Verifiable Responses and Hash Index Hierarchy	-	-	√	-	-	√	Medium
Integration of Forward Error Correction Code with Spot Checking	-	√	√	-	-	-	Low
Sentinel based Proof of Retrievability Protocol	-	-	√	√	-	√	High
Challenge Response Protocol for Multiple-Replica Provable Data Posession	√	-	√	-	-	√	Low

I. CONCLUSION

The overall study of various techniques in the comparative study gives clear idea about the different mechanisms used to secure the data stored in the cloud. All the previous technique does not provide support for dynamic data and multiuser setting. In this paper, a privacy-preserving public auditing for secure cloud storage is proposed. The homomorphic linear authenticator and random masking technique is utilized to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server. Using batch auditing protocol TPA may concurrently handle multiple audit sessions from different users for their outsourced data files.

REFERENCES

[1] Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ’07), pp. 598-609, 2007.

[2] Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Int’l Conf. Security and Privacy in Comm. Networks (SecureComm ’08), pp. 1-10, 2008.

[3] Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Storage Security in Cloud Computing,” Proc.IEEE INFOCOM ’10, Mar. 2010.

[5] Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. ACM Conf. Computer and Comm. Security (CCS ’09), pp. 213-222, 2009.

[6] Govinda, V. Gurunathaprasath, H. Sathishkumar, “Third Party Auditing for secure data storage in cloud through digital signature using RSA”, International Journal of Advanced Scientific and Technical Research, (ISSUE 2, VOLUME 4- August 2012).

[7] Juels and J. Burton, S. Kaliski, “PORs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Comm. Security (CCS ’07), pp. 584-597, Oct. 2007.

[8] 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, 2009.

[9] 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.

[10] M.A. Shah, R. Swaminathan, and M. Baker, “Privacy-Preserving Audit and Extraction of Digital Contents,” Cryptology ePrint Archive, Report 2008/186, 2008.

[11] Makhija, V. Gupta, I. Rajput, “ Enhanced Data Security in Cloud Computing with Third Party Auditor”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 2, February 2013.

[12] 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 and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[13] R. Curtmola, O. Khan, and R. Burns, “Robust Remote Data Checking,” Proc. Fourth ACM Int’l Workshop Storage Security and Survivability (StorageSS ’08), pp. 63-68, 2008.

[14] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-Replica Provable Data Possession,” Proc. IEEE Int’l Conf.Distributed Computing Systems (ICDCS ’08), pp. 411-420, 2008.

[15] 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 and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug.2008.

[16] Shacham and B. Waters, “Compact Proofs of Retrievability,”Proc. Int’l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107,Dec. 2008.

[17] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. Yau, “Efficient Provable Data Possession for Hybrid Clouds,” Cryptology ePrint Archive, Report 2010/234, 2010.

[18] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloudcomputing/
index.html, June 2009.