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

# The Cloud Storage, Enabling Audit is the Main Opposition Threat

**U.Meena**
**M.Tech,**
**Dept of Computer Science Engineering,**
**Christu Jyothi Institute of Technology & Science.**

**A.Poorna Chandra Reddy**
**Associate Professor,**
**Department of Computer Science and Engineering,**
**Christu Jyothi Institute of Technology & Science.**

## ABSTRACT:

Check to verify the integrity of data in the public cloud, cloud storage is considered an important service. The concept of a secret key of the current audit protocols are completely safe for the customer based on the audit. However, the client cannot be held due to weak sense of safety and / or security settings do not get that feeling. The current audit protocol auditing, should be able to work on the disclosure of a secret key. In this paper, we focus on the case of this new cloud storage audit. How can we reduce the loss of the audit client's key cloud storage, and set up the first practical solution to this problem is to make possible a new study. The main risk we audit protocol definition and the flexibility and security model formally proposed such a protocol. Our design system is not a binary tree traversal and the secret keys in the front line of customer technology update job. We are in favor of a new authenticator security building blocks for developing a low-sourcing and property. Proof of safety and efficacy study show that our proposed protocol is safe and effective.

## INTRODUCTION:

The audit protocol can support dynamic data operation. Cancel the user of these proxy audit auditing certification management, and cloud storage, eliminating the other factors studied. In recent years, many research works, cloud storage, cloud storage, audit, audit risk issues, an important security problem has been found in previous research. All protocols are already a client error, or are in the cloud, security dishonesty focus and / or a strong sense of safety systems to reduce ignored. Unfortunately, the previous audit protocols and client secret key audit work on this important issue, to properly consider any accident, unable to make the most of the audit protocol. Loss of key customers, we focus on cloud storage to reduce the risk of audit. Built-in flexibility to significant risks, our goal is to build a cloud storage audit protocols. It brought many new challenges under the new issue of how to effectively addressed by the state. We are the first major cloud storage, the risk of an audit before the show we give to our original protocol, the two primary solutions to the problem. An innocent, it is not the first solution to solve the problem. The second problem can be solved with a good solution, but it is a big burden. They are impractical when applied to the original settings. Then we give the solution more efficient than our basic protocol. Simple solution: In this solution, the customer can still use traditional methods of key revocation. Once the audit client to know his secret key stored in the cloud, it will be canceled, to reveal the secret and the corresponding public key.

Meanwhile, the public key and secret key and the public key certificate to produce a new set, a new update will be released. Authenticators data already in the cloud, however, because of the need to secure all the old secret key stored no longer be updated. Therefore, your data is already preparing their new authenticators, stored in the cloud client, and then uploaded to the cloud, a new secret key is required to download the new authenticators. Clearly, it is a complex process, and consumes a lot of time and resources. Also, the secret key, it is stored in the cloud cloud auditing, data blocks have changed since,, and authenticators. Authenticator's data will be downloaded from the cloud to ensure the accuracy of customers and it is very difficult to do. Therefore, the primary recovery of the secret key and the public key cannot solve this problem. A better solution: (B) (B 1, S1 in), (P 2 S 2), • • • Customer and secret keys at the

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

beginning of a series of output keys. Let the public key (p 1; • • •; B, D), Jammu and secret key term (s j, • • •, SK). Jammu and upload files to the cloud customer's time, so the file the client uses to compute authenticators S T authenticators client will then upload files to the cloud. The affected files, audit, client authenticators SJ The fact that the files are produced by BK When in use to verify that. J J + 1 change, remove the customer's own store. After the new secret key (S JJ + 1, S t, • • •, SK This solution is clearly better than the linear solution. What point jj) First of all, the key to cancel the traditional solution of cloud storage audit it is not practical to apply. Because the public key and secret key and customer data stored in the cloud revitalization authenticators first audit client, customer, product disclosure of a secret key, while there is a new pair. In the process of manufacturing new authenticators, and re-download all of which included the difficult and complex and will need to reload the data from cloud to cloud. And when the customer cannot guarantee that the new authenticators, it cannot reproduce the actual data in the cloud. Secondly, it fixed the main problem is not suitable for the installation of new technology adoption. It is the actual file blocks leads to the confirmation again. The reason for this is technology that is incompatible with the module verification. Authenticators As a result, the audit unacceptably high compute and storage costs, lead to information will not be collected.

## SYSTEM PRELIMINARIES:

### PUBLIC KEY & SECRET KEY:

Public key authentication for logging in to the specification of this module is to provide the user. Secret secret key generated at the time of registration for each candidate

### FILE STORAGE:

To view the options for the user to use the time and provided the key to the archive file and the file can download the file storage volume.

### GENERATE TIME PERIOD KEY:

Perform operation of our critical files on the ice to win this time.

### INDEXING OF THE FILES:

Operation is key to download the file specified by thinking beside perform for the success of, please download the product using the view of snow indexing files.

### VIEW AND DOWNLOAD FILES:

Key authentication viewed playback file is based in the Gulf can be downloaded to the user.

### AUDITOR PUBLIC KEY:

Auditor public key is created to manage the operation of all the modules is important for all

### RELATED WORK:

The integrity of data stored on a remote server, the proposed protocol [1-12, 14, 30] to verify a number of. Public-private authentication and verification, high-capacity, verification, data stateless, dynamic action, confidentiality, etc., preserving the role of the auditor is to focus on the different requirements of these rules, the audit protocol two categories can be divided into. Verifiability a private audit protocol, a secret listener or not to testify is provided for the other parties. The auditor can verify the data integrity. However, the verification protocol verification algorithm with a secret key with the listener does not require public verifiability. Therefore, third-party auditor to audit protocol is such a role. Ateniese et al. Considered unreliable data storage and entered the first public certification, "provable data possession" to ensure (PDP) proposed the concept. HLA they outsource data verification and random sampling techniques. Juels and Kaliski Jr. (POR) models' proof of recovery "are explored. They seized files on remote storage systems, and the error correction code and the tools used to ensure recovery spotchecking.

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

Shacham and Waters has two small and efficient homogenous authenticators: a fictional work based on personal verifiability, other BLS signing is based on public verifiability Dodis et al ROP focuses on the study of different types of work ... Shah et al. TPA a launches online store to be honest. the protocol requires the auditor to perform a safe state, and limits the use suffers. Wang et al., provided to protect the privacy of the property by a public audit protocols. in order property to protect the privacy protocol to realize, they integrate with HLA random masking technique. Wang proposed proxy protocol provable data capture. in this protocol, data integrity proxy client to work with representatives of their verification for. Flexible auditing services, data activity is studying to be a dynamic verification. Ateniese et al.First proposed a partial dynamic PDP. Wang et al. Dynamic data supports the proposed audit protocols. In this protocol, HLA-based BLS and Merkle hash tree used to support dynamic data. Erway et al. PDP supports and abandon a proposed protocol, based on the dynamics of the extended mode with the list. Zhu et al. The data audit proposed to take over a colleague's evidence to support dynamic protocol can be extended.

Yang Jia and duty to protect the confidentiality of the proposed protocol is a dynamic audit. Cloud storage should take the issue of canceling the user authentication. Pour some of the new version of the dynamic control systems have been studied and practicable to outsource. To verify the assumption that the client's secret key, perfectly safe for most of the protocols are built on and cannot be disclosed. But as we have shown in the past, this offer may not be always true. Under the new issue of our workplaces, cloud storage, auditing, major advances in how I perform in the resistance to achieve.

## CONCLUSION:

We audit client cloud storage is the key to dealing with the response to the need to study. Agility is the key with the exhibition, we have proposed a new paradigm validation protocol. Such a code of conduct, integrity of data stored in the cloud, cloud storage is still auditing the current secret key customer risk is observed. We audit and the proposed security model for authorization first key-response protocol definition and agility with practical solutions. Evidence of safety and performance evaluation of the proposed protocol is safe and effective asymptotic show.

## REFERENCES

[1] G. 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 andComm. Security, pp. 598-609, 2007.

[2] G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc.4th International Conference on Security and Privacy inCommunication Networks, 2008.

[3] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPPDP: Multiple-Replica Provable Data Possession," Proc.28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

[6] 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.

[7] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on

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

Computer andCommunications Security, pp. 756-758, 2010.

[8] 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.

[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.

[10] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, Vol. 62, No. 2, pp. 362- 375, 2013.

[11] 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 andDistributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[12] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Trans. on Services Computing, vol. 6, no. 2, pp. 409-428, 2013.

[13] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Proc. of the 16thACM conference on Computer and communications security, pp. 213-222, 2009.

[14] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, Vol. 6, no. 4, pp. 551-559, 2013.

[15] B. Wang, B. Li, and H. Li. "Public auditing for shared data with efficient user revocation in the cloud," INFOCOM2013 Proceedings IEEE, pp. 2904-2912, 2013.

[16] H. Wang, Q. Wu , B. Qin, and J. Domingo-Ferrer, "Identity-based remote data possession checking in public clouds," IET Information Security, vol.8, no. 2, pp. 114- 121, March 2014.

[17]T. Stewart, "Security Policy and Key Management: Centrally Manage Encryption Key," http://www.slideshare.net/Tina-stewart/security-policyand-enterprise-key-management-from-vormetric. August, 2012.

[18]Microsoft, http://technet.microsoft.com/en-us/library/cc961626.aspx, 2014.

[19]FBI, http://www.fbi.gov/news/news blog/is-yourcomputer-infected-with-dnschanger-malware, 2012.

[20] FBI, http://www.fbi.gov/news/stories/2011/april/botnet 041411, 2011.