IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

Cloud Storage Auditing with Key-Exposure Resistance

Bhalshankar Sahebrao Tanaji[1], Prof. Phatak Amol A.[2]

Department of Computer Science and Engineering, NBN Sinhgad College of Engineering, Solapur, Maharashtra, India[1]

Head of Department, Computer Science and Engineering, NBN Sinhgad College of Engineering, Solapur, Maharashtra, India[2]

ABSTRACT: As data is dynamically updated in today's world, the existing remote integrity checking methods which served as a purpose for static data can no longer be enforced to authenticate the integrity of dynamic data in the cloud. In this scenario, cloud storage auditing conveys an efficient and secure dynamic auditing protocol which draws a confidence to the data owners that their data is correctly stored in the cloud. The present auditing protocols assume that the secret key of the client is very secure while in reality, it is not. Thus, to overcome these flaws, this paper introduces an idea of lessening the client's secret key disclosure. In this paper, we propose a system where de-duplication strategy of data is adopted and it will check the delicacy of data and eliminate the redundant one using MD5 hashing. Also, it uses tile bitmap method wherein it will check the previous and the current versions of the data to ease the auditor's workload and to make the system more efficient.

KEYWORDS: cloud storage auditing, homo-morphic linear authenticator, cloud computation, key-exposure resistance, Data Storage.

I. INTRODUCTION

Cloud Computing delivers us a path by which we can easily get access to all the applications as utilities worldwide on the internet. Also, it helps us to create any application or customize and configure the same. Firstly we will see as to what a cloud means. Cloud refers to a network of applications. In other words, we can say that cloud is something, which is remotely located. Cloud grants services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Many applications such as e-mail, video or audio conferencing, customer relationship management (CRM), all run in cloud. Cloud computing basically means manipulation, configuration and ability to access the applications online on internet. Its prime benefit is that it offers data storage and reduces cost which is beneficial for a large number of end users all across the world. The most bothering concern about cloud computing is its security and privacy. Since the whole data management and infrastructure management in cloud is done by a third-party, it is always a compelling task to handover the data as it is not trusted. However, the cloud computing vendors ensure many more secure password protected accounts, as a result of which any sign of security violation would lead to loss of clients and businesses. Cloud storage is a model where data is stored uniformly and maintained which is made available to end users over a large scale network. The end users access data from each and every part of the world.

Storage outsourcing into the cloud is very much cost beneficial and also assists in intricacy of large-scale data storage for long term use. So even if any kind of disruption occurs locally at the client's site, the data which has been uploaded in the cloud will be available for access which the client can download later. Meanwhile, such a service is also wiping out data owner's legitimate control over the future of their data, which they have traditionally forecasted with high service-level requirements. Also, the large amount of data in the cloud and owner's limited computational capabilities further makes the task of storage auditing in a cloud environment expensive and even dismaying for individual clients. Clients will hesitate to store data in cloud if it is a matter of their data security and integrity. For this reason, the Third Party Auditor (TPA) was introduced which is nothing but a software which plays an important role in auditing the integrity and privacy of the data. The TPA, is nothing but a third party software which has the expertise and capabilities that users do not possess, also it can periodically check the integrity of the overall data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

storage correctness in the cloud. Cloud Storage Auditing is basically a scenario where the Third Party Auditor (TPA) audits or checks the integrity of the data in the cloud to see if any unauthorized person or organization has modified the data in any way since the data has been stored in the cloud. This was a major issue since the data can be forged too, which if produced would be invisible to the client. So, in order to maintain the authenticity of the data and to lessen the burden of reckoning and exchanging information in auditing protocols, Homomorphic Linear Authenticator (HLA) technique was studied which permits the auditor to verify the genuineness of the data in the cloud without fetching the whole data. This is also termed as verification. Several cloud storage auditing protocols likewise have been proposed on the basis of this technique.

II.LITERATURE SURVEY

As the previous section reveals various methodologies for enabling cloud storage auditing, but still there is a huge gap to meet the perfection. So, as a step towards this, this paper tried to grab many concepts so that a new and efficient system can be proposed. The detailed studies are as follows. In, a thorough survey of various methods of cloud storage auditing is performed. Few existent methods have been analyzed and the challenged faced have been described in order to make an efficient protocol. When we store the data, the different version of the data is also stored uniformly. Thus, for the minimization of storage overhead, “delta encoding” was adopted wherein the differences between the versions was noted. A specific type of delta encoding, skip delta encoding was adopted to optimize the added cost of storing and retrieving the data. K. Yang et al, introduced a framework for auditing data storage in the cloud and also proposed an efficient privacy-preserving auditing protocol. Furthermore, it was extended to support dynamic operations like addition, deletion or modification of data explains the method of auditing the service dynamically to verify the integrity of a non-trustable and outsourced storage on the basis of fragment structure, random sampling, and index-hash table, which also supported updates to the data outsourced and anomaly detection time to time.

In, the authors have tried to improve the existing proof of storage models by using Merkle Hash Tree (MHT) construction for block tag authentication. In, the authors have presented two provably-secure PDP schemes which are more efficient than the aforementioned solutions, even when compared with schemes that achieve weaker guarantees. Furthermore, extends the previous work on data possession proofs by the Multiple Replica Provable Data Possession (MR-PDP) for a single copy of a file in a client/server storage system introduces a mechanism of storage integrity auditing which permits the end users to compute the cost along with achieving fast data error localization, i.e it identifies if any server misbehaves. However, for an efficient auditing, a much more secure cloud storage system was proposed which supported privacy-preserving public auditing and the results were extended so that TPA could perform audits for multiple users at the same time and also execute it efficiently. Thus, in all the above works the cloud storage auditing is tried to make more efficient in various ways. As we all are already aware that the public key and the secret key play an important role in the encryption and the decryption of the data. If the secret key is exposed, it may lead to data forging and can get in hands of any unauthorized user narrate an idea of public key encryption which uses the concept of Binary Tree Encryption (BTE) wherein there is a master public key associated with the tree.

Every node has a corresponding secret key and to encrypt a message destined for a particular node, one uses both public key and the name of the target node. The cipher text which comes as a result can then be decrypted using the secret key of the target node. Now, at least one secret key is used to sign the message in the current time-period and then obtain the secret key for the next time-period. As in the typical signature scheme, the public key is stable for all time- periods. A verification scheme checks both the validity of the signature and its time-period. The signature scheme is forward secure because it might happen that signature can be forged for the previous time period even if it has the current secret key. As we discussed regarding the encryption of the keys, introduced the concept of key-insulated security whose aim was to lessen the damage caused by secret key exposure this was needed as usually cryptographic computations are performed on insecure devices. Thus, in this paper model has been proposed wherein the secret key stored on the insecure device are refreshed at various time periods along with a physically secure device which already possess the master key.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

III. EXISTING AND PROPOSED SYSTEM

A. EXISTING SYSTEM

These protocols focus on several different aspects of auditing, and how to achieve high bandwidth and computation efficiency is one of the essential concerns. For that purpose, the Holomorphic Linear Authenticator (HLA) technique that supports block less verification is explored to reduce the overheads of computation and communication in auditing protocols, which allows the auditor to verify the integrity of the data in cloud without retrieving the whole data. The privacy protection of data is also an important aspect of cloud storage auditing. In order to reduce the computational burden of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to get the client's data after it executes the auditing protocol multiple times. Wang et al. have proposed an auditing protocol supporting fully dynamic data operations including modification, insertion and deletion.

Disadvantages of Existing System:

- Though many research works about cloud storage auditing have been done in recent years, a critical security problem the key exposure problem for cloud storage auditing, has remained unexplored in previous researches.
- While all existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible weak sense of security and/or low security settings at the client.
- Unfortunately, previous auditing protocols did not consider this critical issue of how to deal with the client's secret key exposure for cloud storage auditing, and any exposure of the client's secret auditing key would make most of the existing auditing protocols unable to work correctly.

B. PROPOSED SYSTEM

In this paper, we focus on how to reduce the damage of the client's key exposure in cloud storage auditing. Our goal is to design a cloud storage auditing protocol with built-in key-exposure resilience. How to do it efficiently under this new problem setting brings in many new challenges to be addressed below. First of all, applying the traditional solution of key revocation to cloud storage auditing is not practical. This is because, whenever the client's secret key for auditing is exposed, the client needs to produce a new pair of public key and secret key and regenerate the authenticators for the client's data previously stored in cloud as shown in Fig.1. Our goal is to design a practical auditing protocol with key- exposure resilience, in which the operational complexities of key size, computation overhead and communication overhead should be at most sub-linear to T. In order to achieve our goal, we use a binary tree structure to appoint time periods and associate periods with tree nodes by the pre-order traversal technique. The secret key in each time period is organized as a stack. In each time period, the secret key is updated by a forward-secure technique. The auditing protocol achieves key-exposure resilience while satisfying our efficiency requirements. As we will show later, in our protocol, the client can audit the integrity of the cloud data still in aggregated manner, i.e., without retrieving the entire data from the cloud.

Advantages of Proposed System:

- We initiate the first study on how to achieve the key- exposure resilience in the storage auditing protocol and propose a new concept called auditing protocol with key- exposure resilience.
- In such a protocol, any dishonest behaviors, such as deleting or modifying some client's data stored in cloud in previous time periods, can all be detected, even if the cloud gets the client's current secret key for cloud storage auditing.
- This very important issue is not addressed before by previous auditing protocol designs. We further formalize the definition and the security model of auditing protocol with key-exposure resilience for secure cloud storage.

We design and realize the first practical auditing protocol with built-in key-exposure resilience for cloud storage. In order to achieve our goal, we employ the binary tree structure, seen in a few previous works on different cryptographic designs, to update the secret keys of the client. Such a binary tree structure can be considered as a variant of the tree structure used in the HIBE scheme. In addition, the pre-order traversal technique is used to associate each node of a binary tree with each time period. In our detailed protocol, the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

stack structure is used to realize the pre-order traversal of the binary tree. We also design a novel authenticator supporting the forward security and the property of block less verifiability.

- We prove the security of our protocol in the formalized security model, and justify its performance via concrete asymptotic analysis. Indeed, the proposed protocol only adds reasonable overhead to achieve the key-exposure resilience. We also show that our proposed design can be extended to support the TPA, lazy update and multiple sectors.

IV.EXPERIMENTAL RESULTS

SCREENSHOT

HOME:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

CLIENT LOGIN:

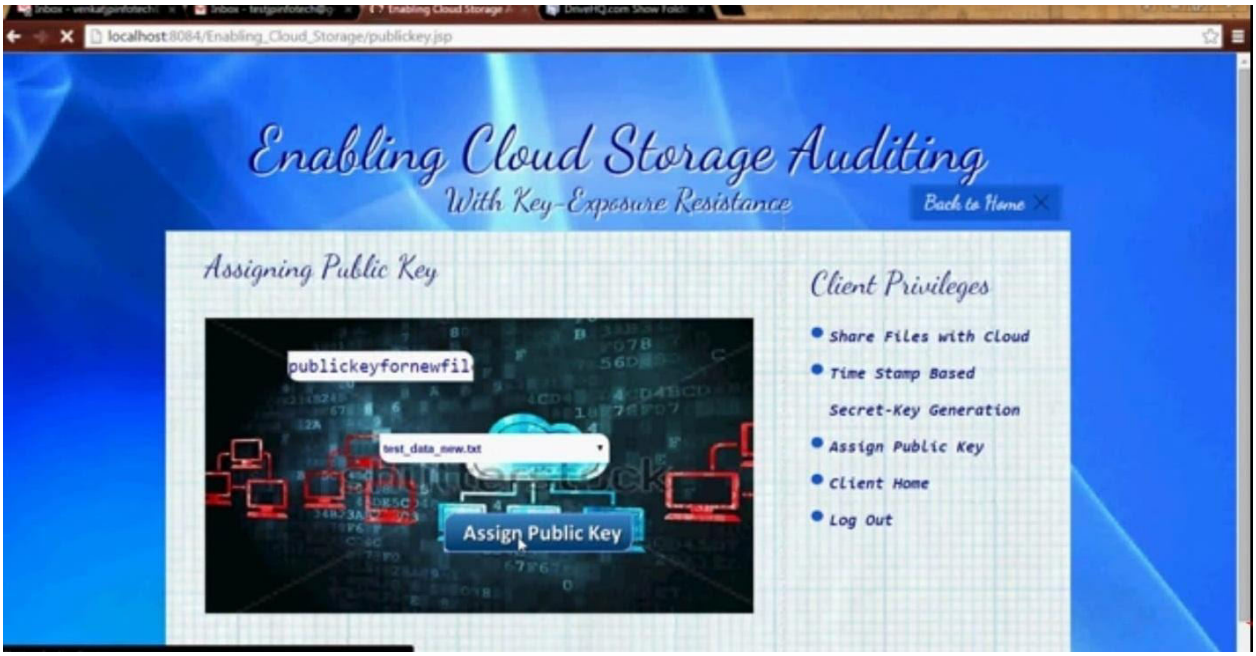
REGISTRATION:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

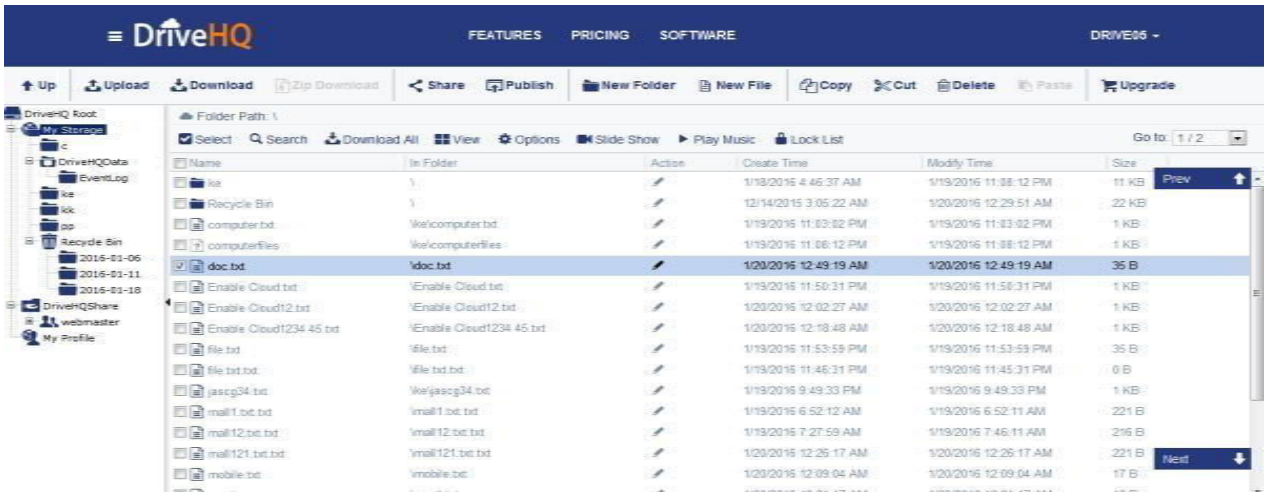
|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

Assign Public Key:



FILE STORED INTO CLOUD:



V. CONCLUSION

As this complete paper narrates the different methodologies on enabling cloud storage auditing with key exposure resilience, but none of the methodologies seems to be perfect. So, this survey paper as a bit proposes a method of an effective key exposure resistance where we adopt the de- duplication strategy of data. Moreover, it will check the duplicity of data and eliminate the redundant one using MD5 hashing algorithm. After the public and private keys are generated, it uses tile bitmap method wherein it will check the previous and the current versions of the data to ease the auditor's workload and to make the system more efficient.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 7, July 2021 ||

| DOI:10.15680/IJIRSET.2021.1007192|

REFERENCES

1. Jia Yu, Kui Ren, Senior Member, IEEE, Cong Wang, Member, IEEE and Vijay Varadharajan, Senior Member, IEEE, "Enabling Cloud Storage Auditing with Key-Exposure Resistance", IEEE Transactions on Information Forensics And Security, Vol Xx . , No1. , 2015.
2. 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 and Comm. Security, pp. 598-609, 2007.
3. 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 in Communication Networks, 2008.
4. 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.
5. 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.
6. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, 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 Computer and Communications 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. 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 and Distributed 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details