International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 09, September 2017
ISSN: 2455-3778
http://www.ijmtst.com

Cloud Storage Auditing Using Key Abstraction with Data Security

M.Praveena

Lecturer, Department of Computer Science, Sri Durga Malleswara Siddhartha Mahila Kalasala, Vijayawada, India.

To Cite this Article
M.Praveena, "Cloud Storage Auditing Using Key Abstraction with Data Security", International Journal for Modern Trends in Science and Technology, Vol. 03, Issue 09, September 2017, pp.121-125

ABSTRACT

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. The large amount of data is stored in the cloud. To verify the integrity of a data which is stored on the cloud, the cloud storage auditing is used. Auditing is an integrity check in the cloud data base. It is an important checking in the cloud auditing protocols that are highly researched on recent years. Each protocols act as a different auditing mechanism. The aim of introducing the protocol is to achieve high bandwidth and computation efficiency. Most of the auditing protocols are based on the assumption that the client's secret key for auditing is secure. The security is not fully achieved, because of the low security parameters of the client. If the auditing protocol is not secured means the data of the client will exposed inevitably. In this paper a new mechanism of cloud auditing is implemented. And investigate to reduce the damage of the client key exposure in cloud storage auditing. Here the designing is built upon to overcome the week key auditing process. The auditing protocol is designed with the help of key exposure resilience. The privacy protection of data is an important aspect of cloud storage auditing. It is used to reduce the computational burden of the client. The third party auditor is introduced to help the client to periodically check the integrity of data in cloud. Auditing protocols are for the privacy of data in cloud.

Keywords *— Cloud Storage Auditing, Client Key Exposure, data storage.*

I. INTRODUCTION

In recent years, auditing protocols for cloud storage have attracted much attention and have been researched intensively. 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 Homomorphism 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. Many cloud storage auditing protocols like have been proposed based on this technique. 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. Auditing protocols are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations. An n get al. has proposed an auditing protocol supporting fully dynamic data operations including modification, insertion and deletion. Auditing protocols can also support dynamic data operations.

Key exposure could happen due to several reasons: 1) Key management- Key management is a process which is done by the client. In case any fault occurs and if the client is using a cheap software-based key management, then key exposure is possible. 2) Internet based security attacks- Suppose if a client downloads any data or file and if that it contains malicious program, then it may infect the system. This allows the hackers to easily access any confidential data [4]. 3) Trading with hackers- It can happen that cloud also earns incentives by trading with the concerned hackers. In this process, the cloud can get the client's data and forge the authenticator by regenerating false data or by hiding data loss. Thus, dealing with key exposure is a vital issue in cloud storage and various methodologies were adopted. Other aspects, such as proxy auditing, user revocation and eliminating certificate management in cloud storage auditing have also been studied. 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. In fact, the client's secret key for cloud storage auditing maybe exposed, even known by the cloud, due to several reasons. Firstly, the key management is a very complex procedure which involves many factors including system policy, user training, etc. One client often needs to manage varieties of keys to complete different security tasks. Any careless mistake or fault in managing these keys would make the key exposure possible.

II. IMPLEMENTATION

Client:

The client produces files and uploads these files along with corresponding authenticators to the cloud. The client can periodically audit whether his files in cloud are correct. The client will update his secret keys for cloud storage auditing in the end of each time period, but the public key is always unchanged.

TPA:

In order to reduce the computational burden of the client, a third-partyauditor (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. Auditing protocols are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations.

Cloud:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Key Exposure Resistance:

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. There is a one- time public key sharing for each file and a Time Stamp based secret key Generation. For each instance the timestamp based key exposure will be vary according to the current time stamp.

III. LITERATURE SURVEY

1) Toward publicly auditable secure cloud data storage services

AUTHORS: C. Wang, K. Ren, W. Lou, and J. Li,

Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements. In order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on-demand data correctness verification on behalf of cloud data owners have to be designed. In this article we propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public auditability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners¿ computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. We describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.

2) Data storage auditing service in cloud computing: Challenges, methods and opportunities

AUTHORS: K. Yang and X. Jia

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. In this paper, we investigate this kind of problem and give an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, we introduce some existing auditing schemes and analyze them in terms of security and performance. Finally, some challenging issues are introduced in the design of efficient auditing protocol for data storage in cloud computing.

3) An efficient and secure dynamic auditing protocol for data storage in cloud computing

AUTHORS: K. Yang and X. Jia

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.

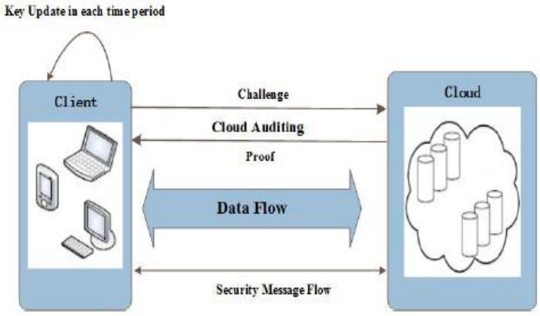
4) Privacypreserving public auditing for secure cloud storage

AUTHORS: C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

IV. RELATED WORK

The Key exposure resilience in the storage auditing protocol is not fully supported in the existing system this mechanism is used to detect any dishonest, such as deleting or modifying some client's data that is stored in the cloud in previous time periods can all be detected, even if the cloud gets the clients current secret key for cloud storage auditing. Auditing protocols can also support dynamic data operations. Other aspects, such as proxy auditing, user revocation and eliminating certificate management in cloud storage auditing have also been studied. Though many research works about cloud storage auditing have been done in recent years, a critical security problem 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, and any exposure of the client's secret auditing key would make most of the existing auditing protocols unable to work correctly. 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. The process involves the downloading of whole data from the cloud, producing new authenticators, and re-uploading everything back to the cloud, all of which can be tedious and cumbersome. Besides, it cannot always guarantee that the cloud provides real data when the client regenerates new authenticators. Secondly, directly adopting standard key-evolving technique is also not suitable for the new problem setting. It can lead to retrieving all of the actual files blocks when the verification is preceded. This is partly because the technique is incompatible with block less verification. The resulting authenticators cannot be aggregated, leading to unacceptably high computation and communication cost for the storage auditing.



V. CONCLUSION AND FUTURE WORK

In this paper, study on how to deal with the client's key exposure in cloud storage auditing. We propose a new paradigm called auditing protocol with key-exposure resilience. In such a protocol, the integrity of the data previously stored incloud can still be verified even if the client's current secret key for cloud storage auditing is exposed. We formalize the definition and the security model of auditing protocol with key-exposure resilience, and then propose the first practical solution. The security proof and the asymptotic performance evaluation show that the proposed protocol is secure and efficient.

In future, data to the Cloud and it is difficult to monitor the data and checking the process in offline. Thus data owner stands in online for integrity checking. This can be achieved by introducing Proxy component to check for the integrity. This is an added advantage to the data owner that he need not stay online for integrity checking. The data owner provides a key to the proxy server using that key proxy is responsible for checking the data.

REFERENCES

[1] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[2] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.

[3] F. Sebe, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information

infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

[5] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology—ASIACRYPT. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.

[6] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./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," in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 756–758.

[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 Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans Comput., vol. 62, no. 2, pp. 362–375, Feb. 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 Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

[12] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

Author Profile:

M.Praveena is presently working as Lecturer, Dept. of Computer Science, Sri Durga Malleswara Siddhartha Mahila kalasala,Vijayawada, A.P., India. She has ten years of experience in teaching field, her area of interests are cloud computing & Big Data.

E-Mail: veena1011@gmail.com