International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Continuous Auditing Approach to the Cloud Service Addressing Attributes of Security

Dr. S.V.M.G. Bavithiraja[1], Mahimasubahari M[2], Mohana Priya K[3], Nishanthini T[4], Pandilakshmi SV[5]

[1]Professor, Department of Computer Science and Engineering, Sri Eshwar College of Engineeering, Coimbatore, Tamilnadu-641202

[2,3,4,5]UG Students, Department of Computer Science and Engineering, Sri Eshwar College of Engineeering, Coimbatore, Tamilnadu-641202

Abstract - *Cloud services (CS) attempt to assure a high level of security and compliance. However, considering that cloud services are multi-year validity periods may put in doubt reliability of such certification and part of an ever-changing environment. We argue that continuous auditing (CA) of selected certification criteria is required to increase trustworthiness of certificates and thereby to assure continuously secure and reliable cloud services. In this work we propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public audit ability, a trusted entity with capabilities and expertise data owners do not possess can be delegated as an external audit party when needed; they can assess the risk of outsourced data. Such an auditing service not only helps us to save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trustworthiness in the cloud. Thus we enhanced customer/user interaction between Owner and cloud server also in this concept. We describe approaches and system requirements that should be brought into consideration, and outline test that need to be resolved for such a publicly auditable secure cloud storage service to become a reality.*

Key Words: **Continuous Auditing (CA), Third Party Auditing (TPA), Message Authentication codes (MAC).**

1. INTRODUCTION

Existing System a straightforward approach to protect the data integrity would be using traditional cryptographic methods, such as the well-known public key encryption method. Initially, data owners can locally maintain a small number of keys for the data files to be outsourced. Whenever the data owner needs to retrieve the file, she can verify the integrity by recalculating the key of the received data file and comparing it to the locally pre computed value. This method allows data owners from the cloud, to verify the correctness of the received data and it does not give any assurance about the correctness of other outsourced data. In other words, it does not give any guarantee about the data in the cloud are actually intact, unless the data are all downloaded by the owner. Because the amount of cloud data can be large, it would be quite impractical for a data owner to retrieve all the data just in order to verify the data is still correct. If the data auditing task is assign to a TPA, this method inevitably violates our suggested requirements, data privacy exposure to the TPA (for retrieving a local copy of data) and with large auditing cost is reduced in a cloud server.

2. Working Procedure

We begin with a high-level architecture description of cloud data storage services illustrated following Fig. 1. The architecture consists of four entities.

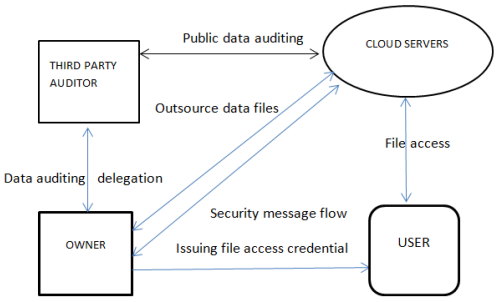

FIG -1: Core Architecture

2.1. Data Owner

If the data owner is new one he/she registered the name and password after he/she entered into the cloud server for storing their data. Else existing user directly login to the Cloud server and enter their data in the cloud server. Data owner regularly watches the updates from the third party auditor. The data owner has own mac address with help of this mac address user going to login the cloud server. While users have a privilege of reading files, then only the data owner can dynamically interact with the CS to update her stored data.

2.2. Cloud server

Cloud computing has been envisioned as the future generation architecture of enterprise IT. It's provides unparalleled advantages in IT: On demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, usage-based pricing and low transference of risk. In most cases cloud data storage

services also provide benefits: Availability being able to access data from anywhere, Relative low cost paying as a function of need users and such a user's are in a collaboration team or employees in the enterprise organization.

3. Third party auditor

Here the TPA is "the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon a request. "The data owner under the cloud paradigm, "may represent either the enterprise the individual or customer, who relies on the cloud server for remote data maintenance and storage and thus is relieved of the burden of maintaining and building maintaining local storage infrastructure. "Within the scope of this article, "we can focus on how to ensure publicly auditable secure cloud data storage services. "As the data owner need not hold physical control of the data for their life time, it is of critical importance to allow the data owner to verify that he/she data is being correctly stored and maintained in the cloud. Considering the possibly large cost in terms of resources and expertise, the data owner may resort to a TPA for "the data auditing task to ensure the storage security of he/she data, while hoping to keep the data private from the TPA."We assume the TPA, who is in the business of auditing, is reliable and independent and thus has no incentive to plot with either the CS or the owners during the auditing process. The TPA should be able to efficiently audit the cloud data storage without any additional online burden for data owners and without local copy of data. Besides, any possible leakage of an owner's outsourced data toward a TPA through the auditing protocol should be prohibited. We consider both a semi-trusted CS and malicious outsiders. "As potential adversaries interrupting cloud data storage services."Malicious outsiders can be economically motivated and "have the capability to attack cloud storage servers and subsequently pollute or delete owners' data while remaining undetected". The CS is semi-trusted in the sense "that most of the time it behaves properly and does not deviate from the prescribed protocol execution." However, for its own benefit the CS banned to keep or deliberately delete rarely accessed data files that belong to ordinary cloud owners. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain its reputation. Note that in our architecture, we assume that basic security mechanisms such as a preloaded public/private key pair "with each entity are already in place to provide basic communication security, which can be achieved in practice with little overhead." Third party auditor has one notice board with help of this board data owner check the details always. If suppose hacker delete the data file. Third party auditor immediately updates those deleted data file into the cloud server and the hacker details also projected this notice board.

3.1 DESIRABLE PROPERTIES FOR PUBLIC AUDITING

Our goal is to enable public auditing for cloud data storage to become realness. Thus, the whole service architecture design should not only be cryptographically strong, but more important, be practical from a systematic point of view. We briefly elaborate a set of suggested desirable properties below that satisfy such a design principle. The in-depth analysis is discussed in the next section. Note that these requirements are ideal goals. They are not necessarily complete yet or even fully possible in the current stage.

3.1.1. MINIMIZE AUDITING OVERHEAD

First and foremost, the overhead imposed on the cloud server by the auditing process must not outweigh its benefit. Such overhead may include both the input and output cost for data access and the bandwidth cost for data transfer. Any extra online burden on a data owner should also be as low as possible. Ideally, after auditing delegation, the data owner should just enjoy the cloud storage service while being worry free about storage auditing correctness.

3.1.2. Protect Data Privacy

Data privacy protection has always been an important factor of a service level agreement for cloud storage services. Thus, the implementation of a public auditing protocol should not break the owner's data privacy. In other words a TPA should be able to efficiently audit the cloud data storage without learning the data content or without demanding a local copy of data.

3.1.3. Support Data Dynamics

As a cloud storage service is not just a data depository, owners are subject to dynamically updating their data via various application purposes. The design of auditing protocol should incorporate this main feature of data dynamics in Cloud Computing.

3.1.4. Support Batch Auditing

The prevalent of large-scale cloud storage service further demands auditing efficiency. When receiving multiple auditing tasks from different owners' delegations, a TPA should still be able to handle them in fast yet cost-effective fashion. This property could essentially enable the scalability of a public auditing service under even a storage cloud with a large number of data owners.

3.1.5. ENSURING CLOUD DATA SECURITY

In this part we start from scratch and a set of building blocks that could form the basis of public auditing services for dependable cloud data storage. For some of the building blocks, we can rely on existing work or newly developed cryptographic primitives; for others, we only sketch the problem and leave it for future research.

4. Module Descriptions

4.1 PROTECTING DATA PRIVACY

The main reason for linear combination of sampled blocks may potentially reveal owner data information is due to the following fact about basic linear algebra theory: if enough linear combinations of the similar blocks are collected, the TPA can simply derive the sampled data content by solving a system of linear equations. This drawback greatly affects the security of using MAC-based techniques in a publicly auditable cloud data storage system. From the view of protecting data privacy, the owners, who own the data and rely on the TPA just for the storage security of their data, do not want this auditing process introducing new exposure of unauthorized information leakage into their data security. Moreover, there are legal regulations, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), further demanding the outsourced data not to be leaked to external parties. They utilized data encryption before deployed is the one way to reduces the privacy concern, but it is only complementary to the privacy-preserving public auditing scheme to be deployed in cloud. Without a properly designed auditing protocol, encryption itself cannot prevent data from flowing away toward external parties during the auditing process. Just they reduce it to the one of managing the encryption keys but it does not completely solve of the problem of protecting data privacy. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. To address this concern, "a proper approach is to combine the homomorphism authenticator with random masking". This is the way of linear combination of similar blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA no longer has all the necessary information to develop a correct group of linear equations and therefore cannot derive the owner's data content, no matter how many linear combinations of the same set of file blocks can be collected. Meanwhile, due to the algebraic property of the homomorphism authenticator, the correctness validation of the block-authenticator pairs (μ and σ) can still be carried out in a new way, even in the presence of randomness. This improved technique "ensures the privacy of owner data content during the auditing process, regardless of whether or not the data is encrypted, which definitely provides more adaptability for different application scenarios of cloud data storage." Besides, with the homomorphism authenticator, the desirable property of constant communication overhead for the server's response during the audit is still preserved.

4.2 SUPPORTING DATA DYNAMICS

Cloud computing is not just a third party data depository. For various application purposes, the data stored in the cloud may not only be accessed but also updated frequently by data owners. Thus, supporting data dynamics, this can be formulated as General block-level operations, including block modification, block insertion and block deletion. It also as critical importance for auditing mechanisms under the cloud data storage paradigm. Using homomorphism authenticators helps achieve a constant communication overhead for public audit ability. However, the direct extension of the approach to support data dynamics may have security and efficiency problems. Take block insertion, for example. In the original homomorphism authentication schemes, to prevent a cloud server using the same authenticator to obtain the correctness proof for a different block, the block index information has to be embedded in the authentication calculation (usually in the form of H(i), where H(·) is a collision resistant hash function).As a result, any insertion operation (e.g., inserting block m* after mi) will inevitably change the indices of all the following blocks after 'I', causing significantly expensive re computation of all the corresponding authentication. "In order to avoid the above dilemma for data dynamics, we have to find a way to eliminate the index information in the homomorphism authenticator calculation while not affecting the security."To satisfy this special requirement, the first intuition would be using authentication data structures, such as the well-studied "Markel hash tree" (MHT), which is intended to efficiently and securely prove that a set of elements is unaltered and undamaged. By treating the leaf nodes of the MHT as the blocks of file mi, we immediately achieve easy verification of mi with respect to a publicly known root value R and the auxiliary authentication information (AAI) of the very leaf, which includes the siblings of the nodes on the path connecting the leaf to the root. The directly using these structures shares the same disadvantages of the straightforward scheme. It requires a linear amount of communication cost with respect to the number of sample data size, which can be arbitrarily large. It introduces vulnerabilities of owner data privacy when applied to decryption data directly. The hybrid approach is achieved by removing the index information in the authenticator treating and construction the MHT leave nodes with the newly computed authenticator instead of mi. In doing so, the integrity of the authentication themselves is protected by the MHT, while the authenticators further protect the integrity of the blocks. This gives two immediate advantages: The individual data operation on any file block, especially block insertion and deletion, will no longer affect other unchanged blocks. Block less auditing is still preserved: for each auditing process, the cloud server can still send back a small-sized linear combination of blocks. μ = Σ anima and an aggregated authentication 'σ', imposing much smaller communication overhead than sending individual blocks. Also, we should notice that this integrated approach can be further combined with the random masking technique, realizing data privacy protection.

4.3 HANDLING MULTIPLE CONCURRENT TASKS

The establishment of public auditing in cloud computing, a TPA may concurrently handle auditing delegations on different data owner's requests. The individual auditing of these tasks in a sequential way can be very tough and very

inefficient for a TPA. Given K auditing delegations on K distinct data files from K different owners, it is more advantageous for a TPA to batch these multiple tasks together and perform the auditing one time, saving computation hanging as well as auditing time cost. Keeping this natural demand in mind, we note that two previous works can be directly extended to provide batch auditing functionality by exploring the technique of bilinear aggregate signature. Such a technique supports the composite of multiple signatures by distinct signers on distinct messages into a single signature and thus allows efficient verification for the authenticity of all messages. Basically, with batch auditing the K verification equations (for K auditing tasks) corresponding to K responses {μ, σ} from a cloud server can now be composite into a single one such that a considerable amount of auditing time is saved. A very freshly work gives the first study of batch auditing and presents mathematical details as well as security reasoning's. Note that the composite verification equation in batch auditing only holds when all the responses are true or false with high probability when there is even one single null response in the batch auditing. To further sort out these null responses, a recursive divide and conquer approach (binary search) can be utilized. Specifically, if the batch auditing fails, we can divide the collection of responses into two halves, and recurs the batch auditing in halves. Preparatory results show that compared to individual auditing, batch auditing indeed helps reduce the TPA's computation cost, as more than 11 and 14 percent of per-task auditing time is saved when the similar block of set is to be 460 and 300, respectively. Moreover, even if up to 18 percent of 256 different responses are null, batch auditing still performs faster than individual verification.

5. USER MODULE

The user will be a third party person either it be customer or organization user. They send a request to the data owner. If the data owner accepts the user then send the mac address to is user with help of those address user logon to the cloud server else they can be blocked from the third party auditor

6. CONCLUSION

Cloud computing has been envisioned as the future generation architecture of enterprise IT. In contrast to traditional enterprise IT solutions, where the IT services are under useful physical, logical, and personnel controls, cloud computing moves the databases and application software to servers in large data centers on the Internet, where the management of the data and services are not fully trusty. This unique attribute raises many new security challenges in areas such as software and recovery, data security and privacy, as well as legal issues in areas such as regulatory compliance and auditing, all of which have not been well understood. In this work we focus on cloud data storage security. We first present network architecture for effectively describing, developing, and evaluating secure data storage problems. We then suggest a set of cryptographically and systematically desirable properties for public auditing services of dependable cloud data storage security to become a reality. Through in-depth analysis, some existing data storage security building blocks are examined. Thus finally, we proved our proposed algorithm overcomes the limitation of existing.

REFERENCES

[1] M. A. Vasarhelyi and F. B. Halper, "The continuous audit of online systems," Auditing, vol. 10, no. 1, pp. 110–125, 1991.

[2] S. Schneider and A. Sunyaev, "Determinant factors of cloudsourcing decisions," J. Inform, Techn., 2014.

[3] S. M. Groomer and U. S. Murthy, "Continuous auditing of database applications," Inf. Syst. J., vol. 3, no. 2, 1989

[4] K. M. Khan and Q. Malluhi, "Trust in Cloud Services: Providing More Controls to Clients," Computer, vol. 46, no. 7, pp. 94–96, 2013.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput.Appl., vol. 34, no. 1, pp. 1–11, 2011.

[6] F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke, "An agent based business aware incident detection system for cloud environments," J. Cloud Comput., vol. 1, no. 1, p. 9, 2012.

[7] P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, and M. Villari, "A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures," in Proc. IEEE Int. Symp. Parallel Distrib. Process. Workshops Phd Forum, Shanghai, China, 2011, pp. 1510–1517.

[8] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services," in Proc. 8th Int. Conf. Availability, Reliability Security, Regensburg, Germany, 2013, pp. 412–417.