Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 10, October 2015, pg.303 – 310

SURVEY ARTICLE

A SURVEY ON A SECURE AUDITING AGAINST ADVERSARY UPDATE ATTACK USING ELGAMAL

[1]S.LOVELY JACINTH KIRTHANA, [2]P.DURGA DEVI
PG STUDENT, ASSISTANT PROFESSOR
NPR COLLEGE OF ENGINEERING AND TECHNOLOGY, TAMILNADU, INDIA
[1] sljkirthana@gmail.com; [2] jhodevi@gmail.com

Abstract— Cloud computing provides services like infrastructure,software,applications and platform from a distant data centre to the client on a pay-per basis. The clients data in the cloud service provider (CSP) has been secured using homomorphic algorithms, which still didn't prevent certain attacks in cloud. Security is a major concern in cloud, in order to enhance the security on clients data an algorithm with greater key length is used,along with signature generation, the EL-Gamal algorithm. Unlike the previous systems with third-party auditing the data blocks are verified using the Merkle Hash Tree(MHT),along with the variable operations.A query is triggered in the storage server by an adversary and it is prevented in case of variable operation in the storage server using the two techniques EL-Gamal and MHT.EL-Gamal algorithm along with the signature creates a more secure environment of data even in Third-party Auditor(TPA),which prevents an intruder to perform Adversary update attack on the data updation stored on the cloud. The trust on TPA is reduced and has used the Elgamal algorithm with signature which strengthens the clients data in public verifiability, and simultaneously to perform variable operations.

Keywords— Elgamal Algorithm; Third-party Auditor (TPA); Merkle Hash Tree(MHT); Public Verification; Variable Operation.

1. INTRODUCTION

Cloud computing applies a virtual platform with elastic resources putting together by on-demand provisioning of hardware, software, and datasets, dynamically. The idea is to move desktop computing to a service-oriented platform using server clusters and huge databases at datacenters. Cloud computing leverages its low cost and simplicity to both providers and users. Cloud computing intends to leverage multitasking by serving many

heterogeneous applications simultaneously. The computations are sent to where the data is located, rather than copying the data to millions of desktops. Cloud computing avoids large data movement resulting in better network bandwidth utilization. Furthermore, machine virtualization has enabled the cost-effectiveness in using the cloud platforms.

Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Cloud vendors are experiencing growth rates of 50% per annum.But due to being in a stage of infancy; it still has some pitfalls which need to be given proper attention to make cloud computing services more reliable and user friendly.

[Specific security challenges pertain to each of the three cloud service models Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

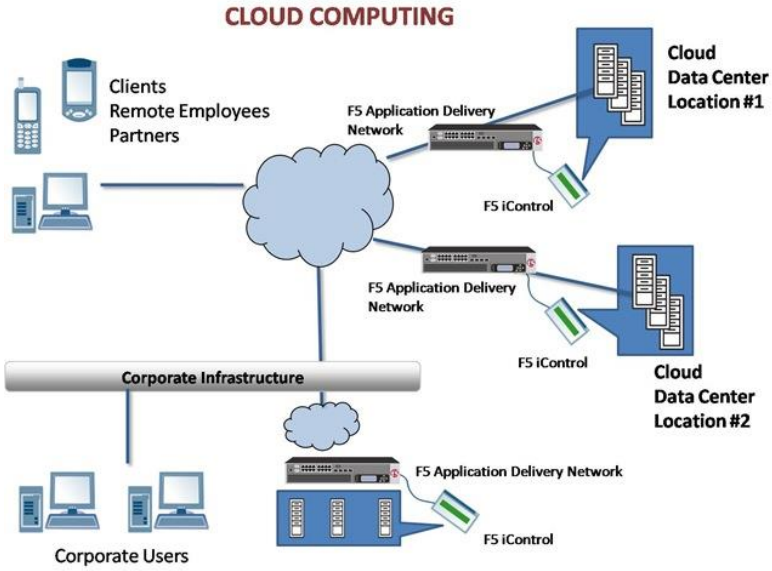
SaaS deploys the provider's applications running on a cloud infrastructure; it offers anywhere access, but also increases security risk. With this service model it's essential to implement policies for identity management and access control to applications. For example, with Salesforce.com, only certain salespeople may be authorized to access and download confidential customer sales information.

PaaS is a shared development environment, such as Microsoft™ Windows Azure, where the consumer controls deployed applications but does not manage the underlying cloud infrastructure. This cloud service model requires strong authentication to identify users, an audit trail, and the ability to support compliance regulations and privacy mandates.

IaaS lets the consumer provision processing, storage, networks, and other fundamental computing resources and controls operating systems, storage, and deployed applications. As with Amazon Elastic Compute Cloud (EC2), the consumer does not manage or control the underlying cloud infrastructure. Data security is typically a shared responsibility between the cloud service provider and the cloud consumer. Data encryption without the need to modify applications is a key requirement in this environment to remove the custodial risk of IaaS infrastructure personnel accessing sensitive data.

Many organizations have implemented encryption for data security, they often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model; thus, if keys are appropriately protected but access is not sufficiently controlled or robust, malicious or

compromised personnel can attempt to access sensitive data by assuming the identity of an authorized user.



2. LITERATURE REVIEW

2.1 COMPACT PROOFS OF RETRIEVABILITY

In proof of retrievability system, the cloud service provider that is the data storage centre must verify the data that has been stored by the client. It is difficult for the prover to pass a verification check. This scheme has used the BLS signatures and the pseudorandom functions (PRFs) which make the clients query and the servers response short and secure. These two schemes use the homomorphic properties which aggregates the proof into a small value. Proof of Retrievability model the prover consists of an arbitrary program as opposed to a simple memory layout and this program may answer these questions in an arbitrary manner. Proof of Retrievability model allows the attacker to execute a polynomial number of proof of attempts before committing to how it will store memory.

The proof of retrievability scheme is secure if no sufficient algorithm wins the game. This gives the security proof against arbitrary adversaries in this model. The clients query and the servers response are short and are up to 20 bytes and 40 bytes in case of public retrieveability,in case of private retirevability the servers response are 20 bytes at the 80 bit security level.

2.2 A DYNAMIC PROOF OF RETRIEVABILITY (POR) SCHEME WITH O (log n) COMPLEXITY

Static PoR scheme is converted to Dynamic scenario. In static operations the client stores files and cannot make any further changes to it. Where as in dynamic scheme the update operations can be performed e.g.,insertion,deletion and modification. Even after the update the client can still detect the data losses even if the server tries to hide it.

The new technique that is used to authenticate the client is done using the merkle has tree(MHT),combined with B+ tree it is called as CMBT i.e.,cloud merkle B+ tree.now with this dynamic version of PoR scheme the worst case communication complexity is O(logn) instead of O(n).Dynamic PoR scheme can be summarized in three stages:

- Preprocess stage: before outsourcing the client will preprocess the file and generate metadata.then the client will outsource the file and save only the metadata.
- Verification stage: The Client will periodically check the integrity of its data. It will query the server randomly and ask the server to provide proof .By verifying the proof with the metadata,the client can detect the file corruption and high probability.
- Update stage:The client will send the server request to update the file. After each update, the server will prove to the client that the update is correctly.

Due to the Byzantine failures and external intrusions, the CSP may lose or corrupt the hosted data inadvertently. When these errors happen, the CSP may try to save its reputation by hiding the truth of data loss. In this dynamic version of PoR detect file corruptions with high probability, but it treat CSS as one entity and is called the server and the other entity has the client, still security is a concern in case of reset attack at upload phase.

2.3 DYNAMIC AUDIT SERVICES FOR OUTSOURCED STORAGES IN CLOUDS

Cloud computing provides a scalable environment for growing amounts of data and processes that work on various applications and services by means of on-demand self-services. Especially, the outsourced storage in clouds has become a new profit growth point by providing a comparably low-cost, scalable, location-independent platform for managing clients data. The cloud storage service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients since their data or archives are stored in an uncertain storage pool outside the enterprises.

These security risks come from the following reasons: first, the cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still

susceptible to internal threats (e.g., via virtual machine) and external threats (e.g., via system holes) that can damage data integrity; second, for the benefits of possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully towards the cloud users; furthermore, disputes occasionally suffer from the lack of trust on CSP since the data changes may not be timely known by the cloud users, even if these disputes may result from the users' own improper operations .

The construction of dynamic audit services for untrusted and outsourced storages has been presented. An efficient method for periodic sampling audit to enhance the performance of third party auditors and storage service providers in used. This experiment has showed that our solution has a small, constant amount of overhead, which minimizes computation and communication costs.

2.4 ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

Cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information identity privacy to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud.

In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity**.**

Oruta, a novel privacy-preserving public auditing mechanism. More specifically, we utilize ring signatures to construct homomorphic authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier.

Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected, the current design of ours does not support traceability.

2.5 COOPERATIVE PROVABLE DATA POSSESSION FOR INTEGRITY VERIFICATION IN MULTICLOUD STORAGE

Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients data. We present a cooperative PDP (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy. This scheme is based on multiprover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties.

In addition, we articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Our experiments show that our solution introduces lower computation and communication overheads in comparison with no cooperative approaches. Provable data possession in distributed cloud environments from the following aspects: high security, transparent verification, and high performance. To achieve these goals, we first propose a verification framework for multicloud storage along with two fundamental techniques: hash index hierarchy (HIH) and homomorphic verifiable response (HVR).

In this paper, we presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero-knowledge interactive proof system, so that it can resist various attacks even if it is deployed

as a public audit service in clouds. Furthermore, we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems.

2.6 OUTSOURCING LARGE MATRIX INVERSION COMPUTATION TO A PUBLIC CLOUD

Cloud computing enables resource-constrained clients to economically outsource their huge computation workloads to a cloud server with massive computational power. This promising computing paradigm inevitably brings in new security concerns and challenges, such as input/output privacy and result verifiability. Since matrix inversion computation (MIC) is a quite common scientific and engineering computational task, we are motivated to design a protocol to enable secure, robust cheating resistant, and efficient outsourcing of MIC to a malicious cloud in this paper. The main idea to protect the privacy is employing some transformations on the original matrix to get an encrypted matrix which is sent to the cloud, and then transforming the result returned from the cloud to get the correct inversion of the original matrix. Next, a randomized Monte Carlo verification algorithm with one-sided error is employed to successfully handle result verification. In this paper, the superiority of this novel technique in designing inexpensive result verification algorithm for secure outsourcing is well demonstrated. We analytically show that the proposed protocol simultaneously fulfills the goals of correctness, security, robust cheating resistance, and high efficiency. Extensive theoretical analysis and experimental evaluation also show its high efficiency and immediate practicability.

In this paper, we have designed a protocol for outsourcing of MIC to a malicious cloud. We have shown that the proposed protocol simultaneously fulfills the goals of correctness, security (input/output privacy), robust cheating resistance, and high efficiency. With MIC already well rooted in scientific and engineering fields, the proposed protocol can be deployed individually or serve as a primitive building block, based on which some higher level secure outsourcing protocols are constructed. Monte Carlo verification algorithm to handle result verification. Its superiority in designing inexpensive Directions to launch further research include:1) establishing formal security framework for MIC outsourcing problem; 2) adding result verification for some early protocols, which do not handle result verification, as

a counter offensive to malicious cloud; and 3) identifying new meaningful scientific and engineering computational tasks and then designing protocols to solve them.

3. CONCLUSIONS

The trust on Audit server is reduced and an efficient algorithm can be used in order to secure the clients data from adversary update attack. Now the trustworthy audit server preprocess and upload the data on behalf of the clients. Computation overhead for label generation on the client side is reduced significantly. The cloud audit server also performs the data integrity verification on updating the outsourced data upon the client's request. The new PoR model can enhance security against adversary update attack .It may also support public verifiability and dynamic data operation. The asymmetric cryptography algorithm with large key length along with the signature can strengthen the clients data on the audit server.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM,vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] D. Cash, A. Kupcu, and D. Wichs, "Dynamic Proofs of Retrievability via Oblivious RAM," Proc. 32nd Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 279-295, 2013.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS '13), pp. 90-99, 2013.

