Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Secured data Storage by Privacy Algorithms and third Party Auditing in Cloud System

Ms Shweta khidrapure , Prof.Archana C.Lomte

Department of Computer Science and Engineering

Bhivarabai Sawant Institute of Technology & Research (BSIOTR), India

Abstract:- Cloud data security is a major concern for the client while using the cloud services provided by the service provider. There can be some security issues and conflicts between the client and the service provider. To resolve those issues, a third party can be used as an auditor. In this paper, we have analyzed various mechanisms to ensure reliable data storage using cloud services. It mainly focuses on the way of providing computing resources in form of service rather than a product and utilities are provided to users over internet. The cloud is a platform where data owner remotely store their data in cloud. The main goal of cloud computing concept is to secure and protect the data which come under the property of users. The security of cloud computing environment is exclusive research area which requires further development from both academic and research communities. In the corporate world there are a huge number of clients which is accessing the data and modifying the data. In the cloud, application and services move to centralized huge data center and services and management of this data may not be trustworthy, into cloud environment the computing resources are under control of service provider and the third-party-auditor ensures the data integrity over out sourced data. Third-party auditor not only read but also may be change the data. Therefore a mechanism should be provided to solve the problem. We examine the problem contradiction between client and CSP, new potential security scheme used to solve problem

Keywords :- —Cloud Service Provider, Data Integrity, Encryption, Third Party Audit

I. Introduction:-

Cloud computing is the term used to share the resources globally with less cost .we can also called as „IT ON DEMAND". It provides three types of services i.e., Infrastructure as a service (IAAS) , Platform as a service(PAAS) and Software as a service(SAAS). The ever cheaper and more powerful processors, together with the software as a service (SAAS) computing architecture, are transforming data centers into pools of computing service on a huge scale. End users access the cloud based applications through the web browsers with internet connection. Moving data to clouds makes more convenient and reduce to manage hardware complexities. Data stored at clouds are maintained by Cloud service providers (CSP) with various incentives for different levels of services.

The cloud computing model represents a new paradigm shift in internet-based services that delivers highly scalable distributed computing platforms in which computational resources are offered 'as a service'. Security is considered one of the top ranked open issues in adopting the cloud computing model includes data Integrity confidentiality. This Paper proposed a enabling public audit ability and data dynamics for storage security in cloud computing. They achieved the integrity guarantee of data storage with support of public audit ability and dynamic data operations. However their protocol lacks in providing privacy of data which is one of the issue for the cloud data storage. In this we proposed a privacy preserving public verifiability for integrity of data storage in cloud computing. We are using RSA public cryptography to provide confidentiality of data. Our scheme is more secure than existing system.

Outsourcing storage into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage. At the same time, though, such a service is also eliminating data owners' ultimate control over the fate of their data, which data owners with high service-level requirements have traditionally anticipated. As owners no longer physically possess their cloud data, previous cryptographic primitives for the purpose of storage correctness protection cannot be adopted, due to their requirement of local data copy for the integrity verification. Besides, the large amount of cloud data and owner's constrained computing capabilities further makes the task of data correctness auditing in a cloud environment expensive and even formidable for individual cloud customers. Therefore, enabling public auditability for cloud storage is of critical importance so that owners can resort to a specialized third party auditor (TPA) to audit cloud storage services and maintain strong storage correctness guarantee, while saving their own precious computing resources.

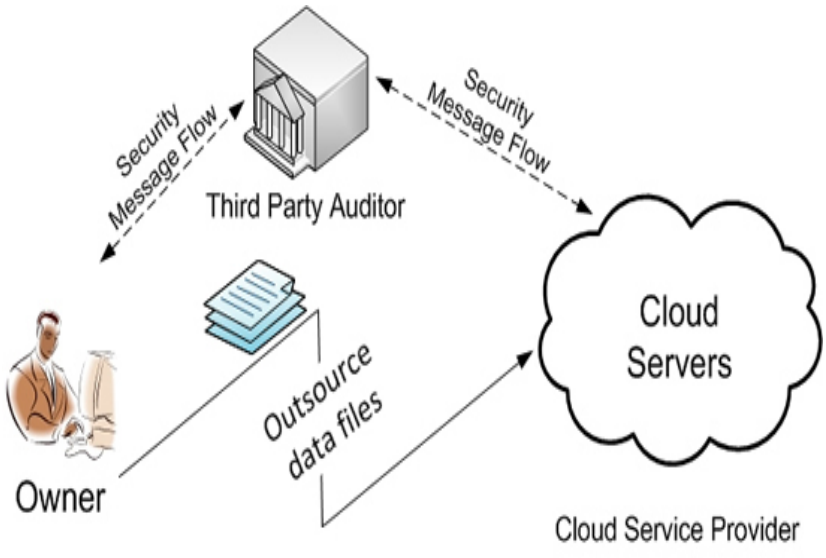
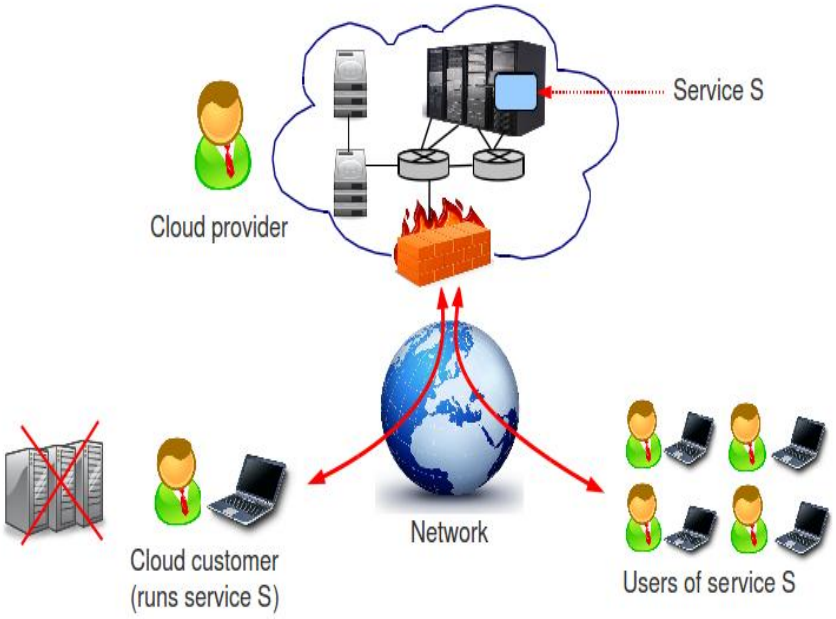


Fig 1 Architecture of Cloud Data Storage System

Considering TPA might learn unauthorized information through the auditing process, especially from owners' unencrypted cloud data, new privacy-preserving storage auditing solutions are further entailed in the cloud to eliminate such new data privacy vulnerabilities. Moreover, for practical service deployment, secure cloud storage auditing should maintain the same level of data correctness assurance even under the condition that data is dynamically changing , and/or multiple auditing request are performed simultaneously for improved efficiency . Techniques we are investigating/developing for these research tasks include proof of storage, random-masking sampling, sequence-enforced Merkle Hash Tree, and their various extensions/novel combinations.

II. Existing System:

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.



Proposed System:

In this paper, we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

Algorithm:

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).

- KeyGen: key generation algorithm that is run by the user to setup the scheme
- SigGen: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing
- GenProof: run by the cloud server to generate a proof of data storage correctness
- VerifyProof: run by the TPA to audit the proof from the cloud server

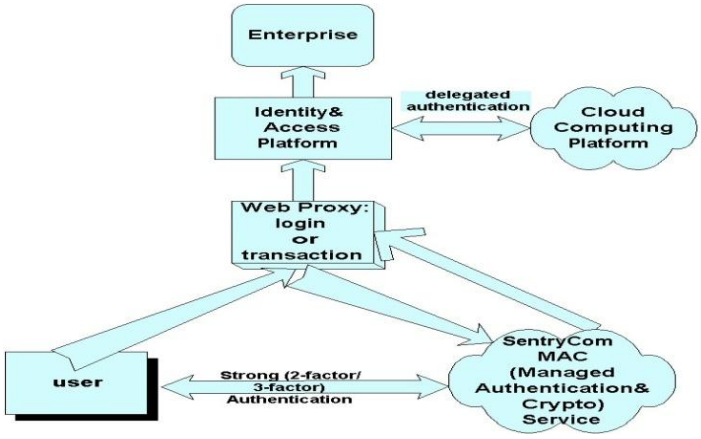


Fig 2 Public Auditing system

III. Privacy-Preserving Public Auditing Module:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

The proposed scheme is as follows:

- Setup Phase
- Audit Phase

1 **Batch Auditing Module**:

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

2 Data dynamics Module:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

Adversary Model

Adversary model was introduced to explore some of threats associated in this model. As we know that the data is not present at users place because data is stored at cloud servers. It may lead to some security threats mainly two, internal attacks and external attacks. Internal attacks comes from the cloud servers itself, these servers may be malicious and lead to byzantine failures and hide some data loss issues. Secondly external attacks are from outsiders who are compromised the data from cloud service providers without its permission. Outsider attacks may lead to modification of data or deleting the users and so on which are completely masked from cloud service providers. All though TPA can also possibly hack the data for itself interested and it is also a case for inside attacks, but we ensure that TPA"s are trusted party servers. Therefore, we consider the adversary in our model to capture all types of attacks both internal and external threats. Once the server is compromised, the data is polluted with fraudulent data and users cannot get the original data from the clouds.

Design Goals

To enable privacy-preserving public auditing for cloud data storage under the model, our protocol design should achieve the following security and performance guarantee:

(1) **Storage correctness**: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

(2) **Fast localization of data error**: to effectively locate the malfunctioning server when data corruption has been detected

(3) **Dynamic data support**: to maintain the same level of storage correctness assurance even if users modify, delete or append their data files in the cloud.
(4) **Dependability**: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e. minimizing the effect brought by data errors or server failures.
(5) **Lightweight**: to enable users to perform storage correctness checks with minimum overhead.

1. ENSURING DATA STORAGE OVER CLOUD

In cloud data storage system, users store their data remotely i.e. on clouds, so that the correctness and availability of data files must be guaranteed to be identical. Our aim is to detect the servers which behaves differently and may leads to internal and external threats. In this paper, we explore the technique used to detect the modified blocks easily with very less overhead using homomorphic token pre computation technique ,later we can use erasure coded technique to acquire the desired blocks from different servers.

1.1. Challenge Token Pre-Computation

To achieve data storage correctness and data integrity, we use an algorithm which takes a few parameters and compute the token

```
procedure
    Choose parameters l, n and function f, φ;
    Choose the number t of tokens;
    Choose the number r of indices per verification;
    Generate master key K_PRP and challenge key k_chal;
    for vector G^(j), j ← 1, n do
        for round i ← 1, t do
            Derive α_i = f_kchal(i) and k_prp^(i) from K_PRP.
            Compute v_i^(j) = Σ_{q=1}^{r} α_i^q * G^(j)[φ_{k_prp^(i)}(q)]
        end for
    end for
    Store all the v_i's locally.
end procedure
```

1.2 Correctness Verification and Error Localization

Error localization is a key prerequisite for eliminating errors in storage systems. It is also of critical importance to identify potential threats from external attacks. However, many previous schemes do not explicitly consider the problem of data error localization, thus only providing binary results for the storage verification

```
procedure CHALLENGE(i)
    Recompute α_i = f_kchal(i) and k_prp^(i) from K_PRP;
    Send {α_i, k_prp^(i)} to all the cloud servers;
    Receive from servers:
    {R_i^(j) = Σ_{q=1}^{r} α_i^q * G^(j)[φ_{k_prp^(i)}(q)] | 1 ≤ j ≤ n}
    for (j ← m + 1, n) do
        R^(j) ← R^(j) − Σ_{q=1}^{r} f_{k_j}(s_{I_q,j}) · α_i^q, I_q = φ_{k_prp^(i)}(q)
    end for
    if ({R_i^(1), ..., R_i^(m)} · P == {R_i^(m+1), ..., R_i^(n)}) then
        Accept and ready for the next challenge.
    else
        for (j ← 1, n) do
            if (R_i^(j) != v_i^(j)) then
                return server j is misbehaving.
            end if
        end for
    end if
end procedure
```

2 File Retrieval and Error Recovery

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one.

3 Towards Third Party Auditing

The user does not have the time, feasibility or resources to perform the storage correctness verification he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable and securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing. We show that with only slight modification, our protocol can support privacy-preserving third party auditing. The new design is based on the observation of linear property of the parity vector blinding process.

IV. Conclusion:-

Cloud data security is an important aspect for the client while using cloud services. Third Party Auditor can be used to ensure the security and integrity of data. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various schemes are proposed by authors over the years to provide a trusted

environment for cloud services. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. This paper provides an abstract view of different schemes proposed in recent past for cloud data security using third party auditor. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make third party auditor store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider and client.

References

[1] Cong Wang, Sherman S.M. Chow "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers (TC), 2011.

[2] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing", To appear, IEEE Transactions on Parallel and Distributed Systems (TPDS), Vol. 22, No. 5, pp. 847-859, May, 2011.

[3] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, Towards Publicly Auditable Secure Cloud Data Storage Services," To appear, IEEE Transactions on Service Computing (TSC).

[4] Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Towards Publicly Auditable Secure Cloud Data Storage Services", IEEE Network Magazine, Vol. 24, No. 4, pp. 19-24, July/August 2010.

