Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Research on Cloud Server Storage Security Using TPA

Surendra Singh Rathod
SVITS,
Indore, M.P., India

Anand Rajawat
Asso. Professor, SVITS,
Indore, M.P., India

Abstract: Cloud computing offers an new method of delivering computing resources where by clients are capable to implement their applications at remote servers with infinite storage capability while enjoying efficient features such as scalability, availability, on-demand self service and elasticity on pay-per-use billing pattern. Many users situate their data in the cloud and so data integrity is very important concern in cloud storage. After moving the data to the cloud, owner hopes that their data and applications are in protected manner. But that optimism may fail occasionally that is the owner's data may be altered or deleted. In this situation the user must download the data in order to authorize it. If the outsourced data is very huge files, such downloading to determine data integrity may become prohibitive in terms of improved cost of bandwidth and time, especially if frequent data checks are necessary. In this research paper, we propose an enhanced technique that consists of five donations such as resilient role-based access control mechanism, Partial homomorphic cryptography, metadata generation and image steganography, Efficient third-party auditing service. The main advantage in this research reducing time consumption on checking files using trusted TPA(Third Party Auditor).

Keywords– RSA, MD5, Homomorphism, Privacy Preserved Data Storage.

I. INTRODUCTION

CLOUD Computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of extraordinary advantages in the IT history: on-demand self-service, location independent resource pooling, rapid resource elasticity, ubiquitous network access, usage-based pricing and transference of risk[1,2].

Cloud computing is widely used in the commercial field, such as Data Store, and cloud application has achieved good effect. In cloud computing, data is moved to a remotely located cloud server. The cloud computing refers to the services and application delivered through internet. The software and hardware are embedded in the data centers providing those services. The data centers are also called cloud (comprise of hardware and software). The National Institute of Standard and Research has given the standard definition of Cloud Computing which is being Accepted Worldwide:-

Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or services provider interactions. Cloud computing is a computing paradigm, where a huge pool of systems are connected in public or private networks, to provide energetically scalable infrastructure for application, data and file storage. With the beginning of this technology, the cost of computation, content storage, application hosting and delivery is reduced significantly.

Cloud computing is a realistic approach to experience direct cost benefits and it has the prospective to transform a data center from a capital-intensive set up to a variable priced environment.

Provides PAAS (platform as a service) and IAAS (Infrastructure as a service). Cloud can be deployed in various forms like:

Private cloud: In this cloud owned by an organization and data centers are not available to general public.

Public cloud : In public cloud data centers are available to general public and the organization sell the services in pay-as-you-go manner.

Community cloud: In community cloud shared by a number of organizations and provide services to a specific community),

Hybrid cloud: In hybrid cloud composition of one or more cloud.

II. CLOUD SYSTEM MODEL

Whole system of cloud architecture can be partition into three significant components:

1) Client: An entity, which contains huge data and data files that are to be stored in the cloud for the monitoring and computation purpose. Client totally relies on the cloud provider for security of their data and they can be either individual consumers or organization.

2) Cloud Services Provider (CSP): It is an entity, which manages and stored all the data stored by the client. The Cloud storage service provider makes all the computation resources available to manage the data files.

3) Third party auditor (TPA): TPA is the third party auditor who will audit the data of data owner or client so that it will let off the load of management of data of data owner [3]. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to estimate the risk of their subscribed cloud data services, but also be advantageous for the cloud service provider to improve their cloud based service platform [4,5].This public auditor will help the data owner that his data are secure in cloud. With the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand.

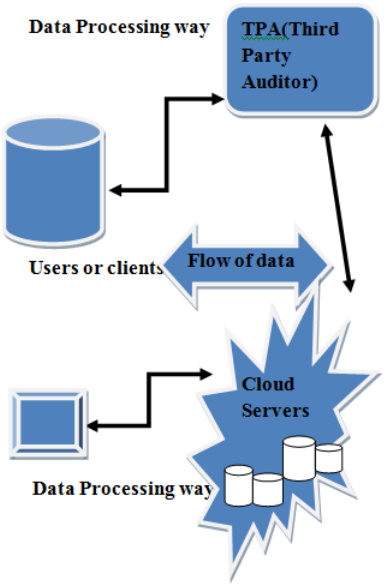


Fig 1: Cloud Data Storage Service Architecture

III. LITERATURE REVIEW

Cloud computing is an rising trend in the field of technology. There are different issues related to cloud computing, major ones being the security and integrity of data.

Many algorithms have been proposed and many frameworks have been designed to resolve such issues.

Nirmala et al. [6] proposed a new proposal to resolve integrity problem by introducing user authenticator to audit and check the integrity of data. Their research focused on providing solutions to all issues of cloud computing and to develop a mold that would provide secure cloud infrastructure which would facilitate to adopt the cloud as and when required.

Raju et al. [7] introduced a protocol for integrity checking of cloud storage that would provide integrity protection of user information. This protocol supports public verifiability and is evidenced to be secure against relate un-trusted server. It's additionally non-public against third-party verifiers.

Attas and Batrafi [8] proposed an integrity checking model over cloud with help of TPA using DSA algorithm. With the help of the model, user can examine and verify the data from unauthorized people who manipulate with the cloud or extract data. Evaluation of the model was done using Windows Azure project that involved digital signature coding. The results showed that the proposed model worked according to what was claimed.

Ateniese et al. [9] are the first to consider

public auditability in their defined "provable data possession" (PDP) model for ensuring possession of files on entrusted storages. In their scheme, they utilize RSA based homomorphism tags for auditing outsourced data, thus public audit ability is achieved. However, Attendees et al. do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer security and design problems.

IV. PROBLEM DOMAIN

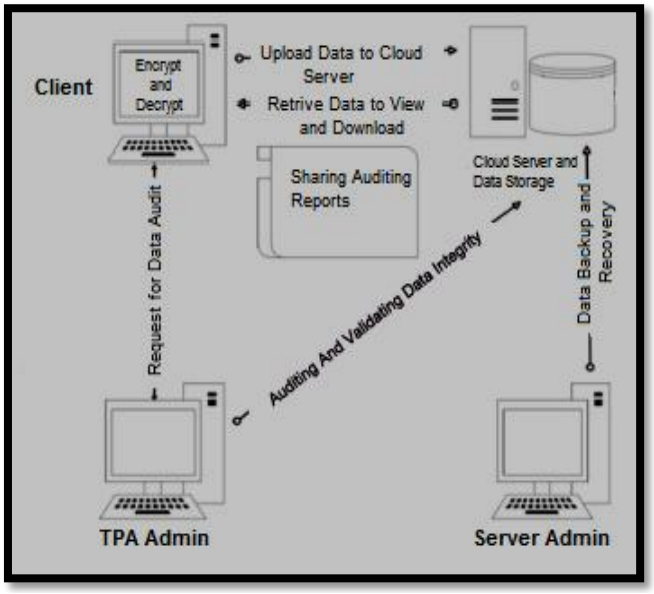
The cloud server storage security problem is foremost and fundamental requirement and it is sensitive area, many of cloud storage are using direct storing techniques to store data on server which is very insecure, some of cloud storage techniques are implemented in manner to resolve this problem but they also using it on server side but still it is very poor and insecure idea, well also the time consumption is fairly high when faced with larger-scale data. So that our main objective of this optimization algorithms based on the objective function, usually by gradient methods to solve the extreme, so the algorithm is easy to converge to the local extreme result and lower time consumption in large data sets by experimental results and analysis.

V. PROPOSED METHOD

In the proposed method, we propose a flexible and effective distributed scheme with explicit dynamic data support to ensure the rightness of users' data in the cloud. In the proposed method, we are implementing the secure system namely Privacy preserving auditing. In this method first the Data Owner will register with the Cloud Service Providers. After the

registration process cloud owner will approve the user to use services. After then getting approved user will be allowed to use the system, user will be allowed to upload their private data on cloud, before uploading the data user have to encrypt their data, the encryption and decryption on client side tool will be available on cloud, which is downloadable. Means user has to download this tool and using this encrypt their data, user has to provide a big integer number as public key, this key will be used to encrypt the user data. After encrypting the data there will be a file created named private key, containing the private key which will be used on file decryption. Now user is safe to upload their data on cloud. Whenever the user starts upload their data on cloud, first of all server will generate HASH CODE for that particular file, using MD5 Algorithm. And a metadata record file will be generated storing HASH CODE of data file.

After this uploading process user may any time request to TPA to audit this data, TPA will check the data auditing requests from different users. Now TPA will request to cloud server to get metadata and file data for a particular file. After getting response from TPA will regenerate the HASH CODE for that particular file, and then compare the current HASH CODE with previous record if it matches then it means file is safe, if it doesn't then file is corrupt or changes have been made. All this record will be updated on metadata record and metadata record will be saved on server side, after this entire process user will be informed that file now corrupt or changed. User will be allowed to download their data any time, at wherever they want. After downloading the data user have to decrypt that data, for decryption the private key file will be required to decrypt data file.



not only eliminates the load of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Widespread analysis shows that the proposed schemes are provably highly efficient and secure.

VI. SYSTEM DOMAIN

Working of cloud server storage security using TPA will be implemented executed on eclipse, jboss application server and MYSQL Server 5.1.

All the experiments and entire process will be performed on a 2.40GHz Intel(R) Core(TM) i5-2430 MB memory, 1GB RAM running on the Windows XP Professional OS. Programs will be coded in J2SE and J2EE on windows platform.

VII. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage and security in Cloud Computing. We utilize the homomorphism authenticator and random masking to assurance that TPA would not learn any information about the data content stored on the cloud server during the efficient auditing process, which

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren et al. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing IEEE INFOCOM 2010.

[2] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, 2009.

[3] Abhishek Mohta and Lalit Kumar Awasthi Cloud Data Security while using Third Party Auditor International Journal of Scientific & Engineering Research,Volume 3, Issue 6, 2012.

[4] Chuang, I-Hsun, "An effective privacy protection scheme for cloud computing." Advanced Communication Technology (ICACT), 2011 13th International Conference on.IEEE, 2011.

[5] Wang, Qian, . "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22.5 2011.

[6] Nirmala V., Sivanandhan R.K., and Lakshmi R.S. "Data confidentiality and Integrity Verification using Authenticator

[7] Dalia Attas and Omar Batrafi, "Efficient Integrity checking technique for or securing client data in Cloud computing," International Journal of Electrical & Computer Sciences, vol. 11, no 5, 2013. Scheme in cloud ," Proc. of 2013 International Conference on Green High Performance Computing, Nagercoil, 2013.

[8] Raju "Data Integrity using Encryption in Cloud Computing," Journal of Global Research in Computer Science, vol. 4, no. 5, 2013.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07. New York, NY, USA: ACM, 2007

