A Survey on: A Secure Cloud Storage System: An Approach

Sangamesh S M
M.Tech(IT),Dept of ISE
SDMCET, Dharwad
Karnataka India

S S Joshi
Dept. of ISE,
SDMCET, Dharwad,
Karnataka India

***Abstract*:- In this paper we purpose a secure cloud storage system to ensure the protection of organizations data from both the cloud provider and the third party auditor and from some users who take advantage of the old accounts to access the data stored on the cloud. The proposed system enhances the authentication level of security by using two authentication techniques; Time-based One Time Password (TOTP) for cloud users verification and Automatic Blocker Protocol (ABP) to fully protect the system from unauthorized third party auditor .Cloud storages in cloud data centers can be useful for enterprises and individuals to store and access their data remotely anywhere anytime without any additional burden. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the major problem of cloud data storage is security. Moreover, cloud users must be able to use the cloud storage just like the local storage, without worrying about the need to verify the data integrity and data consistency. Some researchers have been conducted with the aid of Third Party Auditor (TPA) to verify the data stored in the cloud and be sure that it is not tampered. However, the TPA is leased by the provider and after a time cloud service provider may contract with the TP A to conceal the loss of data from the user to prevent the defamation.**

Keywords:- Keywords are Cloud Computing; Privacy Preserving; public auditability; Third Party Auditor (TPA); One Time Password (OTP); Automatic Blocker Protocol (ABP).

INTRODUCTION

Cloud computing is storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. It is defined as 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 service provider interaction. The National Institute of Standards and Technology (NIST) defames cloud computing by five essential characteristics, three service models and four deployment models. The essential characteristics are on demand self-service, location independent resource pooling, broad network access, rapid resource elasticity, and measured service. The main three service models are software as a service (SAAS), platform as a service (P AAS) and infrastructure as a service (TAAS), while the deployment models include private cloud, public cloud, community cloud and hybrid cloud. . However, the major problem of cloud data storage is security. Therefore, cloud data storage should have some mechanisms able to specify storage correctness and integrity of data stored on a cloud. Cloud storages in cloud data centers can be useful for enterprises and individuals to store and access their data remotely anywhere anytime without any additional burden. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. We are proposing a novel secure cloud storage system to ensure the protection of organizations' data from both the cloud provider and the third party auditor and from some users who take advantage of the old accounts to access the data stored on the cloud.

The proposed system enhances the authentication level of security by using two authentication techniques; Time-based One Time Password (TOTP) for cloud users verification and Automatic Blocker Protocol (ABP) to fully protect the system from unauthorized third party auditor. The experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity. The notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different system and security models. Public auditability model called Provable Data Possession (PDP) is presented for ensuring possession of files on untrusted storages. The PDP model employees the RSA-based homomorphic authenticators for data auditing. By using the PDP model, public auditing is achieved, but that model only supports static data. In subsequent work, the authors in present partially dynamic version of the PDP model. But, the system imposes a priori bound on the number of queries and does not support fully dynamic data operations. That is, it only allows very basic block operations with limited functionality, and block insertions cannot be supported.

The scheme is essentially a fully dynamic version of the PDP solution. To support updates, especially for block insertion, the extended PDP eliminates the index information in the tag computation in the PDP model and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure. The proofs can be aggregated into a small authenticator value, and public irretrievability is achieved. Although the enhancement achieves the purpose, still, the authors only consider static data files. Tn, the authors introduce the concept of Third Party Auditor (TPA) to reduce online burden and keeps data integrity and privacy preserve. An improved technique of verifying data integrity on cloud by utilizing the concept of Third Party Auditor (TPA) is introduced, the authors approved that involving the TP A may associate additional risk to the confidentiality of data.

RELATED WORK

Cloud computing as evolution of distributed computing—a case study for SlapOS distributed cloud computing platform.

The cloud computing paradigm has been defined from several points of view, the main two directions being either as an evolution of the grid and distributed computing paradigm, or, on the contrary, as a disruptive revolution in the classical paradigms of operating systems, network layers and web applications. This paper presents a distributed cloud computing platform called Slap OS, which unifies technologies and communication protocols into a new technology model for offering any application as a service. Both cloud and distributed computing can be efficient methods for optimizing resources that are aggregated from a grid of standard PCs hosted in homes, offices and small data centers. The paper fills a gap in the existing distributed computing literature by providing a distributed cloud computing model which can be applied for deploying various applications.

Resource allocation in a network based cloud computing environment: design challenges.

Cloud computing is a utility computing paradigm that has become a solid base for a wide array of enterprise and end-user applications. Providers offer varying service portfolios that differ in resource configurations and provided services. A comprehensive solution for resource allocation is fundamental to any cloud computing service provider. Any resource allocation model has to consider computational resources as well as network resources to accurately reflect practical demands. Another aspect that should be considered while provisioning resources is energy consumption. This aspect is getting more attention from industrial and government parties. Calls for the support of green clouds are gaining momentum. With that in mind, resource allocation algorithms aim to accomplish the task of scheduling virtual machines on the servers residing in data centers and consequently scheduling network resources while complying with the problem constraints.

A Survey on Privacy Preserving Technique to Secure Cloud

There is a danger factor in storing your personal data on public cloud; data encryption is a great way to discourage people from accessing unauthorized data. If you plan to store your data on the public cloud security key will identify them as your own work and discourage people from copying them or claiming them. As their own and in case of cloud storage it makes it very difficult for maintaining storage space and also security for that matter.

METHEDOLOGY

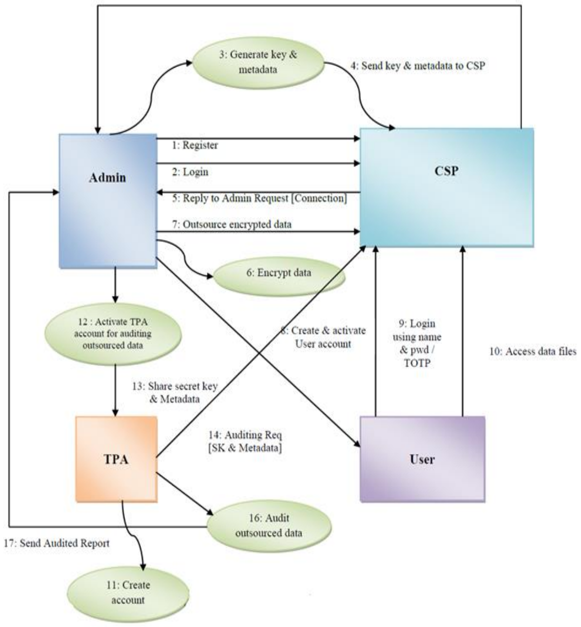
3: Generate key & metadata
4: Send key & metadata to CSP
Admin
CSP
1: Register
2: Login
5: Reply to Admin Request [Connection]
7: Outsource encrypted data
6: Encrypt data
12 : Activate TPA account for auditing outsourced data
8: Create & activate User account
9: Login using name & pwd / TOTP
10: Access data files
13: Share secret key & Metadata
14: Auditing Req [SK & Metadata]
TPA
User
16: Audit outsourced data
17: Send Audited Report
11: Create account

Fig1: Flow of operation for the proposed system

Modules

i. Admin
ii. CSP
iii. TPA
iv. Cloud-User

Admin

In this module, Admin is an entity, who has huge amount of data to be stored in the cloud, can be either enterprise or individual customers. The admin has all the privileges over the users and the third party auditors. Admin will outsource their data to CSP. Before outsourcing data to the CS,
data is encrypted by a powerful encryption technique called Advanced Encryption System (AES).The organization admin generate the keys and metadata and then shares it with the TPA and also sends keys & metadata to the CSP when auditing is required for his outsourced file. Admin is also responsible for creating user account to avoid data access by pre-activated accounts. The admin is the only one that can activate or not the accounts. There by we can achieve the information confidentiality, integrity, and availability

CSP

In this module, CSP is the one who can manage the cloud servers that have a large storage space available for any organization wants to store their data. CSP receives keys and metadata from admin, then replies to the request from the admin and establish a connection with the admin. CSP will stores all the registered admin and user information.

When CSP receives request from TPA to audit the admin file, it will further request Admin to check whether it receives a request from valid TPA or not. Later it will permit TPA for further auditing.

TPA

In this module, TPA is the one who may rent upon request from the admin to audit the data stored on the cloud. If the organization admin wants to audit the outsourced data on the cloud server, he resorts to the TP A who has the expertise to audit the data. However, the TP A must have an account in the system. This account must also activate from the organization admin. If the TPA account is activated from the organization admin, then secret key and metadata would send to the TP A to audit the outsourced data on the CS, otherwise the TPA can't access the system. TP A with the secret key and metadata sends the auditing request to the CSP to initialize the auditing process. After getting permission from CSP, TPA will audit the file, and send the audited report to respective admin.

Cloud-User

In this module, cloud-user is the users that can access (update or retrieve) the data on the cloud and he is under the supervision of the organization admin. To achieve the information confidentiality, integrity, and availability, the user must have an account (Emails and password) to access stored data. In this system, more restrictions upon these accounts are done by the admin to avoid data access by pre-activated accounts. Where, the admin is the only one that can activate or not the accounts. The activated users' accounts can login by using the two stages authentication technique; username with password, and the TOTP that is permitted for one session between the user and the cloud server.

CONCLUSION

In this paper we proposed a novel secure cloud storage system is proposed to ensure the protection of organizations' data from both the cloud provider and the third party auditor and from some users who take advantage of the old accounts to access the data stored on the cloud. The proposed system increases the authentication level of security by using two authentication techniques; Time-based One Time Password (TOTP) and Automatic Blocker Protocol (ABP). In the proposed system, the data owners control all the privileges to be sure that who can access their outsourced data on cloud storage servers. To increase security, user authentication is verified by two-factor authentication: the first is exercised with a username and password while the second is caused by the implementation of TOTP. The experimental results demonstrate the effectiveness and efficiency of the proposed system when auditing shared data integrity.

REFERENCES

1. Sheren A. E!-Booz, Gama! Attiya and Nawa! E!-Fishawy “A Secure Cloud Storage System Combining Time-based One Time Password and Automatic Blocker Protocol” Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt “IEEE TRANSACTIONS 10.1109/ICENCO 2015.
2. George SUCIU, Simona HALUNGA, Anca APOSTU, Alexandru VULPE, Gyorgy TODORAN, "Cloud Computing as Evolution of Distributed Computing - A Case Study for SlapOS Distributed Cloud Computing Platform,"' Informatics Economics, Vol. 17, No. 4, pp. 109-122,2013.
3. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory, October 7 2009. http://www. nist. govlitI/cloud/
4. Mohamed Abu Sharkh. Manar Jammal, Abdallah Shami, and Abdelkader Ouda, "Resource Allocation in a Network Based Cloud Computing Environment: Design Challenges," IEEE Communications Magazine, Vol. 51, Issue l l, pp 46-52, November 2013.
5. c. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage." IEEE Transactions on Computers, Vol. 62, No. 2, pp. 1-12,2013.
6. M. Venkatesh, M. R. Sumalatha and C. SelvaKumar, "Improving public auditability, data possession in data storage security for cloud computing,'· Proc. of the International Conference on Recent Trends in Information Technology (ICRTIT), pp. 463-467, 19-21 April 2012.
7. S. Bhagyashri and Y. B. Gurave, "A Survey on Privacy Preserving Techniques for Secure Cloud Storage·', International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 3, Issue. 2, pp. 675-680, Feb. 2014.