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

A Group Verification Framework for Secure Storage in Cloud

[1]Santosh Kumar Ganta[*], [2]Dr. Penmetsa V Krishna Raja, [3]Ravi Kumar Routhu
[1, 3]M.Tech, CSE & Assistant Professor, Sri Sivani Group of Colleges, Andhra Pradesh, India
[2]M.Tech, Ph.D, Principal, AIMS College of Engineering, Andhra Pradesh, India

Abstract: ***In cloud computing more amount of data store in the cloud such software, hardware etc. The main issue is providing security and frequent verification of files. In this work we proposed batch auditing framework which audit multiple data owner's files simultaneously. We used polyalphabetic ciphers to encrypt files of data owners and for secure message passing to owner we used simple mail transfer protocol.***

Keywords: API, RSA

I. INTRODUCTION

Cloud computing is a model for enabling convenient on request network access to a shared and configurable computing resources such as networks, servers, storage, applications and that can be frequently provisioned and released with minimal management effort or service provider interaction. This cloud model leads to availability and is composed of five essential characteristics and three service models and four deployment models.

Private cloud: The cloud infrastructure is operated solely for an organization. It is managed by the organization or a third party and may exist on premise or off premise.

***Community cloud*:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns for example mission, security requirementsand compliance considerations. It is managed by the organizations or a third party and may exist on premise or off premise.

Public cloud*:* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: It is defined as the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

Cloud Computing is both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been defined to as Software as a Service. The datacenter consists of hardware and software is what we will call a Cloud. The Cloud is made available in a pay as go way to the general public and we call it a Public Cloud. The service is Utility Computing and we use to called as Private Cloud to refer to internal datacenters of a business or other organization and not made available to the general public. The Cloud Computing is the sum of software service and Utility Computing and but doesnot include Private Clouds. People can be users or providers of (SaaS), or users or providers of Utility Computing. Wefocus on Providers (Cloud Users) and Cloud Providers and it is received less attention than SaaS Users

There are many ways to compromise data. Deletion or alteration of records such as update is without a backup of the original content is an obvious example. The record from a larger context may render it unrecoverable and it storage on unreliable media. Loss of an encoding key may result ineffective destruction. The un-authorized parties must be prevented from gaining access. The threat of data compromise increases in the cloud and due to the number of and interactions between risks and challenges which are either unique to cloud or it is more dangerous because of the architectural or operational characteristics of the cloud environment.Account or service hijacking is not new. Attack methods such as phishing as well as fraud and exploitation of software vulnerabilities still achieve results. Credentialsand passwords are often reused and which amplifies the impact of such attacks. There are some Cloud solutions add a new threat to the landscape. There is conditionif an attacker gains access to your credentials and they can eavesdrop on your activities and transactions and alter data and the return falsified information then redirect your clients to illegitimate sites. Your service instances may become and new base for the attacker. From here may leverage the power of your reputation to launch frequent attacks. There are different approaches such as

- On-demand self-service. A consumer can unilaterally provision computing capabilitiessuch as server time and network storage as needed automatically and without requiringhuman interaction with a service provider.
- Broad network access is defined as capabilities are available over the network and accessedthrough standard mechanisms that promote use by heterogeneous thin or thick clientplatforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloudbasedsoftware services.• Resource pooling. The provider's computing resources are pooled to serve multipleconsumers using a multi-tenant mode is with different physical and virtual resourcesdynamically assigned and reassigned according to consumer demand. Thedegree of location and the

customer generally has no control or knowledge overthe exact location of the provided resources and may be able to specify location at ahigher level of abstraction.Evenprivate clouds tend to pool resources between different parts of the same organization.

- Rapid elasticity. Capabilities can be rapidly and elastically provisioned in some casesautomatically to quickly scale out and rapidly released to quickly scale in. The capabilities available for provisioning often appear to be unlimited and canbe purchased in any quantity at any time at any location.
- Measured service. Cloud systems automatically control and optimize resource usage byleveraging a metering capability at some level of abstraction appropriate to the type ofservice. Resource usagecan be monitoredand reported providing transparency for both theprovider and consumer of the service.

II. RELATED WORK

For the third party auditing in cloud storage systems and there are several important requirements which have been proposed in some previous works. The auditing protocol should have the following properties:

1) Confidentiality. It should keep owner's data confidential against the auditor.

2) Dynamic Auditing. It should support the dynamic updates of the data in the cloud.

3) Batch Auditing. It should also be able to support the batch auditing for multiple owners and multiple clouds.

Problem Statement: In the verification process there may be chance to leak the received data. There is a chance to following attacks: Replay attack, Forge attack and Replace attack.

1) Replace Attack. The server may choose another valid and uncorrupted pair of data block and data tag (mk, tk) to replace the challenged pair of data block and data tag (mi, ti), when it already discarded mi or ti.

2) Forge Attack. The server may forge the data tag of data block and deceive the auditor and if the owner's secret tag keys are reused for the different versions of data.

3) Replay Attack. The server may generate the proof from the previous proof and without retrieving the actual owner's data.

In the existing cloud architecture is as shown below. In this for one time auditor verifies the data in the cloud. Due to scalability more number of data owners verification process taking more time. So there are some missing files for verification. And there is no chance to correct the data in cloud such as data correctness.

In "Provable Data Possession" model ensures the possession of data files on untrusted storages. It uses a RSA based homo-morphic linear authenticator for auditing outsourced data and this model leaks the data to external auditors and hence was not provably privacy preserving. "Proof of Retrievability" model where spot checking and the error correcting codes are used in order to ensure the possession and Retrievability. But this method works only with encrypted data. There are some improved versions of protocols had been proposed which guarantees private auditability and one which make use of BLS signatures? But these approaches were not privacy-preserving. Then comes an approach to keep online storage honest. This scheme only works for encrypted files which requires the auditor to keep state, and suffers from bounded usage and which potentially brings in online burden to users when the keyed hashes are used up. Thus to provide secure cloud storage supporting privacy-preserving many methodologies and protocols have been proposed.

Cloud Computing is presently one of the hottest topics in information technology (IT). Since the outsourcing of all the essential data is available with a third party and there is always having a concern of cloud service provider's trust-worthiness. Due to data privacy, it is essential for users to encrypt their sensitive data before storing them into the cloud. Their existence of some shortcomings in the situation of traditional encryption and when a secret key owner wants to look for some data that are stored in the cloud storage and may be needed to download all encrypted data from the cloud serverand then decrypts and searches them. The encrypted data are huge or the client is a mobile user and then it will be very inefficient and is not convenient or otherwise he must send his key to the cloud server which performs the decryption and search procedures. It causes a serious trouble that the cloud server obtains the secret key So many models were existed to ensure the integrity of data file.With 24x7 availability and accessible by almost any device with a browser, cloud computing allows organizations to scale their IT infrastructure and software applications as needed. However like any technology the cloud computing has its risks.

Changes the business model*:* Cloud computing changes the way IT services are delivered. No longer delivered from an on-site location the servers, the storage, and applications are provided by external service providers. Organizations need to evaluate the risks associated with the loss of control of the infrastructure.

Abuse*:* Initial registration with a cloud computing service is a pretty simple process. The service provider even offers a free trial period. Organizations should consider their risks due to anonymous signup the lack of validation service fraud, and ad-hoc services.

Insecure interfaces*:* Application programming's interfaces (API) are used to establish manage and monitor services. These interfaces may be subject to security vulnerabilities that put your users at risk.

Malicious insiders*:* One of the benefits of cloud computing is that your organization doesn't need to know the technical details of how the services are delivered. The provider's procedures the physical accesses to systems monitoring of employees and compliance related issues are transparent to the customer. Without full knowledge and control your organization may be at risk.

Shared technology: Cloud computing allows multiple organizations to share and store data on the servers. The original server hardware and operating systems were most likely designed for use by a single tenant (one organization). Organizations should ensure the appropriate controls are in place to keep your data secure.

Data loss and leakage: With shared infrastructure resources, organizations should be concerned about the service provider's authentication systems that grant access to data. Organizations should also ask about encryption data disposal procedures and business continuity.

Account hijacking: Organizations should be aware that account hijacking can occur. Simple Internet registration systems, phishing and fraud schemes can allow a hacker to take over control of your account.

Risk profile*:* For many service providers, the focus is on functionality and benefits not security. Without appropriate software updates the intrusion prevention and firewalls your organization may be at risk.

Users: When using cloud services, your users' activities such as clicking links in e-mail messages. Instant Messaging and visiting fake web sites etc. can download malware to a local workstation. Once installed the malware can launch attacks against your internal network.

Browsers: Several years ago, hackers used to attack software operating systems. More recently the hackers have shifted their attacks to target user browsers. By exploiting browser vulnerabilities the hackers have access to the same applications and data that your users access.

Internet cloud computing services provide both business and technical benefits. Risk assessments help organizations identify and manage and reduce their cloud computing risks so that they may achieve the greatest benefits at the lowest level of risk.

III. PROPOSED WORK

We propose as framework which contains an ability to audit multiple files in the cloud. We divide the framework into three phases such as initialization, data storage, and auditing.

1) Initialization:

phase all members in system will register. There are three types of users such as data owner, users and auditors.

Data owner is have all access rights to insert, update delete a file from cloud. He allows users to access his file on request.

Users have to register in the system and he/she only have reading rights on file which is stored in the cloud on request to the data owner.

Auditor is a trust member between the cloud and data owner, cloud and user. The work of this member is verifying the stored files in the cloud. He also registers his identity in the system.

2) Data Storage:

In this data owner uploads his file in encrypted format and update to auditor such as meta data contains file Id, filename. Data owner also generates signature for the file. For encrypting the file the data owner uses poly alphabetic ciphers. The algorithm is shown below:

A normal alphabet for the plaintext across the top. The process of encryption is very simple: Given a key letter x and a plaintext letter y, the cipher text letter is at the intersection of the row labeled x and the column labeled y; in this case the cipher text is V.

To encrypt a message, a key is needed that is as long as the message. Generally the key is a repeating keyword. Consider the example if the keyword is deceptive the message "we are discovered save yourself" is encrypted as follows:

key: deceptivedeceptivedeceptive

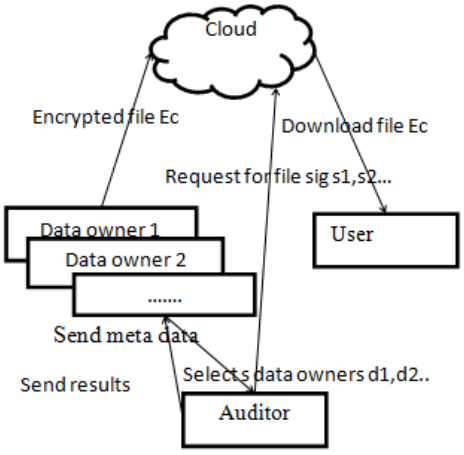
plaintext: wearediscoveredsaveyourself

cipher:-- ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row and the position of the cipher text letter in that row determines the column and the plaintext letter is at the top of that column.

The strength of this cipher is that there are multiple cipher text letters for each plaintext letter and one for each unique letter of the keyword. Therefore the letter frequency information is obscured.For generating the signature it simply uses message digest.

Then on request to the cloud data owner stores the encrypted file in cloud.



3) Auditing/ verification:

In this process, based on the meta data sent by data owner , auditor requests cloud to verify the files in the cloud based in file Id. Then auditor generates signature to file following the initial method followed by the data owner. Then compares the generated signature and the signature sent by the data owner. If these two signatures are equal the file in cloud files are secured. But the problem is batch auditing we give a solution for batch auditing that is as follows. In the registration of the data owner, have to select his auditor to verify his files. Then at the time of verification the auditor checks whether has files to check then he selects group of files to verify then follow the below process.

IV. CONCLUSION

In this work we propose a framework consists of group auditing and secure authentication for users and data owners. It reduce time complexity of auditing files in server. For spontaneous verification of the files in cloud this very helpful. For security purpose and we used polyalphabetic ciphers to secure the content of the files. It reduces processing time.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[2] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.

[3] 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, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[4] Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010.

[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof- mass-email-deletions/, 2006.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http://techcrunch.com/2008/07/10/mediamaxthelinkup-closesits- doors/, July 2008.

[7] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[10] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.

