International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

An Advanced Mechanism for Storing Data in Multi Cloud Environment

Srinivas Potharaju & Swathi Amancha
[1,2]Assitant professor, CSE, St Martin's Engineering College

***Abstract**:*

*In the current scenario usage of cloud has become a part of any organization. The maintenance of cloud storage in distributed cloud storage platform is a bottleneck in the organization. In this paper we proposed an efficient cloud storage scheme using hash function and key encryption scheme. This scheme enables the organizations to maintain distributed cloud storage in an easier manner***.**

Keywords

Cloud Architecture, Data Retrievability,

1. Introduction

H In the past decades cloud storage applicability has become a rapid growth point by providing a comparable low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. Present study calls such a distributed cloud environment as a multi-Cloud (or hybrid cloud). Often, by using virtual infrastructure management (VIM), a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2.

There exist various tools and technologies for multicolor, such as Platform VM Orchestrator, VMware vSphere, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. Such an important platform is unguarded to security attacks; it would bring irretrievable losses to the clients.

For example, the confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or damaged when they are stored into an uncertain storage pool outside the enterprise. Therefore, it is indispensable for cloud service providers (CSPs) to provide security techniques for managing their storage services.

Provable data possession (PDP) (or proofs of retrievability (POR) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The evidence-verification without downloading data frames it especially important for huge-sized files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without downloading the latest version of data. Thus, it is able to replace traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed, such as Scalable PDP and Dynamic PDP. All the existing schemes mainly focuses on PDP issues at suspicious servers in a single cloud storage provider and are not suitable for a multi-cloud environment.

2. LITERATURE SURVEY

Literature survey is important in any software development process. Before developing any tool it is necessary to determine the time factor, economy and company strength. Once these things r satisfied, then next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

We have to analysis Cloud Computing Outline Survey:

Cloud Computing:

Cloud computing provides boundless framework to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use.

- Benefits of Cloud Computing:
- Minimized Capital expenditure
- Location and Device independence
- Utilization and efficiency improvement
- Very high Scalability
- High Computing power

Security a major Concern:

Security concerns arising because both customer data and program are residing in Provider Premises.

Security is always a major concern in Open System Architectures

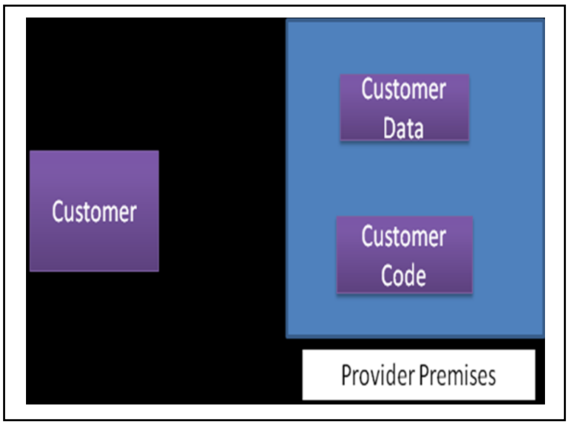


Figure 1:Open System Architecture

Data centre Security?

Professional Security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.

When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked.

All physical and electronic access to data centers by employees should be logged and audited routinely.

Audit tools so that users can easily determine how their data is stored, protected, used, and verify policy enforcement.

Data Location:

When user uses the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in?

Data should be stored and processed only in specific jurisdictions as define by user.

Provider should also make a contractual commitment to obey local privacy requirements on behalf of their customers,

Data-centered policies that are generated when a user provides personal or sensitive information, that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy

Backups of Data:

Data store in database of provider should be redundantly store in multiple physical locations.

Data that is generated during running of program on instances is all customer data and therefore provider should not perform backups.

Control of Administrator on Databases.

Data Sanitization:

Sanitization is the process of removing sensitive information from a storage device.

What happens to data stored in a cloud computing environment once it has passed its user's "use by date".

What data sanitization practices does the cloud computing service provider propose to implement for redundant and retiring data storage devices as and when these devices are retired or taken out of service.

Network Security:

Denial of Service: where servers and networks are brought down by a huge amount of network traffic and users are denied the access to a certain Internet based service.

Like DNS Hacking : Routing Table "Poisoning", XDoS attacks

QoS Violation: through congestion, delaying or dropping packets, or through resource hacking.

Man in the Middle Attack: To overcome it always use SSL

IP Spoofing: Spoofing is the creation of TCP/IP packets using somebody else's IP address.

Solution: Infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

How secure is encryption Scheme:

Is it possible for all of my data to be fully encrypted? What algorithms are used?

Who holds, maintains and issues the keys? Problem:

Encryption accidents can make data totally unusable.

Encryption can complicate availability Solution

The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.

Information Security:

Security related to the information exchanged between different hosts or between hosts and users.

This issues pertaining to secure communication, authentication, and issues concerning single sign on and delegation.

Secure communication issues include those security concerns that arise during the communication between two entities.

These include confidentiality and integrity issues. Confidentiality indicates that all data sent by users should be accessible to only "legitimate" receivers, and integrity indicates that all data received should only be sent/modified by "legitimate" senders.

Solution: public key encryption, X.509 certificates, and the Secure Sockets Layer (SSL) enables secure authentication and communication over computer networks.

3. EXISTING SYSTEM:

There are various existing tools and technologies are available for multi cloud, such as Platform VM Orchestrator, VMwarevSphere, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform for managing clients' data. However, this platform is vulnerable to security attacks; it would bring irretrievable losses to the clients. For example, the confidential data in an enterprise may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or damaged with when they are stored into an uncertain storage pool outside the enterprise. Therefore, it is indispensable for cloud service providers to provide security techniques for managing their storage services.

DISADVANTAGES OF EXISTING SYSTEM:

- Single cloud providers are less popular because of potential problems such as failure of service availability and malicious insiders.
- Cloud providers should address privacy and security issues as a matter of high and urgent priority.

4. PROPOSED SYSTEM :

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. To check the availability and integrity of outsourced data in cloud storages, The existing basic approaches are Provable Data Possession and Proofs of extraction, Based on this we proposed the PDP model for ensuring the control of files on suspicious storages and provided an RSA-based scheme for a static case that achieves the communication cost. This is also a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data possession but also an insubstantial PDP scheme based on secret hash function and symmetric key encryption, but the servers can entrap the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere.

ADVANTAGES OF PROPOSED SYSTEM:

1. Data Integrity.
2. Service Availability.
3. Easy to maintain the data in multi clouds.
4. Cloud service providers should ensure the security of their customer's data and should be responsible if any security risk affects their customer's service infrastructure.

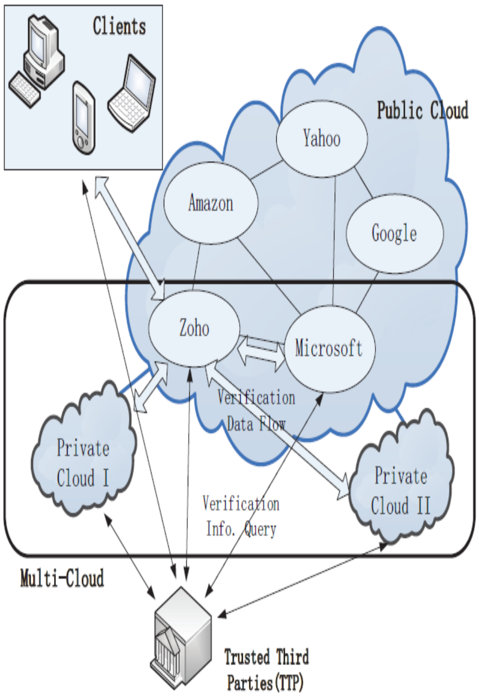
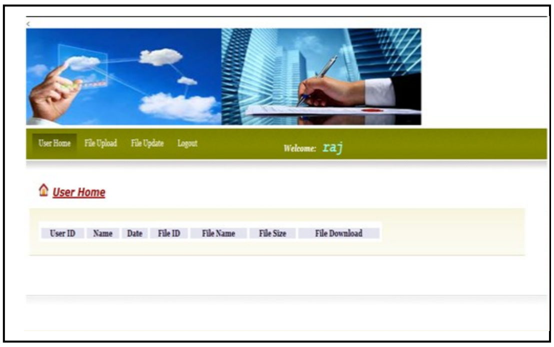


Figure 2: Cloud Architecture

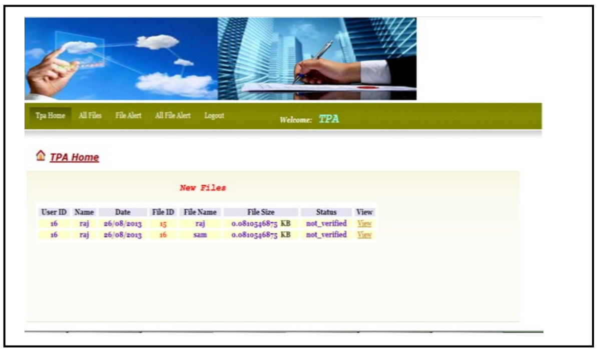
5. Results



User Home

User ID	Name	Date	File ID	File Name	File Size	File Download

Figure 3:User Homepage

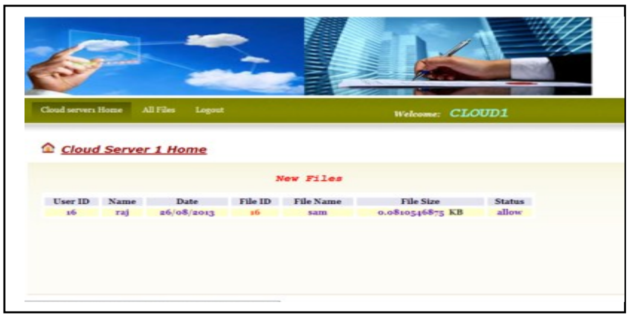


TPA Home

New Files

User ID	Name	Date	File ID	File Name	File Size	Status	View
16	raj	26/08/2013	15	raj	0.081054687 5 KB	not_verified	View
16	raj	26/08/2013	16	sam	0.081054687 5 KB	not_verified	View

Figure 5:TPA Homepage

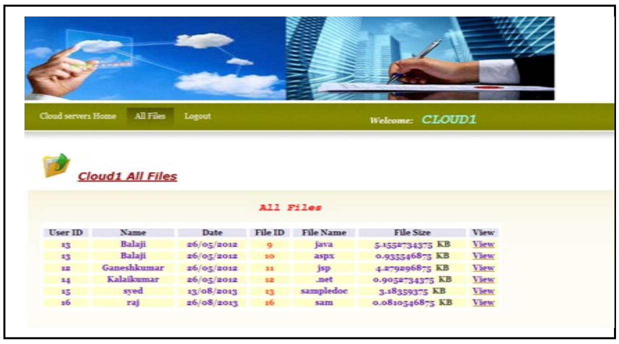


Cloud Server 1 Home

New Files

User ID	Name	Date	File ID	File Name	File Size	Status
16	raj	26/08/2013	16	sam	0.0810546875 KB	allow

Figure 6: Cloud Server Homepage

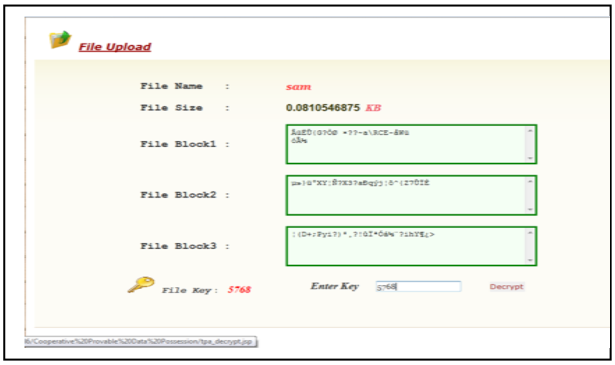


Cloud1 All Files

All Files

User ID	Name	Date	File ID	File Name	File Size	View
13	Balaji	26/05/2012	9	java	5.1552734375 KB	View
13	Balaji	26/05/2012	10	aspx	0.93554687 5 KB	View
12	Ganeshkumar	26/05/2012	11	jsp	4.279296875 KB	View
14	Kalaikumar	26/05/2012	12	.net	0.9052734375 KB	View
15	syed	13/08/2013	13	sampledoc	3.18359375 KB	View
16	raj	26/08/2013	16	sam	0.08105468 75 KB	View

Figure 7: Files in Cloud Server



File Upload

File Name : sam

File Size : 0.0810546875 KB

File Block1 : ÅœËÛ¦G?Öø •??~a\RCE-åW¤ ó¼

File Block2 : µ»}ü"XY¦Š?X3?aÐqÿ¦ð^{Z?ÛÎË

File Block3 : :(D+:Pyi?)".?!GÏ*Óä¾¯?ihY¶¿>

File Key : 5768

Enter Key 5768

6/Cooperative%20Provable%20Data%20Possession/tpa_decrypt.jsp

Figure 8:Decryption of file in Server

6. Conclusion:

In this paper we have proposed a new scheme for cloud storage in distributed cloud environment; it had given good results compared to the existing schemes.

7. References

[1] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. T. Foster, Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14–22, 2009.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner,Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609.

[3] A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson,Eds. ACM, 2007, pp. 584–597.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1–10.

[5] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer,2009, pp. 355–370.

[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[9] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198.

[10] Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

8. Author's Biography

Mr.SrinivasPotharaju,Post Graduated in Computer Science and Engineering (M. Tech)from JNTUH in 2013 and graduated in Computer Science and Engineering (B. Tech) from JNTUH in 2011.Having 3 years of experience as Asst. Professor. He is presently working as Asst. Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. Area of interest in Computer Networks, Network Security, Cloud Computing, Big Data.

. Ms Swathi Amancha, Post Graduated in Computer Science and Engineering (M. Tech) from JNTUH in 2012 and graduated in Computer Science and Engineering (B.Tech) from JNTUH in 2009.Having 8 years of experience as Asst Professor. She is presently working as Asst Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. Area of interest in Computer Networks, Network Security, Big Data, Information Security, Image processing, Cloud Computing,etc.