International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

SECURE REPLICATION IN CLOUD COMPUTING ENVIRONMENT: A SURVEY

Shweta Alguje[1], Harish Patidar[2] , Varsha Mishra[3]
Research Scholar-MTech, CSE-LNCT, Indore
Head,CSE-LNCT, Indore
Asst. Professor, CSE-LNCT, Indore
svs1391@gmail.com
harish.cs@gmail.com
varsha.it @gmail.com

ABSTRACT

Cloud computing technology is viewed as the gathering of web based services for using the resource in more appropriate way. It utilizes distributed system technology to oversee and controlled accumulation of computer terminals that are geologically circulated and associated via a communication link. Replication is the way toward making and overseeing copy versions of a database or document or file to maintain backup or duplicate copy of original one.Security is an imperative and interesting phenomenon gives sheltered and isolated environment. Security model and standards are characterized to execute security features with any applications. For achieving security confidentiality, authentication and integrity are key factors. An investigation of replication issues infers that security is one of the significant worries amid replication. With presence of insecure replication and shaky file management can result in loss of data along with trust of node. This paper investigates the difficulties of replication and observes that security is one of the major significant prerequisites in replication. Here, work proposed security design for secure replication in dispersed frameworks. The entire implementation and evaluation have been utilizing java technology.

Keywords: Replication, RSA, SHA-1

1. INTRODUCTION

Cloud computing technology is viewed as the accumulation of web based services for better utilizing resources. It is the new evolution which uses virtualization, parallel and distributed processing into single unit. It suggests the offering of assets to deal with applications to decreases capital and low support cost. It gives expanded scalability and minimizes complexity with much better access.

Cloud computing can be defined as " A model for enabling ubiquitous, convenient, on –demand network access to a shared pool of resources (e.g., networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Cloud model basically have five basic building blocks along with three service model. It is the blend of computing and services. The key idea is internet will be a single actor which will be capable of providing all kind of services and resources at whatever time required.

Five essential components of cloud environment can be listed as follow:

1. Data: It the collection of unrefined material which might be valuable or not.

2. Storage: This is collection of well refined information for trouble-free access, update, and management purpose. It uses datacenters, disk, taps for storage purpose and database servers for management of data.

3. Client Networks: The major classification is thin, thick and mobile client. All the devices used in day to day life like computers, laptops, smart phones, PDA are part of it.

4. Applications & Computing:

To accomplish a certain specific goal applications are generated which can be human or machine developed. Computing is creation of sequence of algorithms for accomplishment of desired task using computer.

5. Virtualization:

Virtualization is using operating systems, storage devices, and server in virtual form to have two environments simultaneously in accordance of need.

A block representation of component architecture of cloud computing is shown in figure 1.

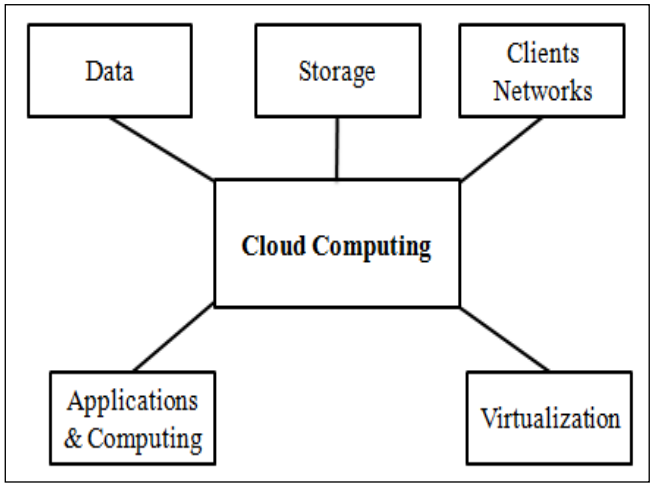


Figure 1: Components of Cloud Computing

Without cloud services cloud computing environment is not possible. It can be explained as:

1. Software as a Service [Saas]:

Using different software and applications on demand by the use of network is facility of this service. Any required software can be accessed through browsers.

2. Platform as a Service [Paas]:

All the runtime environments, development languages system software and collection of libraries comprise to form platform. One can access a required platform using internet.

3. Infrastructure as a Service:

All the software, operating system or any platform or service can be virtually transmit in it. Renting the desired resource is utility of cloud.

Cloud computing deployment models: Cloud services are typically made available to its customer via types of cloud. Types of cloud are shown below.

Private Cloud: When the services are available to limited area network .It can be a single organization, or single home based cloud. Using cloud services within intranet is private cloud.

e-ISSN: 2394-8299
p-ISSN: 2394-8280

Public Cloud:
It is owned by one person. When owner provides all the resources to general public also than such cloud is public cloud. These services can be pay per use or may be free.

Community Cloud: The cloud which is use by collection of organizations and resources are shared among them then such cloud is community cloud. The cost is intermediate between public and private cloud.

Hybrid Cloud – This type of cloud is combination of private and public cloud.

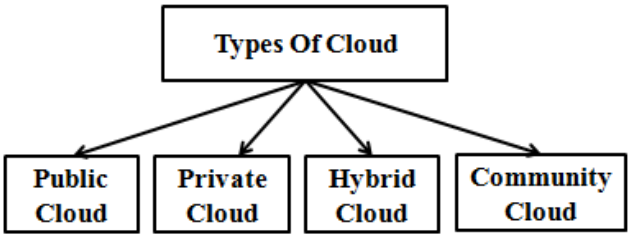


Figure 2: Cloud Computing Service model.

Distributed System & Replication

A distributed system comprises of a accumulation of autonomous computers, associated through a network and distribution middleware, which enables computers to manage their activities and to share the resources of the system, with a goal that users perceive the system as a solitary, integrated computing facility.

In other words, distributed system uses collection of protocols to coordinate the actions of multiple processes on a network, by clubbing entire components for achievement of specific task.
The benefit of this approach is it provides others the capability to connect remotely in scalable manner. Along with this it is also open which conveys interaction of two components is feasible.
Scalability allows us to enhance the number of user whenever needed. All this qualities makes distributed system better than stand alone system. Reliability is one feature which is needed to achieve. Although achieving is not that easy because of the complexities involved all running components.
Replication is method of generation of duplication of a databases or any other content or file. It just not involves only creation but also management and synchronization are need. Synchronization is technique of maintaining the changes in all the databases instead of one used at a time. This in all gives impression to one as if it is working on centralized database. Applications which are developing and maintained at different geographical locations can be very well managed by replication. Thus replication is one the most efficient method for database access.
There are two ways by which replication can be done one is active replication and second is named as passive replication. Active replication can be defined as replication scheme in

which all the servers processed each client request. The major pitfall of this approach is that servers in general give different output for same input i.e. is non-deterministic. Even after presence of this drawback this replication is preferable the reason being quick response is needed in real time system. For all the system with error and faults system like byzantine fault can be handles using this replication. If instead of all servers only one will handle client request then replication is passive replication. The disadvantage of this replication is response is delayed in time of crash.

Figure 2 shows the replication methods of active and passive replication.

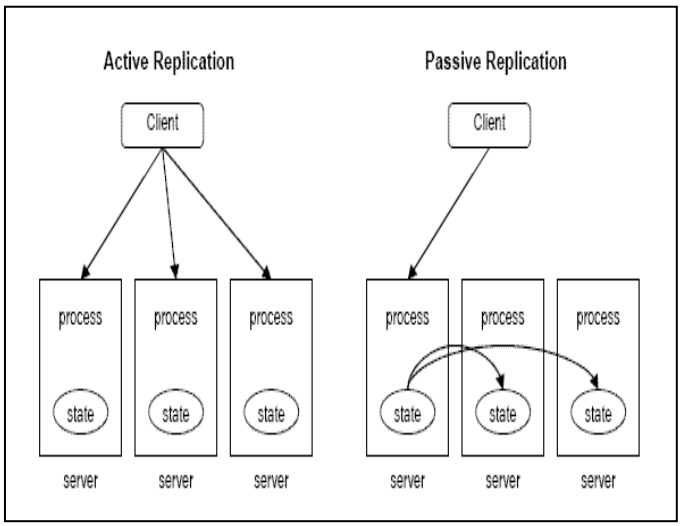


Figure 1.2: Active and Passive Replication

Challenges for Replication

Following challenges are observed in replicated environment which can be listed as:

1. Data Consistency;
2. Downtime during new replica creation:
3. Maintenance overhead:
4. Lower write performance:

3. PROBLEM STATEMENT

In so many areas and wide applications cloud computing environment can be deploy. With invent of computing it was well known that security will be the issue. By combining cloud with it security issues become even more pronounced. Cloud computing uses different computing capabilities like distributed storage and parallel computing. The real need is elaborating its scope from intranet to worldwide level and uses services of cloud in best possible way.

No matter who is accessing whenever the public access scenario comes into frame, the first thought that clashes one mind is security. Security and privacy related issues are always in one mind due to well known attacks. This security need becomes more pronounced in cloud based environment.

The study shows that all the existing solutions can give security at one end but not at all the remaining can be covered. Security at just one or two level can be maintained. No model gives complete level of security. This dictates the need of strong security model which take into consideration security as a prime issue.

Following major problems has been observed during the study of Base Paper [Base Paper Citation].

- Poor Privacy and Confidentiality Approach
- Single Authentication Approach
- No User Role Classification
- Absence of storage level privacy

Furthermore, work also examines the need of privacy maintenance at database level. Previous work does not consider such critical issue and store data into plain format. They only concentrate to maintain privacy at communication level not background level.
In the proposed work, author want to dictate security for public cloud environment .This work doesn't consider that trusted node can't be involved in security issues i.e. cant involves in security breaching. Capability list based access control classifies the user on the basis of user involvement but doesn't consider system while classifying. Scalability of user characteristics can be achieved through Role specification but involvement discovery can't be discovered.
Further analysis gives us a realization of the need of privacy at database level. Previous work doesn't consider work in plain format. Privacy at communication level is considered always not at background level.

5. SOLUTION STATEMENT

A distributed atmosphere raises variety of security problems. First, the published nature of most native space networks makes them notably liable to eavesdropping. Anyone with a private digital computer on associate LAN will simply monitor all network traffic. Secondly, the shortage of management over the code run in a private digital computer makes masquerades, replays, and similar active threats potential. These issues square measure solved in single-machine or centralized environments by physical security: bolted machine rooms and guarded terminal lines. Sadly, the suburbanized nature of distributed systems precludes such measures. Logical instead of physical schemes should be used instead. The only downside to unravel is that of eavesdropping. The answer uses encryption: 2 persons want to speak do so by encrypting all their messages with a secret key illustrious solely to them. This effectively constructs a secure non-public channel on high of the underlying insecure public channel.

Certain steps are involved to draw proposed concept into physical manner. A Java Based application has been developed with replication concept and security principles. A MySql Database has been used to design backend of the project.

The complete scenarios are developed into three Modules which are listed below;

Module 1: Client End

e-ISSN: 2394-8299
p-ISSN: 2394-8280

A java based upload file application has been developed to select and upload text file and forward to Main Server or Master server for secure replication and backup purpose.

Module 2: Master Server / Distributed Server

This module is responsible for receiving the text file from client end and preparation of integrity verification, secure replication and chunk preparation. The complete module performs four major procedures which are listed below;

1. SHA-1 Calculation for Integrity Verification.

2. Chunk Preparation as per given size.

3. Encryption of Chunk for Confidentiality Management.

4. Replication Creation and Distribution.

A detailed description of all the above written process has been explained in the next section of the chapter.

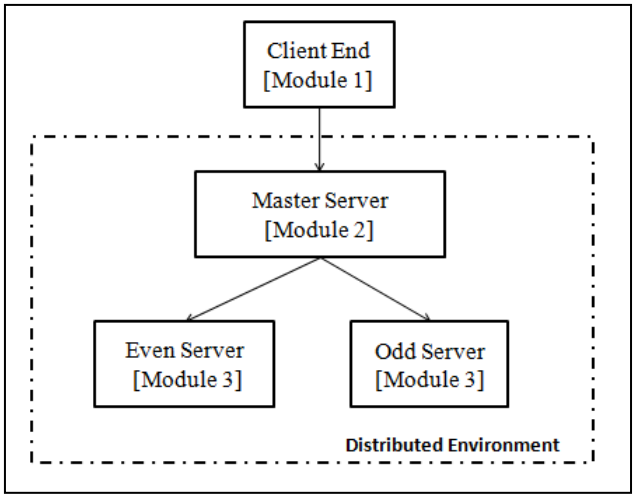
Module 3: Replication

This module executes the replication procedure of the chunk files. It uses Even-Odd Scheme for replication of the chunk file.

1. Even Replica Server consist all even id replica chunk files and maintain backup of the replication.

2. Odd Replica Server consist all odd id replica chunk files and maintain backup of the replication.

A block representation of all above modules is shown in figure 2.



5. CONCLUSION

Despite the continues effort for file replication and consistency management, a secure method is still awaited. Proposed solution not only helps to implement security with data file but also provide secure replication in distributed system.

REFERENCE

1. Atul Kahate "*Cryptography and Network Security*", Second Edition-2003, Tata McGraw Hill New Delhi, 10th reprint-2010.
2. Do Van Thanh, Tore Jenvik, Do Van Thuan & Ivar Jorstad :"*Enhancing Internet service security using GSM SIM authentication"* , Proceedings of the IEEE Globecom 2006 conference - ISBN 1-42440357·X - San Francisco, USA, Nov 27 - Dec 1, 2006.
3. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012
4. Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia
5. Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015
6. P. Triantafillou and C. Neilson "*Achieving Strong Consistency in a Distributed File*" IEEE Transactions on Software Engineering vol 23.No1 January 1997.
7. M. Wiesmann, F. Pedonet, A. Schiper, B. Kemmet, G. Alonso "*Database Replication Techniques: a Three Parameter Classification*" published in Reliable Distributed Systems, 2000. SRDS-2000. Proceedings The 19th IEEE Symposium on at Lausanne PP. 206-215
8. H. Shen,; "*Integrated File Replication and Consistency Maintenance in P2P Systems*" , IEEE Transactions on Parallel Systems,Vol. 21,no 1, January 2010.
9. Y. Huang, J. Cao, B. Jin, X. Tao, J. Lu and Y. Feng "*Flexible Cache Consistency Maintenance over Wireless Ad Hoc Networks*" IEEE Transactions on Parallel Systems,Vol. 21, no 8, August 2010.
10. T. Repantis, A. Iyengar, V. Kalogeraki and I. Rouvellou "*Consistent Replication in Distributed Multi-Tier Architectures*" published in International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, Florida, USA, October 15-18, 201
11. Diana, P. Fatos Xhafa, F. Pop and V. Cristea "*Evaluation of Optimistic Replication Techniques for Dynamic Files in P2P Systems*" published in International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2011.
12. Sulistio, C. Shin Yeo, and R. Buyya "*Simulation of Parallel and Distributed Systems: A Taxonomy and Survey of Tools*".

13. A. Ahmed', A. Abdullah2, and P.D.D.Dominic3; "*A multi-Agent Based Replication Strategy for Improving Availability and Maintaining Consistency of Data in Large Scale Mobile Traffic Control Environments*" published in International Symposium on High Capacity Optical Networks and Enabling Tech. HONET, 2008.
14. X. Sun, J. Zheng, Q. Liu, Y. Liu "*Dynamic Data Replication Based on Access Cost in Distributed Systems*" Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009.
15. F. Huber, S. Molterer, A. Rausch, B. Sch¨atz, M. Sihling, O. Slotosch "*Tool supported Specification and Simulation of Distributed Systems*".
16. G. Yadgar "*Multilevel Cache Management Based on Application Hints*" PhD work Sumbitted to the Senate of Technion - Israel Institute of Technology, Iyar 5772,Haifa, in 2012.
17. Ben-Zvi, "*Causality, Knowledge and Coordination in Distributed Systems*", PhD thesis Submitted to the Senate of the Technion — Israel Institute of Technology Adar Bet 5771 Haifa March 2011.
18. R. Al Ekram and R. Holt, *"Multi-Consistency Data Replication"* published in 16th International Conference on parallel and distributed systesm in 2010.