International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 2 February 2018

Secure Storage and Replication Framework for Cloud Computing using Even-Odd Approach

Shweta Alguje[1], Dr. Harish Patidar[2]
CSE-LNCT, Indore (M.P) 452010, India[1]
Associate Professor, RGPV University, Bhopal(M.P)462001, India[2]
svs1391@gmail.com[1], harish.patidar@gmail.com[2]

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. A research on replication refers that security is the big anxiety, which creates insecure replication of data and it results in loss of trust on node and loss of data.

This paper investigates the difficulties of replication and observes that security is one of the major significant prerequisites in replication. Here, work proposed is for security design, for secure replication in dispersed frameworks. The entire implementation and evaluation have been utilizing java technology.

Keywords: *Cloud Computing;Replication;RSA;SHA-1.*

1. INTRODUCTION

Cloud permit there user to use data, resources, software, hardware, application etc. 88% of the consumer uses public cloud, 63% uses private cloud, this data is evaluated from a survey made by researchers. It is the platform which is beneficial for user and intruders are attracted towards it. Consumers have to pay for what they utilize from cloud. Cloud models are the service model which are described as infrastructure as a service, platform as a service and software as a service. IaaS is the base of cloud computing and is the first layer, where the resources and networks are managed and stored by service providers. To build, manage web application, develop and without any need to deploy infrastructure, a platform is provided to user, this service is called as PaaS, platform as a service. Example of platform as a service is Google app engine. The last model is software as a service model, where end user is provided with the service of software applications. This layer is SaaS and its example is, Email.

Cloud deployment models are the common model on the basis of which cloud is represented. For the individual access to resources public cloud is used, which is easily accessible. Private cloud made availability of services within an organization. Hybrid cloud is the combination of public and private cloud. Community cloud, in which services are accessible by the organizations or group of organization. Cloud services are used to store large files on cloud. Internet is used to run software on a server. It is the cost effective way to use cloud computing and take its advantages. Handling cloud is critical because of some issues, which is also not good for the confidential data saved on cloud.

Recovery point and recovery time of an application does not met is defined as Data Replication. It is essential due to disasters and is done for the backup recovery.

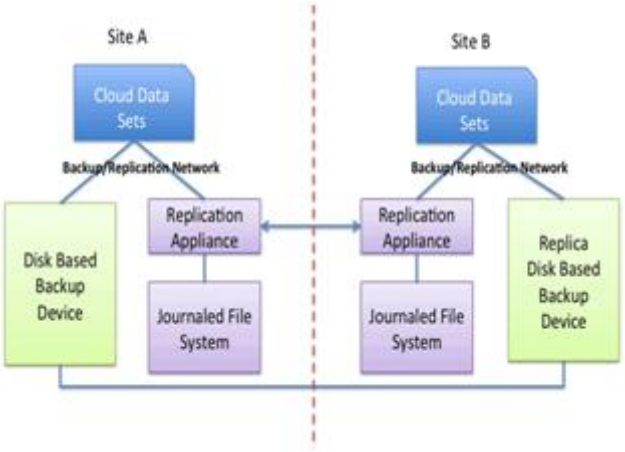

Figure 1.1 Data Replication in Cloud

1.1 Components of Cloud Computing:

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 data centers, disk, taps for storage purpose and database servers for management of data.

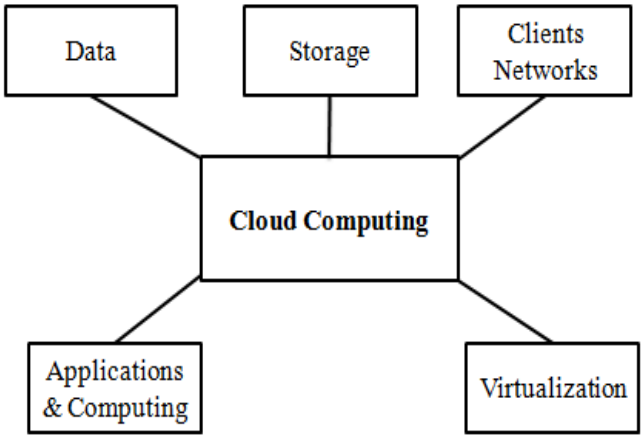

Figure 1.2 Components of Cloud Computing

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.

2. RELATED WORK

Sanjay Ghemawat et al. In[1] concluded about Google File system (GFS) to meet the rapidly growing demands of Google's data processing needs. Google file system shares many of the same goals as previous distributed file system such as performance, scalability and availability. The file stored through Google file service client are divided into chunks and indexed. Instructions are passed to chunk server for the file system, these instructions are passed through control messages and chunks are handled. Data message which is in the form of chunk data is forwarded to Google file system client.

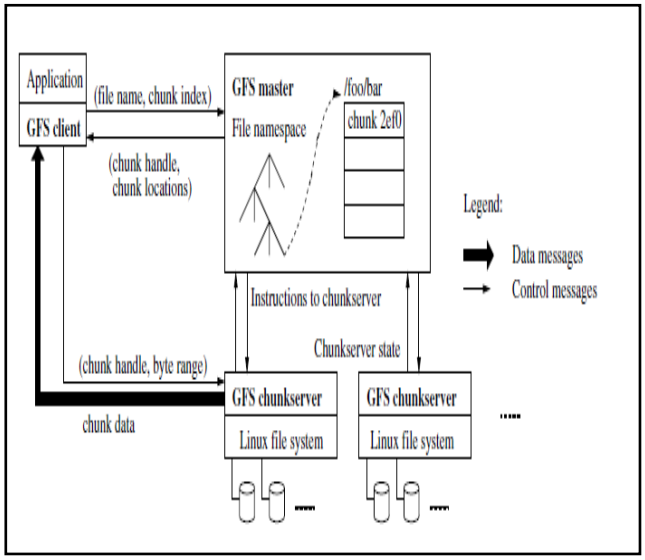

Figure 2.1 Google File System Architecture

AtulKahate et al.In[2] described about replication, where replication means creating duplicates of the present file or data. Distributed system for the process of replication concludes some challenges like integrity, confidentiality, authentication and facing this issue at the time of replication.

Birman et al.In[3] introduces about reliable distributed system, where data is stored on many computers and can be accessible by other system called client. Author concluded about client server computing by implementing NFS,

network file system. Its aim is to handle disk file system. Faces with the limitation of validating data.

XiuyanGuo et al.In[4] described about the dynamic replication of file. Issue arises in the video system for the replication of media file. Its performance for balancing load and storage is affected by the replication algorithm. Considering the flowing of media and its growing capacity handle the migrating files, which is responsible for acceptance rate. Author presented an strategy for transferring and deploying file through on demand system. The strategy computes the probability of migration at the time of request. All this done, through theoretical and experimental analysis to describe the improvement in acceptance rate request and media server.

Chao-Tung Yang et al. In[5] proposed about the technique called data grid which solves the issue of huge experimental data used in scientific work and simulations process. And also IDMSBN, for the reduction in cast maintenance, it uses Bayesian network with Implicit Dynamic Maintenance service (IDMSBN). It's centralized focus is only on the improvement of performance of replication, does not concentrate on security maintenance. It lacks in security.

3. PROBLEM DOMAIN

3.1 Overview

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.

3.2 Detailed Problem Statement

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.

- 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. can't 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.

4. PROPOSED METHODOLOGY

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.

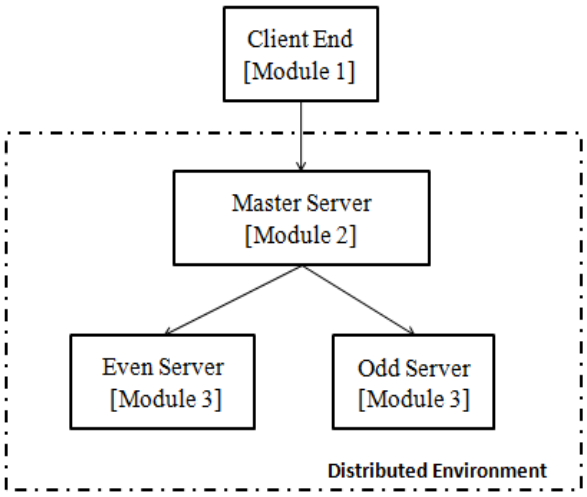

Figure 5.1 System Architecture

Step by step analysis of system architecture and its working is cited below:

1. Client end or module 1, where user can upload there file and is forwarded to master server for the secure replication and backup of file.
2. File is uploaded in cloud environment by user.
3. The distributed server receives the file from client end and for the secure replication it creates integrity using SHA-1.

SHA-1 is a cryptographic algorithm stands for Secure Hash Algorithm 1 and is used in our work to calculate integrity for the verification and authenticity of password. SHA 1 works as, whenever user enter there password, password is converted into checksum. The current password is checked by comparing it with the stored password. This is how integrity and verification is maintained using SHA-1.

4. After, it file is divided into chunks as per given size for further process, chunk preparation is done here.
5. Data is divided into chunks and is done for encrypting data, encryption is done for achieving and managing confidentiality of data.
6. Then replication of file and distribution is done.
7. File is replicated in different server called as even server and odd server. This scheme is the odd-even scheme for the replication of chunk file.
8. Even replica server replicates the even id of the chunk files.
9. Similarly, odd server works. Where, odd replica server replicates the odd id of chunk files.

5. RESULT

Result of the proposed solution for the given file size and computation time is represented through graphs.

The below graph represents RSA time computation graph for different file size.

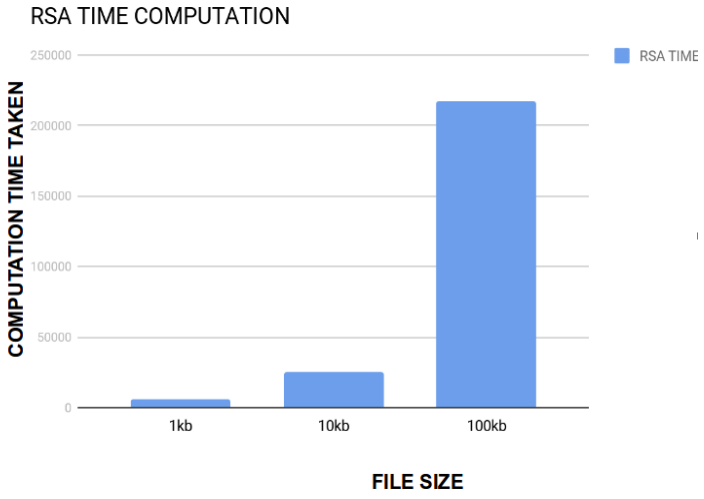

Figure 5.1 RSA Time Computation

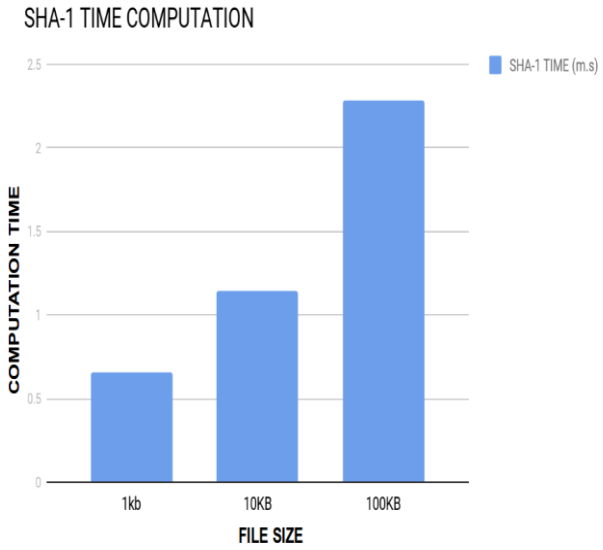

Figure 5.2 SHA-1 Time Computation

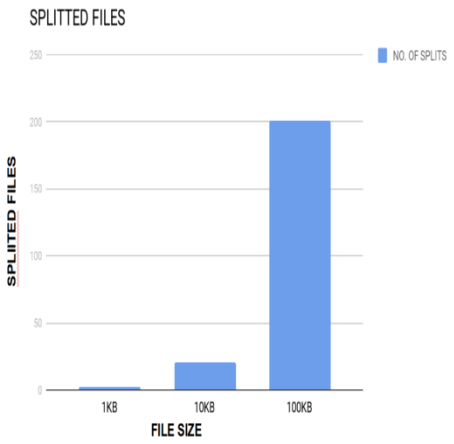

Figure 5.3 Graph of Splitted Flies

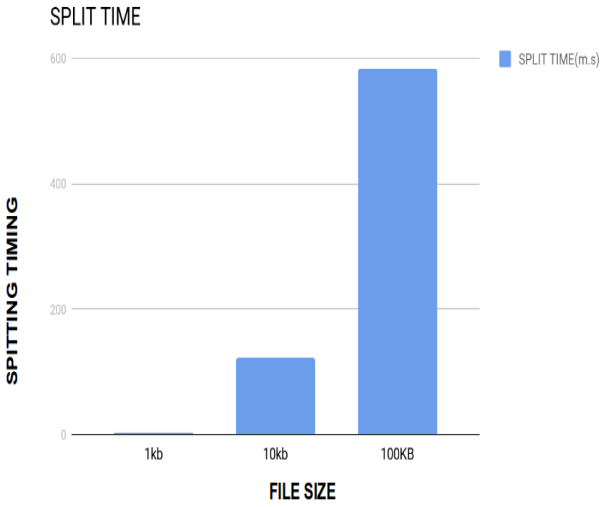

Figure 5.4 Graph of Splitted Times

6. CONCLUSION

In this modern time, new features are always added to maintain the privacy of data. Proper services are used for the exchange of information and security maintenance. Data used should be reliable and security is must. With different entities accessibility of services are in secure manner with secure transfer. Encryptions are changed depending upon the need. For confidentiality purpose encryption is must.

Despite the continues effort for file replication and consistency management, a secure method is still awaited. The complete study concludes that there is need to develop a separate security solution to establish secure replication scheme into cloud storage. Proposed solution not only helps to implement security with data file but also provide secure replication in distributed system.

REFERENCES

[1] Sanjay Ghemawat, Howard Gobioff, and Shun-TakLeung"The Google File System",2003.
[2] AtulKahate "Cryptography and Network Security", Second Edition-2003, Tata McGraw Hill New Delhi, 10th reprint-2010.
[3] Birman, Kenneth. Reliable Distributed Systems: Technologies, Web Services and Applications. New York: Springer-Verlag, 2005.
[4] XiuyanGuo, Jun Li, Jian Yang , "The Research on Dynamic Replication and Placement of File Using Dual- Threshold Dynamic File Migration Algorithm"2008.
[5] [Chao-Tung Yang Chien-Jung Huang Ting-Chih Hsiao "A Data Grid File Replication Maintenance Strategy Using Bayesian Networks",2008.
[6] H.Shen,; "Integrated File Replication and Consistency Maintenance in P2P Systems" , IEEE Transactions on Parallel Systems,Vol. 21,no 1, January 2010.
[7] Kang Chen and Haiying Shen Global Optimization of File Availability Through Replication for Efficient File Sharing in MANETs 2011.
[8] R. C. Merkle, "Protocols for public key cryptography," BNR Tech. Rep. Palo Alto, CA, 1980.
[9] R..M. Needham and M.D. Schroeder, "Using encryption for authentication in large networks of computers," Comm. ACM, vol.2, pp. 993-999, 1978.
[10] Manu Vardhan, AkhilGoel, AbhinavVerma, Dharmender Singh Kushwaha Demand Based File Replication and Consistency Mechanism2012.
[11] De Canniere and C.Rechberger Institute for Applied Information Processing and Communications (IAIK) Graz University of Technology, Inffeldgasse 16a A–8010 Graz, Austria "Finding SHA-1 Characteristics: General Results and Applications.
[12] 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. International Journal of Research and Scientific Innovation (IJRSI) Volume IV, Issue IX, September 2017 ISSN 2321–2705 www.rsisinternational.org Page 96

[13] R. Rivest, A. Shamir, and L. Adleman.A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM 21(2):120-126, Feb, 1978.

[14] Richard M. Karp and Michael O. Rabin Efficient Randomized Pattern-Matching Algorithms.Technical Report TR 31-81, Aiken Laboratory, Harvard University, December, 1981.

[15] MinzheGuo and Prabir Bhattacharya school of computing science and Informatics University of Cincinnati, Mechanism Design based Secure Data object Replication 2012 IEEE 11th International Conference on Trust, Security and Privacy in computing and communication.