ISSN:0975-9646

Security Enhancement for Cloud Storage Systems

Er.Harmanbir kaur , Prof.Meenakshi Sharma

Computer Science and Engineering, SSCET,
Badhani, PTU, Punjab, India

***Abstract*— Cloud enables us to put in many resources for use. However, many security threats have been associated with confidential data being saved in public cloud. With increase in business enterprise might decide to develop their own private storage cloud system. However, there are many security issues in PSC (Private Storage Cloud). In this paper, we have discussed security aspects to be taken care when saving data in cloud system. We have mainly discussed various cloud storage syetms (HDFS, Luster).We also discussed various security threats and its solution is provided. We have also provided the comparison of Existing System with the Proposed System.**

***Keywords*— HDFS, Luster, PSC, Cloud Storage, Session Hijacking, Spoofing**

I. INTRODUCTION

1.1 Cloud Computing:

A cloud is an integration of computational devices including hardware and software infrastructure that offers reliable, cost effective and persistent access to high speed computational capabilities. It can change the way of computing and data access. It follows the path from standalone systems to highly linked clusters, to enterprise wide clusters, to geographical dispersed computing environments.

1.2 Cloud Computing Framework:

Service Models: There are three service models of cloud computing:

Software as a service (SaaS): In this case the provider allows the customer only to use its applications. The software interacts with the user to use its applications. The software interacts with the user through a user interface. These applications can be anything from web based email to applications like Twitter.[2]The SaaS provider gives subscribers access to both resources and applications .SaaS makes it unnecessary for you to have a physical copy of software to install on your devices.

Platform as a Service (PaaS): A PaaS provider gives subscribers access to the components that they require to develop and operate applications over the internet. It is a set of software and development tools hosted on the providers servers. Google apps is one of the most famous Platform as a Service providers. Paas is an application development and deployment platform delivered as a service to developers over the Web.[2]Paas services include application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and database integration, security, scalability, storage, persistence, state management, application versioning.

Infrastructure as a Service Infrastructure-as-a-Service (IaaS): Infrastructure as a service delivers a platform virtualization environment as a service. Instead of purchasing servers, software, data centre space or network equipment, clients can buy these resources as outsourced service. In other words the client uses the third party infrastructure services to support its operations including storage, hardware, servers and networking components.

Cloud Framework System	Application/Software as a Service
	Platform as a Service
	Infrastructure as a Service

Figure 1 Cloud Computing Framework

1.3 Distributed File System

In this section, we will introduce three typical cluster file systems: Hadoop Distributed File System (HDFS), Luster.

A. ***Hadoop Distributed File System (HDFS):*** HDFS is designed to reliably store very large files as a sequence of data blocks across machines in a large cluster (see Figure2)[5].

Components of HDFS:

a. Name Node: The HDFS namespace is a hierarchy of files and directories. Files and directories are represented on the Name Node by inodes, which record attributes like permissions, modification and access times, namespace and disk space quotas. The Name Node maintains the namespace tree and the mapping of file blocks to Data Nodes.

a. Data Node: The Data Nodes are responsible for serving read and write requests from the file system's clients [11]. The Data Node gets the operation of creating, deleting, and replicating upon instruction from the Name Node.

b. Secondary Name Node: Secondary Name Node is responsible for saving the file system image (fsimage) in Name Node.

c. HDFS Client: User applications access the file system using the HDFS client, a code library that exports the HDFS file system interface.

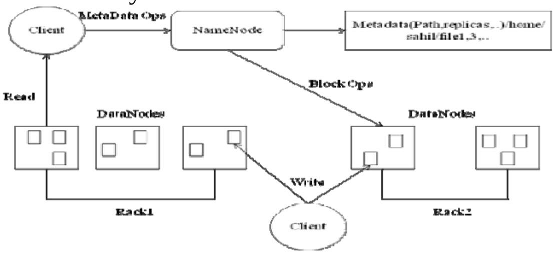

Figure 2 Architecture of HDFS

B. Luster File System: Figure 3 shows the architecture of Luster File System. Luster file system is a system that aims to provide high performance and scalability [1]. Its architecture consists of five components, including MDS (Metadata Server), MDT (Metadata Target), OSS (Object Storage Server), OST (Object Storage Target), and FSC (File System Client).

A. **MDS (Metadata Server):** MDS is responsible for all the operations on the file system name space.

B. **MDT (Metadata Target):** MDT is the storage of MDS. OSS provides the service of file I/O.

C. **OST (Object Storage Target):** OST is the storage of OSS.

D. **FSC (File System Client):** FSC can be used to access the file system [13]. It creates files, read or write files by transmitting instruction to MDS and OSS.

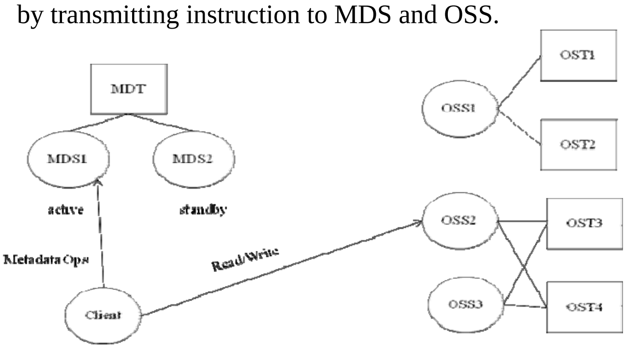

Figure 3 Architecture of Luster File System

Figure 3 shows the architecture of Luster File System. Luster file system is a system that aims to provide high performance and scalability [1]. Its architecture consists of five components, including MDS (Metadata Server), MDT (Metadata Target), OSS (Object Storage Server), OST (Object Storage Target), and FSC (File System Client). MDS is responsible for all the operations on the file system name space. MDT is the storage of MDS. OSS provides the service of file I/O. OST is the storage of OSS. FSC can be used to access the file system [13]. It creates files, read or write files by transmitting instruction to MDS and OSS.

II. LITERATURE SURVEY

Rajesh Lakshman Gaikwad , et.al (2013)[1] has examined Hadoop cluster and security for Hadoop clusters using Kerberos. In this Paper security is enhanced using role-based access control, reviewing built-in protections and weaknesses of these systems. There are several ways a user access the data on Hadoop Clusters. This paper explores those methods and also suggests some available methods for scalable, flexible and fine-grained hierarchical access methods for big data that may be consider for accessing data on Hadoop Clusters. There are many areas to improve in the various security aspects of Hadoop clusters and new technologies are proposed to ensure the security in terms of reliability and flexibility still lot of work is remaining to make Hadoop clusters as fully fledged database system in terms of user accountability and dynamic data updating.Qingni Shen, Yahui Yang, et.al (2012) [5] have proposed architecture of enforcing security services on the layer of HDFS including Data Isolation service, Secure Intra-Cloud Data Migration Service, and Secure Inter-Cloud Data Migration Service. SAPSC have implemented security in inter and intra cloud levels using AOP which makes it very easy to use and implement security in PSC and Public network based clouds in intra cloud system. The performance analysis of the security services proves the efficiency of the security design. These security services can also be compatible with other cloud storage software systems. SAPSC has considered internal and external threats where unauthorized data access can be attempted or data could be corrupted by unauthorized access to intra cloud systems separated by departments and regions.Wen-Feng Hsu,shyan-Ming Yuan,et.al (2012) [4] have proposed a low cost, flexible and recoverable private cloud storage system using NAS. The proposed system is called Aiolos. In this paper, techniques “migration” and “cell recovery” for enhancing the flexibility and recoverability are introduced and evaluated. The prototype implementation of Aiolos is based on HDFS.The evaluation shows that the performance of migration is related to the no. of files and size of file. For different cloud file system implementation, may not perform checksum calculation before add a file into file system. The calculation time may not exist, thus, the performance of migration based on other implementation would be better and obtain better speed up when comparing with pure file upload. The techniques presented in this paper could be realized on other cloud storage systems with necessary modification. Shaikh.F, Haider.S, et.al (2011)[6] have identified top security concerns of cloud computing and these concerns are Data loss, Leakage of Data, Clients trust, Users Authentication, Malicious users handling, Wrong usage of Cloud computing and its services, Hijacking of sessions while accessing data. This paper aims to identify most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing and also critical analysis about the different security models and tools proposed. Their work is limited on security issues of cloud computing. There is no security standards available for secure cloud computing.Minqi Zhou, Rong Zhang, et.al(2010) [10] have investigated a several cloud computing system providers about their concerns on security and privacy issues. it is found that those concerns are not adequate and more security strategies should be deployed in the cloud environment to achieve the five goals(i.e. availability, confidentiality, data integrity, control and audit) as well as privacy acts should be changed to adapt a new relationship between users and providers. The claimed that the prosperity in Cloud Computing literature is to be coming after those security and privacy issues. Kevin Hamlen , et.al(2010) [12] have discussed the security issues for cloud computing and present a layered framework for secure clouds and then focus on two of the layers, i.e., the storage layer and the data layer. This paper presents a scheme for secure third party publications of documents in a cloud and will converse secure federated query processing with map Reduce and Hadoop , and also discussed the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing.Sun Microsystem White Paper (2007)[13] provided basic information about the Lustre file system. It gives the general characteristics and markets in which the Lustre file system is strong. This describes a typical Lustre file system configuration and provides an overview of Lustre networking (LNET). It also introduces Lustre capabilities that support high availability and rolling upgrades. This Paper also describes some additional features of the Lustre file system and provides information about a how a Lustre file system compares to other shared file systems. R.P.Padhy,M.R.Patra,et.al(2011) [7]various models of cloud computing, security issues and research challenges in cloud computing are discussed. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. They have highlighted all these issues of cloud computing.. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture.

III. Hadoop Security Overview

Hadoop is an open source project and many security threats have been associated with confidential data being saved in public cloud. With increase in business enterprise might decide to develop their own private storage cloud system. Hadoop environment can include data of variety in classifications and security sensitivity concerns. Collection of data into one environment also increases the risk of data theft and disclosure. The technology to collect and store data from multiple sources can create problems like access control and management as well as data entitlement and ownership. However, there are many security issues in PSC. In our proposed system we have discussed security aspects to be taken care when saving data in cloud system. We have mainly discussed user authentication and data encryption.

3.1 SECURITY THREATS:

In Cloud Computing there are various security threats that may arise:

A. Session Hijacking*:* Session hijacking is when a hacker takes control of a user session after the user has successfully authenticated with a server. It involves an attack identifying the current session IDs of a client/server communication and taking over the client's session. The session ID is normally stored within a cookie or URL [2]. For most communications, authentication procedures are carried out at set up. Session hijacking takes advantage of that practice by intruding in real time, during a session. The intrusion may or may not be detectable, depending on the user's level of technical knowledge and the nature of the attack. If a Web site does not respond in the normal or expected way to user input or stops responding altogether for an unknown reason, session hijacking is a possible cause.

B. Spoofing*:* In the spoofing attack, the hacker performs sniffing and listens to traffic as it is passed along the network from sender to receiver. The hacker then uses the information gathered to spoof or uses an address of a legitimate system [10]. Hijacking involves actively taking another user offline to perform the attack. The attacker relies on the legitimate user to make a connection and authenticate. After that, the attacker takes over the session, and the valid user's session is disconnected.

Threat	Cause	Solution
Session Hijacking	Changing browser to behave like other users	Token sync between server and client.
Spoofing	Spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.	Token sync between all users and server.

Table 1 Security Threats, its causes and solution

IV.Performance Analysis

Below is the comparison cost of enhanced system with existing system. Compared with existing system, enhanced system has reduced cost and increased system.

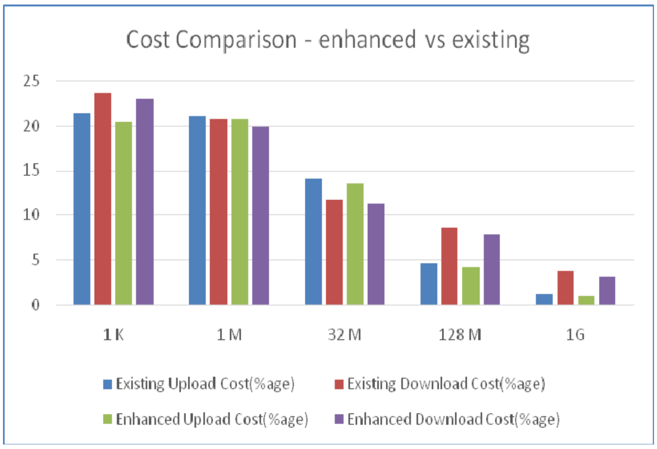

Figure 4 Graph showing the cost comparison between existing and enhanced system

V. Conclusion

In this Paper various security threats are discussed and its solution is provided. Proposed solution was compared with existing security technique. Our service based security system provides enhanced security as shown in results. In our proposed system, comparison of uploading and downloading cost is done and the results provide that the enhanced system has reduced cost and increased system.Securing private cloud storage system can be further researched for securing cloud systems from intra cloud data transfer security.

REFERENCES

[1] Rajesh Lakshman Gaikwad , et.al "Network Security Enhancement in Hadoop Clusters" International Journal of Application or Innovation in Engineering And Management (IJAIEM)",vol.2, pp.151-157,March 2013.

[2] H.Gajjar "Security Users Data in HDFS" International Journal of Computer Trends and Technology (IJCTT), vol.4, Issue5, pp.1327-1335May, 2013.

[3] Z.Cheng,H.Huang "Design and Implementation of Data Encryption in cloud based on HDFS" International Workshop on Cloud Computing and Information Security (CCIS), 2013.

[4] Wen-Feng Hsu,shyan-Ming Yuan,et.al "Constructing Private Cloud Storage Using Network Attached Storage", " 9th International Conference on Ubiquitous intelligence and Computing and 9th International Conference on Automatic and Trusted Computing, 2012.

[5] Qingni Shen, Yahui Yang, et.al "SAPSC: Security Architecture of Private Storage Cloud Based on HDFS" 26th International Conference on Advanced Information Networking and Applications Workshops, pp.1292-1297, IEEE 2012.

[6] Shaikh.F, Haider.S, et.al "Security Threats in cloud computing",6th International Conference on Internet Technology and Secured Transactions 2011 IEEE, pp.214-219,11-14December 2011,Abu Dhabi, United Arab Emirates.

[7] R.P.Padhy,M.R.Patra,et.al "Cloud Computing: Security Issues and Research Challenges",IRACST-International Journal of Computer Science and InformationTechnology&Security(IJCSITS),Vol.1,No.2,pp.136-146,December 2011.

[8] G.Jai Arul Jose,et.al "Implementation of Data Security in Cloud Computing"International Journal of P@P Network Trends and Technology,pp.18-22,Vol.1,Issue1,2011.

[9] Kuyoro S.O,Ibikunle F.,et.al "Cloud Computing security Issues and Challenges", International Journal of Computer Networks(IJCN),vol.3,Issue(5),2011.

[10] Minqi Zhou, Rong Zhang, et.al "Security and Privacy in Cloud Computing: A Survey" Sixth International Conference on Semantics, Knowledge and Grids, 2010.

[11] Shvachko, H. Kuang, S. Radia, R. Chansler " The Hadoop Distributed File System" In Proceedings of the 26th IEEE Symposium on Mass Storage Systems and Technologies,pp:1~10,3-7 May 2010,Nevada USA.

[12] K.Hamlen,M.Kantarcioglu,et.al "Security Issues for Cloud Computing" International Journal of Information Security and privacy,4(2),39-51,April-June 2010.

[13] Sun Microsystem White Paper (2007) "Lusture File System: High Performance Storage Architecture and Scalable Cluster File System" Sun Microsystem White Paper, 2007.