INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

SECURED CLOUD STORAGE USING MULTI-CLOUDS

M. V. Bramhe[1], M. V. Sarode[2] and L. G. Malik[1]
[1]Dept. of CSE, G.H.Raisoni College of Engineering, Nagpur
[2]Dept. of CE, Jagdamba College of Engg. & Technology, Yeotmal

Abstract:
Cloud computing is widely used by organizations for data storage as it is cost saving. However, security of data is major concern for users as whole important information is in the hands of cloud service provider who cannot be trusted fully. Main problems with single cloud service provider are vendor-lock-in, data integrity loss and malicious system administrator where cloud end user may not get access to data whenever needed which can be solved by moving towards Multi-Clouds. In this paper we have proposed secure cloud storage using multi-clouds. User can split data into multiple chunks and then securely upload it in various public cloud infrastructures. This system is secure as adversary / malicious system administrator will never get full copy of data. Service availability is also well addressed by multiple clouds.
Keywords: Cloud Computing, Multi-Clouds, Security, Storage

Introduction

Now a day's cloud computing has become successful and trendy computer paradigm because of "pay-as-you-go" model. Cloud Computing is defined by NIST as model for enabling convenient,on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. It consists of 5 essential Characteristics, three delivery models and four deployment models [1].Cloud security Alliance has given five necessary characteristics as on-demand self service, broad network access, resource pooling, rapid elasticity and measured services [2]. Cloud has three delivery model as software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a service (IaaS). Cloud has public, private, hybrid and community cloud as deployment models. Cloud computing helpscustomersto have less operational and capital expenses [3] but its unique architecture has raised various security and privacy concerns. Successfulness of cloud depends on how much security and privacy is provided to cloud provider and customer. Various solutions were proposed for handling cloud vulnerabilities and threats arising for maintaining confidentiality, integrity, availability, accountability like VM isolation, trusted computing, third party auditing, replication, encryption techniques, accountable Map Reduce etc [3] but most of which concentrate on single cloud environment which faces many problems like malicious system administrator, failure of service, untrusted cloud provider, data integrity loss and data intrusion problem which can be reduced by shifting from single to multi cloud environment [5]. It is observed that till 2010, only 20 % research was carried out in multi-clouds[4].

In multi Cloud environment user data is fragmented among various private / public clouds so that adversary cannot get complete set of data a time which removes most of threats occurring in single cloud environment. This data is managed by distributed file system (DFS) which is used to share and access files from multiple hosts in distributed environment with transparency to user. DFS has provided major breakthrough for Cloud Computing applications at multi cloud environment. Our objective is to design and implement secured cloud storage using multi-clouds with DFS mechanism .It will divide cloud user applications and data into multiple chunks, which will be deployed in multiple clouds in secured manner. Adversary and malicious system administrator cannot affect cloud user data as they can never get full information at one place.

Related Work

Several researchers studied security challenges and proposed various defense mechanisms related to Cloud computing models. In this section, we conduct a brief study of relevant work done. Zhifeng Xiao and Yang Xiao [3] described in their survey paper various security vulnerabilities, threat models and respective defense mechanism for confidentiality, availability, integrity, privacy-preservability and accountability. They have proposed various threats like Cross-VM attack, malicious system administrator for cloud confidentiality which can be defended by VM

placement prevention, No hypervisor model and use of trusted computing.

Single cloud environment is affected with service unavailability, malicious system administrator and data integrity challenges which can be solved by the use of multiple clouds. Mohammed A. Alzain et al. in [4] described multi-cloud model as combination of various clouds where user data will be distributed and executed simultaneously. It is observed that multi–cloud system performs better than single cloud environment because they distribute security, reliability and trust among different clouds. They have made a survey of various techniques available for multi cloud security like use of cryptography, secret sharing algorithm, DepSky system, redundant array of cloud storage (RACS) and HAIL protocol.

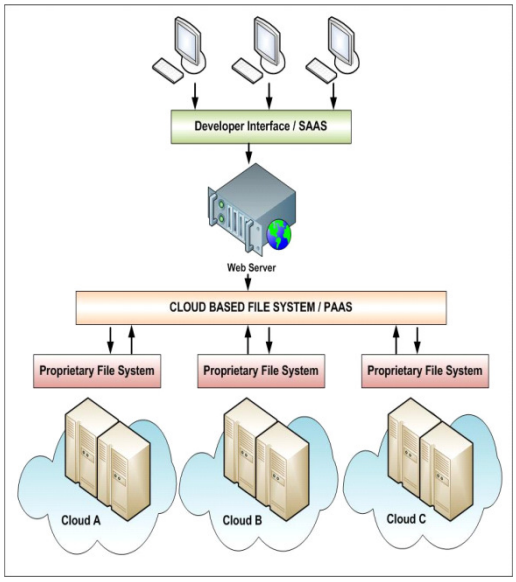
We came to the conclusion after review that we can attain more security by distributing user data and application among multiple clouds with full control to user at SaaS level. A distributed file system (DFS) is used to support storing and sharing of files of multiple users physically scattered in distributed network with location transparency. A DFS can solve purpose of secure storage with reducing most of challenges faced by single cloud. In [5] authors had given survey of various popular DFS like Google GFS, NFS, Andrew, KFS, Hadoop with their advantages and disadvantages based on features of architecture, processes, replication, fault tolerance and security. Survey shows that none of available DFS are fully secure. In [6] a revised Blakely's secret sharing mechanism is proposed to improve security and reliability of DFS without affecting scalability. This scheme does not require key management .To reduce computation overhead in this scheme, Graphical processing unit is used. Fan-Hsun et al. proposed secure and reliable cloud DFS using replacement of Hadoop DFS with open source based Tahoe least-authority file system [7]. This system improves fault tolerance by recovering data even though some storage nodes are faulty. It is more secure as Tahoe-LAFS incorporates AES encryption.

KhengKok Mar in [8] introduced multiple cloud based secure virtual diffused file system by hosting it on exiting setup of public cloud. This system used information dispersal algorithm to divide data into multiple parts and diffused them in various clouds. It used registry server for managing metadata and data distribution. This DFS scheme supports random read/ write and streaming I/O operations.

Proposed System

Cloud computing provides industry a wide range of security; still the data is not safe from malicious users having administrative rights. One having super user rights can access the data from cloud storage with wrong intensions. Proposed system is designed by keeping this scenario in consideration where we will distribute and secure the data at different location in order to hide original data directly from user. System willsplit the data securely using encryption in to different blocks and store it on the multiple clouds as per user request, now malicious user /system administrator can access the partial data which is of no use. Following figure shows proposed architecture of multi-cloud based secure storage service.

This system is divided into 3 parts as Web Interface at SaaS level, Distributed file system at PaaS level and multiple cloud services at bottom layer which will store user's data.



Proposed System Architecture

User will interact with web interface at SaaS level to select, split, encrypt and upload files in multi-clouds. User can perform encryption after splitting files or can split file first followed by encryption. Our DFS at PaaS level will upload chunks securely in multiple clouds which can be retrieved only by user whenever required as he only knows splitting and encrypting information. The system will also be able to download data even if some cloud service provider is not working, solving the problem of service availability.

Result and Discussions

We have proposed multi-cloud based secure storage. Currently very few researchers had proposed their systems in this area like DepSky, RACS, Icstore and HAIL [4]. We have developed basic version of system and hosted it in private cloud. We have tested it for basic operations like user registration, file split, encrypt, upload and download. We are currently studying open source DFS and will implement similar one with all functionality to test in real public cloud environment.

Conclusion

It is observed that organizations are still hesitating to use cloud for data storage solution as they considered cloud security as a major issue.Customers never want to lose their important information to the malicious user in the cloud. Major problems with single cloud architecture is service availability, data integrity loss and malicious system administrator which can be removed using multi-clouds

We support moving from single cloud to multi-cloud architecture as it will reduce security risks. We have proposed multi-cloud based secure cloud storage in which system will take decision on user request to securely distribute data in various public clouds where each cloud stores partial data hence malicious user never get full copy of data.

References

[1] Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas DRAFT Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2011

[2] Cloud Security Alliance (CSA). "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," (Released December 17, 2009), http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[3] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, March 2012

[4] MohammedA. AlZain, Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", IEEE 45th Hawaii International Conference on System Sciences, 2012

[5] Tran Doan Thanh, Subaji Mohan, EunmiChoil, SangBum Kim, Pilsung Kim "A Taxonomy and Survey on Distributed File Systems," IEEE Fourth International Conference on Networked Computing and Advanced Information Management, 2008

[6] Su Chen, Yi Chen, Hai Jiang, Laurence T Yang, Kuan-Ching Li, " A secure distributed file system based on revised Blakely's secret sharing scheme," 11th IEEE international conference on trust, security and privacy in computing and communications, 2012

[7] Fan-Hsun Tseng, Chi-Yuan Chen, Li-Der Chou, Han-Chieh Chao, "Implement a reliable and secure cloud distributed file system," IEEE international symposium on intelligent signal processing and communication systems, November 2012

[8] KhengKok Mar, "Secured virtual diffused file system for the cloud," 6th International IEEE conference on internet technology and secured transactions, UAE, December 2011