JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing the Security for Dynamic Data Sharing in Multi-Cloud Environment

Monica Mitra
Research Scholar,
Department of Computer Science and Engineering
Shri Venkateshwara University, Gajraula(Uttar Pradesh)

Prof. (Dr.) P. K. Bharti
Research Supervisor,
Hon'ble Vice Chancellor,
Shri Venkateshwara University, Gajraula(Uttar Pradesh)

Abstract

Cloud computing is sharing various computing resources rather than having local servers or personal devices to handle applications over the internet. To share these resources cloud provides three services namely, Software as a Service, Platform as a service and Infrastructure as a service. The deployment models of cloud include Private cloud, Public cloud and Hybrid cloud. Due to the benefits of cloud computing, there is a lot of data stored on cloud and multiple requests come for resources, hence it is customary to enforce adequate protection to the data in Cloud. Factors responsible for cloud security are Confidentiality, Privacy, Integrity and Availability of the data. The Multi-Cloud or 'Cloud–of–Clouds' has emerged as key solution to various obstacles faced in a single cloud platform. Multi cloud is highly needed due to the fact that sensitive data could not be entrusted to a single cloud and also to avoid dependency on just one cloud provider in risk of some failure. Hence switching the cloud computing from single cloud to multi-cloud is mandatory to fulfill data security. Existing Multi-cloud types include Intra Cloud, Hybrid cloud, Federated Clouds and Multi-Cloud. There are several approaches available to enhance security in multi-clouds. One of the methods is where data to be stored is split into various blocks and distributed among different cloud storage providers in a redundant way. Other methods include Homomorphic encryption, Attribute based Encryption (ABE), building a Multi-Cloud Database Model (MCDB) etc. This paper analyzes various research activities and methods for enhancing the security and safety in the Multi-Clouds.

KeyWords and Phrases: Cloud Computing, Cloud Service Provider, Cloud Security, Data Privacy, Data Availability, Encryption, Multi-Cloud.

INTRODUCTION

A model for ubiquitous, continuous, on-demand network access to a shared pool of reconfigurable computing resources, such as networks, servers, storage applications, and services, is known as cloud computing. It enables these resources to be quickly provisioned and re-leased with little management work or service provider involvement.

It's important to consider various features of cloud computing.The list is given below:

Multi- tenancy: Sharing computing resources, storage, services, and applications with other tenants who are residing on the same physical or logical platform at the provider's location is known as multi-tenancy (shared resources).

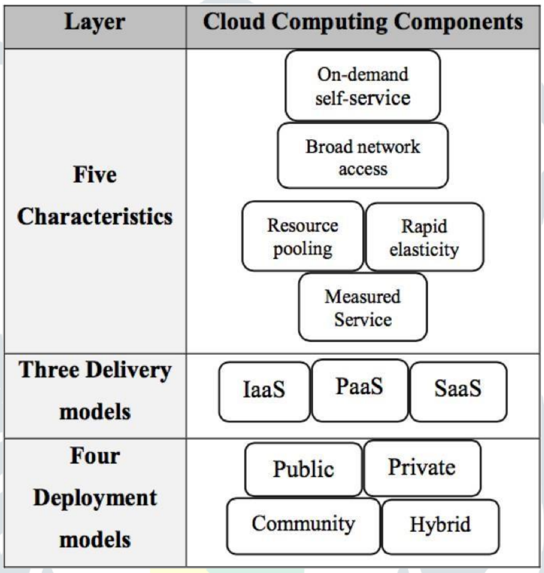
Huge scalability: An increase in systems, bandwidth, and storage capacity.
Elasticity: Users' computer resources are elastic and can be increased or decreased as needed.

Pay as we use: Users only have to pay for the resources and the time they actually utilize.

Self-provisioning of resources: Users set up their own networks, storage, and software.

Layers of Cloud Computing

The following diagram shows layers in Cloud Computing:



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

2. BENEFITS OF CLOUD COMPUTING

The advantages of cloud computing are significant. Organizations reap most benefits as they adopt cloud computing for IaaS, PaaS, or SaaS services.They are:

- Lower computing costs
- Improved performance
- Reduced software costs
- Instant software updates
- Unlimited storage capacity
- Device independence
- Increased data reliability

Given that cloud computing is one of the hottest emerging fields, potential security concerns must be addressed. This covers outsourcing, shared responsibility, extensibility, multi-tenancy, virtualization, and heterogeneity.

FACTORS OF CLOUD SECURITY

The following are the factors that are taken into consideration for Cloud Security:

- **Confidentiality**
- **Privacy**
- **Integrity**
- **Availability**

There are various security limitations of the Single Cloud that should be discussed before goinginto detail about cloud security. Those are explained below:

It's possible for the data in circulation between a client and cloud service provider to be damaged or lost.
A server malfunction in Danger's data centres results in the loss of all Sidekick users' data (directories of calendars, contacts, and photographs) in Microsoft. Microsoft realized after a year that the majority of the deleted data could not be recovered.
Due to a full failure, Server Magnolia experienced a total loss of data; the loss of half a terabyte of data rendered any attempt at recovery impossible, therefore rendering the websiteinoperable.
Data Confidentiality and Privacy: The primary priority of CSP should be safeguarding sensitive data, such as bank account information or medical records. An example of a breachin confidentiality is the ability to access all instances and resources of an Amazon account by only knowing the password.
Data Availability: If data is entrusted to a single Cloud provider who lacks a backup solution,hosts the data on a single platform, or is located in the same region, it increases the risk ofdowntime and puts customers in a situation where they are unable to access their data for several hours.
All of these call for the simple solution of transferring the data onto multiple clouds.

REASONS FOR MULTI CLOUD

A cloud storage architecture known as the "many clouds method" creates a virtual cloud storagesystem by combining various Cloud storage providers. The data that has to be saved is broken up into distinct pieces and redundantly distributed to numerous cloud storage providers. Because sensitive data shouldn't be trusted to just one cloud, having several clouds is essential to avoid reliance on a single cloud provider. To ensure data security, cloud computing must be switched from a single cloud to multiple clouds.

Existing Multiple-Clouds Types

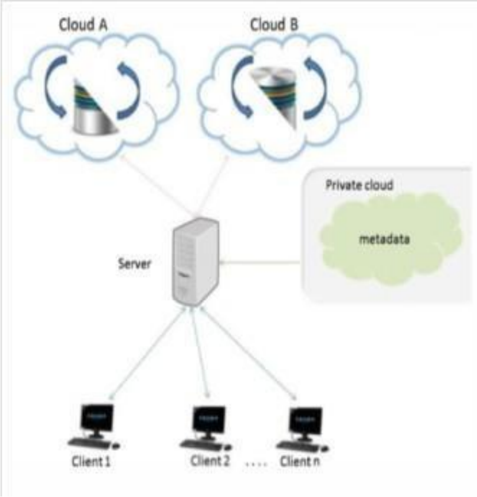
Intra Cloud: This cloud consists of two or more distinct services that work togetherand are owned by the same cloud provider.

Hybrid cloud: When the private cloud is unable to handle the processing and/or data load, this hybrid of a private and public cloud is used.
Federated Clouds: These are composed of two or more independent cloud service providers who have agreed to pool their infrastructure, work as a team to share resources, and provide the necessary services with a predetermined level of qualityservice.

Multi-Cloud: Using the available resources, more than one separate cloud will be employed to carry out the necessary tasks. The management of resources and capabilities, job scheduling, and load balancing will fall under the purview of thecustomers.

Multi-Clouds Architecture

Data is split up, kept in Clouds A and B, the broker can be outsourced to a reliable server, and the metadata is kept secretly in a private cloud. This paper conducted a review of the literature and analyzedseveral Multi-Cloud Security techniques.



Dai Yuefa et al used HDFS technique for Hadoop Distributed File System into which three level defence system structure using mathematical model was analysed.

Minqizhou et al studied availability, confidentiality, data integrity control and audit as well as analyzed privacy act which are outdated. Also multi-location issues were discussed.

Amarnath et al studied virtual machines utilization along with multiple virtual machines MVM's on the same server and its aspects of multi tenancy in VM's and their security.

AkhilBehl et al discussed the factors of multi tenancy, elasticity, SLA, secure information management, information integrity and privacy into cloud secure federation.

Jason Flood et al made a research on active protection system along with the risk of data exposure in a multi tenancy and environment in order to acquire secured data from third party using APS.

Eman M. Mohamed et al analysed encryption algorithm into which speed, higher security and performance were taken as the parameter in order to evaluate encryption time, which was least in AES.

Md Kausar Alam et al studied protecting the data in cloud algorithm sharing Shami's secret into the multi cloud system.

Mohammed A. Al Zain et.al constructed MCDB model for handling data in multi cloud system.

Ganesh A. Prajapati et al DepSky system was developed for enhancing the security into which Byzantine protocols, secret sharing algorithm were implemented.

Sura Khalil Abd et al followed a protocol and the usage of PEP and PDP for client accessingto PEP and PDP.

Veena Khandel- wal et al used database as a service and categorization of user data as well asit read the data privacy as normal sensitive and critical levels and split the user data into chunks and gave them to CSP's to provide database as a service which ensures client privacy
and data distribution.

He Kai, Huang Chuanhe et al employed public batch Data integrity auditing protocol and applied homomorphic cipher text verification for developing multi cloud storage and recoverable coding approach.

Vrushali K Gaik- wadl et al access Provable data possession (PDP) and proofs of retrievability (POR) and hence the client uses the secret key to preprocess a file which has collection of N blocks. It also generates a set of public verification information that is stored inTTP and hence TTP is verified.

Yun Tian et al secured replica allocation scheme called SecRA was studied into which security, reliability and performance of a cloud storage system were considered. Shamir secret key algorithm for data confidentiality was implemented and hence security, reliability and performance of a cloud storage system were improved.

Tara Salman et al distribution based, cryptography based and hybrid based solutions were studied for security requirements in multi cloud and its architecture and hence data security in multi clouds was strengthened.

CONCLUSION

A classification of data at rest and data in transit is necessary for the effective handling of data security aspects. Various analyses are carried out to examine the security of multiple clouds. Each strategy briefly covers the architecture required to improve security as well as the algorithm that was employed.

A breakthrough in multi-cloud security should integrate several cryptographic functions with the best algorithm for data encryption and deduplication techniques to store just one copy of the data, preserving data integrity and ensuring availability.

REFERENCES

- Dai Yuefa, Wu Bo, GuYaquang, Zhang Quan, Tang Chaojing.” Data Security Model for Cloud Computing”, Proceedings of the 2009 International
- Workshop on Information security and Application(IWISA 2009), China.
- Minqi Zhou, Rong Zhang, WeiXie, Weining Qian, Aoying Zhou, ”Security and Privacy in Cloud Computing: A Survey”, 2010 Sixth International
- Conference on Semantics, Knowledge and Grids.
- Amarnath Jasti, Payal Shah, Rajeev Nagraj and Ravi Pendse, ”Security in Multi- Tenancy Cloud”, IEEE 978–1-4244–7402-8/10 2010.
- Akhil Behl and KanikaBehl.“An Analysis of Cloud Computing Security Issues”IEEE/978–1-4673–4805-8/12, 2012.
- Jason Flood, Anthony Keane, ”A proposed Framework for the Active Detection of security Vulnerabilities in Multi-tenancy cloud Systems”, Third
- International Conference on Emerging Intelligent Data And Web Technologies, IEEE 978–0-7695–4734-3/12, 2012.
- Eman Mohamed, Hetem S. Abdelkar and Sherif El-Etrib.”Enhanced data Se- curity Model for Cloud Computing”, 8th International
- Conference on INFormatics and system (INFOS2012)–May 2012.
- Md KausarAlam, Sharmila Banu K, ” An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds”,
- International Journal of Scientific and Research Publications, Volume 3, Issue4, April 2013.
- Mohammed A. Al Zain, Ben Soh and Eric Pardede, ”MCDB: Using Multi- Clouds to Ensure Security in Cloud Computing”, Department of Computer
- Science and Computer Engineering, La Trobe University, Bundoora 3086, Aus-tralia.
- Ganesh A. Prajapati, SayaliS. Satav, Sonali Dahiphale, Sadhana More, Prof N. Bogiri. ”Cloud Computing Security: From Single to Multi-
- Clouds using Digital Signature”, International Journal of Engineering Tech- nology, Management and Applied Sciences Nov.2014 Vol.2 Issue ISSN 2349- 4476.
- Sura Khalil Abd, Rawia TahirSalih, S.A. RAl Haddad, Fazirul- hisyamHashim.“Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol” IEEE/978–1-4799–8641- 5/15, 2015.
- Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah Masrah Azrifah AzmiMu- rad, Faculty of Computer Science & IT IInformaton System Department, Uni- versity Putra Malaysia, ” Security Framework of Cloud Data Storage Based on Multi Agent System Architecture-A Pilot Study”.
- Amandeep Kaur, Sarpreet Singh. “An efficient data storage Security Algorithm Using RSA algorithm”.–International Journal of Application or Innovation in Engineering & Management (IJAIEM) March 2013.

- Veena Khandelwal. ”Secure and Efficient Data Storage in Multi- Clouds”.- International Journal of Information and Computation Technology- November 9 2013.
- He Kai, Huang Chuanhe, Wang Jinhai, Zhou Hao, Chen Xi, LuYilong Zhang Lianzhen, Wang Bin, Computer School, Wuhan University, Wuhan, China “An Efficient Public Batch Auditing Protocol for Data Security in Multi-Cloud Storage”-IEEE/978–0-7695–5058-9/13 2013.
- Abdul Razague, saty Siva VarmaNadimpalli, SuharshVommina. “Secure Data Sharing in Multi–Clouds”.
- Prakash G L, Dr Manish Prateek and Dr Indersingh.”Data security Algorithms for Cloud storage system using Cryptographic Method”.-March 2014 Interna- tional journal of Scientific & Engineering Research, volume 5, Issue 3.
- Prakash G L, Dr Manish Prateek and Dr Indersingh.”Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud Sys- tem”, April 2014, International journal of Engineering And Computer Science,Volume 3, Issue 4.