International Journal of Pure and Applied Mathematics
Volume 118 No. 6 2018, 323-334
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Survey on Data Security in Multi-Cloud Environment

D.I. George Amalarathinam[1] and J. Madhu Priya[2]
[1]Jamal Mohamed College (Autonomous),
Tiruchirappalli–620 012.
di_george@ymail.com
[2]P.G Saradha Gangadharan College,
Pondicherry.
madhupriyanarassimman@gmail.com

Abstract

Cloud computing is sharing various computing resources rather than having local servers or personal devices to handle applications over internet. There are different types of cloud services namely, Software as a Service, Platform as a service and Infrastructure as a service. 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 Clouds. Factors of cloud security are Confidentiality, Privacy, Integrity and Availability. The Multi-Cloud or 'Cloud–of–Clouds' has emerged as key solution to various obstacles faced in single clouds. Multi cloud is highly required due to the fact that sensitive data should not be entrusted to a single cloud, to avoid dependency on just one cloud provider. 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. 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 implementing the same in Multi-Clouds.

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

1 Introduction

Cloud computing is a model for enabling ubiquitous, continuous, on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

There are several different aspects of Cloud Computing that must be looked into. They are given below.

Multi-tenancy (Shared Resources): sharing computational resources, storage, services and applications with other tenants residing on same physical or logical platform at the provider's place.

Massive scalability: Increase in the number of systems, bandwidth, and storage space.

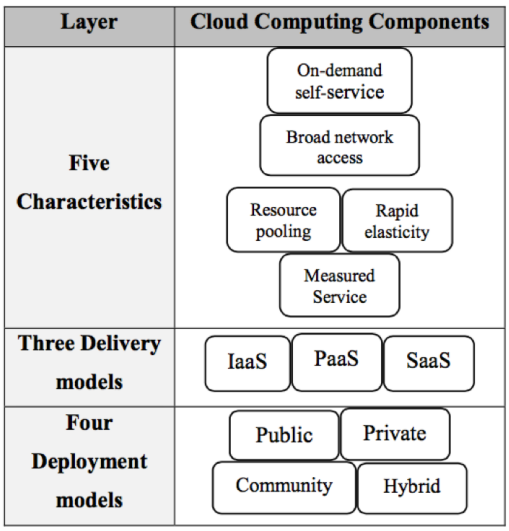
Elasticity: users can increase or decrease their computing resources as needed.

Pay as we use: users to pay for only the resources they actually use and for the time they require them.

Self-provisioning of resources: users self-provision resources such as software, storage and network.

Layers of Cloud Computing

The following diagram shows layers in Cloud Computing:



2 Benefits of Cloud Computing

There are predominant advantages of Cloud Computing. As Organizations make use of Cloud in IaaS or PaaS or SaaS services, they enjoy maximum benefits. They are

- Lower computing Costs
- Improved Performance
- Reduced Software Costs
- Instant software updates
- Unlimited storage capacity
- Device Independence
- Increased data Reliability

As Cloud Computing being hottest emerging area, there are potential Security Concerns in Cloud Computing which need to be addressed. This includes Outsourcing, Extensibility and Shared Responsibility, Virtualization, Multi-tenancy, Service Level Agreement and Heterogeneity.

3 Factors of Cloud Security

The following are the factors of Cloud Security.

- Confidentiality
- Privacy
- Integrity
- Availability

Before elaborating the details of Cloud Security, **there are several Security limitations of the Single Cloud**

(1) Data Integrity The transmitted data between the client and cloud providers may be lost or corrupted. Examples given below:

(2) A loss of all Sidekick users' data (directories of calendars, contacts photos) due to a server malfunction in Danger's data Centers (Microsoft). After one year Microsoft has conceived that the majority of the lost data cannot be covered.

(3) Server Ma.gnolia has suffered a total loss of data due to a complete failure; the loss of half a terabyte of data has made the process of recovery impossible, making the site essentially dead.

(4) Data Confidentiality and Privacy: Protecting sensitive data such as Bank details or documents of health care should be the top priorities of CSP. Example of loss of confidentiality occurred: by just knowing the AMAZON account password, the totality of account‘s instances and resources can be reached.

(5) Data Availability: If the data is entrusted to a single Cloud provider and does not have a backup solution, or it hosts the data in a single platform or in a same geographical area, this will increase the risk of downtime and it will cause customers who can get stuck for several hours without access to their data.

All these necessitate the obvious solution of moving the data into more than **ONE CLOUD**

4 Reasons for Multi-Clouds

Multi clouds approach is a cloud storage architecture that builds a virtual cloud storage system by using a combination of different Cloud storage services. Data to be stored is split into various blocks and distributed among different cloud Storage providers in a redundant way.

Multi clouds is highly required due to the fact that sensitive data should not be entrusted to a single cloud, to avoid dependency on just one cloud provider. Hence switching the cloud computing from single cloud to multi-clouds is mandatory to fulfill data security.

4.1 Existing Multiple-Clouds types

(1) Intra Cloud: This cloud has two or more different services that belong to the same cloud provider and that collaborate together.

(2) Hybrid cloud This is a combination between a private and single cloud, and used when the private cloud cannot deal with the processing and /or data load.

(3) Federated Clouds: This has two or more independent cloud–service providers that agreed to share their infrastructure and collaborate together for sharing resources and deliver the required services with agreed Quality of Service.

(4) Multi-Cloud: It is more than one independent cloud that will be used to execute the requested tasks through the available resources. The customers will take the responsibility of resources/capabilities managing, task scheduling and load balancing.

4.2 Multi-Clouds Architecture

Broker can be outsourced to a trusted server, data is divided into parts, stored in Cloud A and B and the metadata is stored privately in a private cloud.

This Paper carried out a Literature Review and analysis of various methods in Multi-Cloud Security.

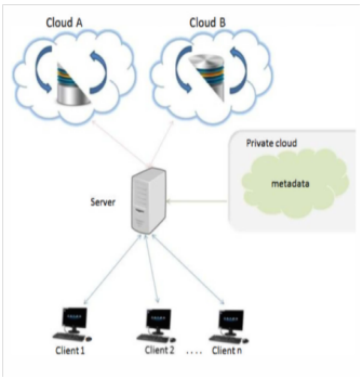


Table 1: Literature Review.

No.	Author name	Technique	Implementation Details	Advantages
1	Dai Yuefa et al	HDFS	Hadoop Distributed File system	Three level defense system structure using mathematical model
2	Minqizhou et al.	Availability, Confidentiality, Data Integrity, Control and Audit are addressed	Analyze privacy acts which are outdated	Multi-location issues were discussed
3	Amarnath et al.	Virtual machines utilization	Multiple virtual machines (VM's) on the same server	Aspects of Multi tenancy in VM's and their security
4.	AkhilBehl et al.	Factors of Multi-tenancy, Elasticity are discussed	SLA, Secure information Management, information Integrity and privacy	Cloud secure federation
5.	Jason Flood et al.	Active Protection system	Risk of data exposure in a multi-tenancy environment	Secured data from third parties using APS
6.	Eman M. Mohamed et al.	Analysed 8 Encryption algorithms	Speed, higher security and performance were taken as parameters	Encryption time was least in AES
7.	Md Kausar Alam et al.	Shamir's Secret sharing algorithm	Multi-clouds and use of Shamir's Secret sharing algorithm	Protection of data in cloud
8.	Mohammed A. Al Zain et.al.	MCDB model	Architecture of MCDB to handle data in multi-clouds	Development of a model to handle data in multi-cloud

Continued...

Continued from previous page

No.	Author name	Technique	Implementation Details	Advantages
9.	Ganesh A. Prajapati et al.	DepSky System	Byzantine Protocols, Secret Sharing Algorithm are implemented	Security is enhanced
10.	Sura Khalil Abd et al.	AAAS protocol	Usage of PEP & PDP	Client accessing to PEP, PDP done
11.	Amir Mohamed Talib et al	Multi-Agent System (MAS)	Interacting with each Other across a network	Security framework
12.	Amandeep Kaur et al.	RSA algorithm	RSA alg for data storage	Data security
13.	Veena Khandelwal et al.	Database as a Service and categorization of user data	Treating data privacy as 'Normal', 'Sensitive' and 'Critical' levels and split the user data into chunks and give them to CSP's to provide Database as a Service	Client privacy and data distribution
14.	He Kai, Huang Chuanhe et al.	Public batch data Integrity auditing protocol	Applied homomorphic cipher text verification	Multi-cloud storage and recoverable coding approach
15.	Abdul Razaque et al	Lagrange polynomial of the form: $f(x) = \sum_{i=0}^{2} Y_i(l)$	Using polynomial, secret points are computed	Data sharing in Multi-clouds
16.	Prakask G.L. et al.	MAC	Computing the MACs for entire file with a set of secret keys before the file is sent to the Cloud Server. When the key is revealed to the cloud server by the data owner, a new MAC is computed	Signature generation function for every block using hashing function
17.	R.K. Banyal et al.	Dynamic Trust Based Access Control Frame work (DTBAC)	Centralized access control for cloud resources	Security of cloud is ensured
18.	Vrushali K Gaikwadl et al.	Provable data Possession (PDP) & Proofs of Retrievability (POR)	The Client uses the secret key to pre-process a file which has collection of n blocks. It also generates a set of public verification information that is stored in TTP	TTP is verified

Continued...

Continued from previous page

No.	Author name	Technique	Implementation Details	Advantages
19.	Yun Tian et al.	Secure replica allocation scheme called SecRA	security, reliability and performance of a cloud storage system, Shamir secret key algorithm for data confidentiality	Security, reliability and performance of a cloud storage system are improved
20.	Tara Salman et al.	Distribution based, Cryptography based and Hybrid based solutions	Security requirements in Multi-Cloud, Its architecture	Data security in multi-clouds is strengthened
21.	C. Divya Shaly et al.	CHARM	High availability data hosting scheme	Cost-efficient data hosting scheme
22.	A. Manimaran et al.	efficient based privacy preserving authentication protocol(EAPA)and Anonymous ID assignment based data sharing algorithm	Authentication without compromising a user's private information. The data integrity verification is done by using a Third party auditor. It used Anonymous ID assignment based data sharing algorithm	Data integrity verification is done
23.	Weijuan Fan et al.	Trust management	Trust management architecture based on a group of distributed Trust Service Providers (TSP's)	Multi-cloud trust management is discussed
24.	Maha TEBAA et.al.	BFT, DEPSKY, RACS, HAIL and IC Store	Limitations of single cloud and proposed security mechanisms in Multi-clouds namely BFT, DEPSKY, RACS, HAIL and IC Store	Security of data in multi-cloud is evaluated with 5 different methods
25.	Mark D. Ryan et al.	Homomorphic Encryption	Data replication, availability of stored data, dependability of the clouds, high authentication level, Security through auditability, Robust Data sharing with Key (RDSKVS), High Availability and Integrity Layer(HAIL)-developed as an updated Version of (RAID)	High Data security is achieved

Continued...

Continued from previous page

No.	Author name	Technique	Implementation Details	Advantages
26.	hassanO. Karame et.al.	Message locked Encryption (MLE) Popularity based solution	Limitations of single cloud are discussed and Byzantine fault tolerance protocol, Depsky model, RACS, HAIL, IC Store are designed for multi-cloud security	High Data security is achieved
27.	Ouadia Zibouth et.al	Depsky-A and Depsky-CA	Convergent encryption which encrypts data with a unique key that is derived. Popularity based solution: use convergent encryption for more sharing data and use semantically secure encryption for user's personal data	2 different kinds of encryptions are done
28.	Jun T Tang et.al	Confidentiality, Integrity and Privacy are addressed	Data is divided into blocks as $f+1$ blocks are necessary to recover the original data and f or less blocks were not enough to retrieve the original stored data, Confidentiality by Assured Cloud Data service, Owner Controlled Cloud data sharing, Integrity-Guaranteed Cloud Data Storage, Privacy-preserving Cloud Data Access	Cost of cloud storage is minimized. Security of data storage and data access are implemented

5 Conclusion

There are different analysis that are conducted to look into the security of multi-cloud and a classification about data at rest and data in transit is required for efficient handling of data security features. Each approach discusses briefly about the algorithm used and the architecture needed to enhance the security.

A novelty in multi-cloud security should have the flavors of cryptographic functions combined with the selection of best algorithm for encryption of data together with Deduplication measures to ensure one copy of the data is stored thereby ensuring data Integrity and ensure availability

References

[1] 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.

[2] 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.

[3] Amarnath Jasti, Payal Shah, Rajeev Nagraj and Ravi Pendse, "Security in Multi-Tenancy Cloud", IEEE 978–1-4244–7402-8/10 2010.

[4] Akhil Behl and KanikaBehl."An Analysis of Cloud Computing Security Issues" IEEE/978–1-4673–4805-8/12, 2012.

[5] 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.

[6] Eman Mohamed, Hetem S. Abdelkar and Sherif El-Etrib."Enhanced data Security Model for Cloud Computing", 8th International

Conference on INFormatics and system (INFOS2012)–May 2012.

[7] 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.

[8] 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, Australia.

[9] 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 Technology, Management and Applied Sciences Nov.2014 Vol.2 Issue ISSN 2349-4476.

[10] Sura Khalil Abd, Rawia TahirSalih, S.A. RAl Haddad, FazirulhisyamHashim."Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol" IEEE/978–1-4799–8641-5/15, 2015.

[11] Amir Mohamed Talib, Rodziah Atan, Rusli Abdullah Masrah Azrifah AzmiMurad, Faculty of Computer Science & IT IInformaton System Department, University Putra Malaysia, " Security Framework of Cloud Data Storage Based on Multi Agent System Architecture-A Pilot Study".

[12] 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.

[13] Veena Khandelwal. "Secure and Efficient Data Storage in Multi- Clouds".-International Journal of Information and Computation Technology- November 9 2013.

[14] 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.

[15] Abdul Razague, saty Siva VarmaNadimpalli, SuharshVommina. "Secure Data Sharing in Multi–Clouds".

[16] Prakash G L, Dr Manish Prateek and Dr Indersingh."Data security Algorithms for Cloud storage system using Cryptographic Method".-March 2014 International journal of Scientific & Engineering Research, volume 5, Issue 3.

[17] Prakash G L, Dr Manish Prateek and Dr Indersingh."Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", April 2014, International journal of Engineering And Computer Science, Volume 3, Issue 4.

[18] R.K. Banyal, V.K. Jain, Pragya Jain, "Dynamic Trust Based Access Control Frame Work for Securing Multi-Cloud Environment", ACM/ 978–1-4503-3216–3/14/11.

[19] Ms Vrushali K Gaikwadl, Prof. Ramesh Kagalkar. "Data Security & Availability in Multi-clouds Storage with Cooperative Provable Data Posession".–IJES February 2015.

[20] Yun Tian, Xiao Qin, Yafei Jia." Secure Replica Allocation in Cloud Storage with Heterogeneous Vulnerabilities".–IEEE/978–1-4673-7891–8/15.

[21] Tara Salman. "On Securing Multi-Clouds: Survey on Advances and Current Challenges", Nov 2015.

[22] C. Divya Shaly, R. Anbuselvi, " Multi-Cloud Data Hosting for Protection Optimization and Security"-International Journal of Computer Science and Mobile Computing. April 2016.

[23] A. Manimaran and K. Somasundaram."An efficient Data Security Mechanism in Cloud Computing Using Anonymous ID algorithm. 2016.

[24] Mark D. Ryan, "Cloud computing security: The Scientific challenge and a Survey of solutions". Elsevier 2013.

[25] Maha Tebaa, Said El Hajji, " From Single to Multi-Clouds Computing Privacy and Fault Tolerance". Elsevier 2014.

[26] Farrukh Shahzad, " State–Of–the–art Survey on Cloud Computing Security Challenges, Approaches and Solutions". Elsevier 2014.

[27] Ouadia Zibouth, Anouar Dalli, Hilal Drissi, "Cloud Computing Security through parallelizing fully Homomorphic Encryption Applied To Multi Cloud Approach".–Journal of Theoretical and Applied Information Technology ATIT, May 2016.

[28] Hassan Saad Alqahtani, Paul Sant, " Multiple-Clouds Computing Security Approaches: A Comparative Study". ACM Transactions 2016.

[29] Jun Tang, Tsinghua et al." Ensuring Security and Privacy Preservation for Cloud Data Services"–ACM Computing Surveys June 2016.

[30] Young Joo Shin, "A Survey of Secure Data Deduplication Schemes for Cloud Storage Systems". ACM Computing Surveys January 2017.

[31] Ghassan O. Karame, Matthias Neugschwandtner et al. "Reconciling Security and Functional Requirements in Multi-tenant Clouds", ACM Transactions April 2017.