IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

Security Aspects of Cloud Based Environments

E. Suganthi[1*], F. Kurus Malai Selvi[2]

[1,2]Dept. Of Computer Science, Govt. College for Women (A), Kumbakonam, India

Corresponding Author: esuganthi@rediffmail.com

Available online at: www.ijcseonline.org

Abstract— Cloud computing is a specialized form of distributed computing. It involves introduction of utilisation models for effective utilisation, remote provisioning, and scalability of measured resources available, ending up in creating useful working environments. Virtualization separates functions from hardware and allows creation of multiple simulated environments or dedicated resources from one physical hardware system to other. It gives specific users, access to packaged resources in on-demand basis, for specific purposes. Virtualisation allows all types of resources to be added to a system, which is managed by a single operating system or Administrator. The concept of virtualization has two serious battles ahead, one is that of data security and the other one is to meet the demand from corporate to store their client data safely. The threat of data breach is generating newer techniques in virtualisation leading to multiple virtual environments being linked,so that it reduces possibility of hardware failure and data security breach. Virtualisation management is also one key element of the virtualisation process and it provides the ability to create, modify, transform and link the virtualised environments in order to effectively manage the environment. With the advent of linking virtual environments, new concept of Multi cloud has come up, wherein multiple cloud services are interconnected or multiple cloud services are accessed by the user for one particular job. This paper proposes to look upon the techniques that shall transform the future of cloud and the security or insecurity that shall come with it.

Keywords— Virtualization, Cloud computing, Multi cloud, Data security, Virtual environments

I. INTRODUCTION

Cloud Computing provides resources to users in a new way "as a service accessible via the internet". The old approach towards storage of data was that the owner of the data stored the data too. However, the modern approach towards cloud computing has taken the data storage process to the cloud service provider. Here the cloud computing user does not own the infrastructure which stores the data. This transfer of infrastructure control and storage of data in the cloud, has transferred the responsibility associated with data security. This gives rise to data security and privacy issues. In this paper, we deal with data security aspects related to the use of cloud computing.

II. CLASSIFICATION BASED ON DATA SECURITY

Data security is a common concern in all technologies. As cloud computing is a relatively uncontrolled environment, it is a major challenge to secure data. We need to distinguish between the security risks associated with the use of cloud computing and that which is common to all IT infrastructures. These risks are generally associated with open, shared and distributed environments. Therefore, when analyzing the risks, it is important to separate existing problems from those raised by Cloud Computing. Data outsourced to Cloud infrastructure is more vulnerable than that stored on a traditional infrastructure, mainly for three reasons: (1) data is stored on the service providers infrastructure (2) data of different users shares the same physical infrastructure(3) data is accessible via internet.

2.1 Issues of Data related to Cloud Environment

Cloud infrastructure is different from traditional infrastructure. These differences offer many benefits but also introduce numerous inconveniences, which may affect security. The main characteristics and their direct benefits and inconveniences are as follows:

Leased infrastructure

Infrastructure in cloud no longer belongs to user but to the service provider. The user need not purchase dedicated hardware and is free to lease it for a payment from any cloud service provider. While there is a cost savings advantage, loss of control over data is the major disadvantage.

Open infrastructure

Generally Cloud infrastructure is accessible via internet. Advantage of such infrastructure is ubiquitous access to services, and multiple entry points is its main disadvantage.

Shared infrastructure

Unlike dedicated traditional infrastructure, Cloud infrastructure is shared among service users. While it has a cost savings advantage, isolation failure risk between various users of the cloud is the disadvantage.

Elastic infrastructure

Resources can be scaled up and down according to their need. Therefore, unlike the traditional infrastructure that depends on peak of demand, Cloud infrastructure is scaled to current demand. Optimal use of resources is the advantage and resource reallocation risks is the major disadvantage.

Virtualized infrastructure

Basic concept behind cloud is Virtualization .It refers to a Virtual machine. Advantage is infrastructure optimization and disadvantage is classical problems associated with virtualization.

Distributed infrastructure

Infrastructure of cloud is distributed geographically around the world. Advantage is increased Computing and storage capacity. Disadvantage is Management and maintenance of infrastructure.

III. BENEFITS OF VIRTUALIZATION IN CLOUD ENVIRONMENT

There are predominant advantages of virtualization[26]. They are

- Protection from System Failures
- Glitch free Transfer of Data
- Firewall and Security
- Smoother IT Operations
- Cost-Effective Strategy

IV. MULTICLOUD ARCHITECTURE

Storage and computing of data within a single varied and assorted architecture is called a Multicloud architecture. This is also known as a Polynimbus cloud strategy. It involves distribution of almost all of the cloud assets, related software applications, operating systems etc., across multiple cloud-hosting environments. A typical multi cloud architecture eliminates provides the freedom of carrying out operations across many cloud service providers. This process involves using more than one public cloud as well as multiple private clouds. In a hybrid cloud environment we use multiple deployment modes like public cloud and private cloud and compute within a single service provider. In a multicloud architecture we use multiple cloud services.

4.1 Multi-Clouds Database Model

Multi-Clouds Database Model presents cloud with database storage in multi clouds service provider. It is unlike one of the pioneer cloud service like Amazon cloud service which provides a single cloud storage data. MCDB model does not provide security by using a single cloud. MCDB model provides security and privacy of data implementation of multi shares technique on multi-cloud providers. With this approach the MCDB model nearly eliminates the negative effects of single cloud.

- Security risks from malicious insiders residing inside a single cloud environment and having potential to access entire data is reduced.
- Negative impact of encryption techniques, failure of encryption decryption keys is reduced.
- Data is replicated inside several clouds by using a secret sharing approach. Potential of a single cloud crash is eliminated
- Offers a option to transfer or shift entire data base to some other trusted cloud service with ease.

But, at the same time, breach in data security can occur from the point of Cloud Management Programs (CMP's), as many of these CMP's would not have been created in the same pattern.

V. CLOUD SECURITY

Cloud computing has brought about several advancements in various fields. These advancements have been in areas like improving

- Scalability
- enhancing bandwidth
- providing efficient methods for load balancing
- taking backups

Enhancing cloud security requires knowledge on the following aspects**.**

1)Where in the cloud is the data stored

Cloud provides a nearly unlimited amount of storage capacity. Many System Administrators and Data security experts at the organisational level are not convinced in migration of their data to the cloud for one simple reason. They simply do not know where their data is physically stored on the cloud..

2) Level of Cloud Data Encryption

The next major area of security is that of confidentiality of data. This requires deployment of various data encryption techniques and related keys. While the organisation can plan the encryption of data, planning for the encryption of the entire cloud is a big security concern.

3) Disaster Recovery & Backup Plan

Data in the cloud is stored at physical storages located around the globe. Organisations have to make sure that their cloud service provider has a well planned disaster recovery and backup in place, to prevent data theft. There is also the need to keep the system downtime at the barest minimum. So, organisations must have a effective disaster recovery plan in place.

4) Knowledge on Cloud Managers

Security of the cloud and its data requires very efficient cloud service professionals and workforce. The cloud managers should possess vast experience in handling data breach, data theft and keeping the downtime to the barest minimum. Otherwise subscribing to a cloud environment will be a wise decision. A versatile cloud manager and workforce will form the backbone of an effective cloud based infrastructure.

5 Comparative study of various models of Cloud Security

There are various models of cloud security and these models have been put to exhaustive use. Table 1 specifies a Comparative study of these security models displays their strengths and also their shortcomings.

Table 1: Comparative study [13]

Models **Parameters**	**Multiple Tenancy model**	**Risk accumulation model**	**Jerico Formu's Cloud cube model**	**Multiclouds Database model**
Technology used	Virtualisation	Layer dependency of clouds	Four dimensional layers information like location, owner, security range and owner	Secret sharing of algorithm in use in multiple cloud services
Controls	User not in charge	User not in total control	User in partial control	User not in charge
Security	Medium	Medium	High	High
Malicious insiders	Less	More	More	Less

The above comparison reveals that a multicloud database model is more secure and agile, and it has very limited shortcomings compared to the others.

VI. IAM (IDENTITY AND ACCESS MANAGEMENT) SECURITY STANDARDS

While cloud offers multifarious capacities, its usage should also be user friendly and at the same time be secure. So Cloud computing should look for IAM capabilities that support:

• ***Federated Ids****:* In order to make access easier for the user, Ids are held directly either by the user or a trusted third party service provider. This enables the user to use the cloud without the need to establish additional user identities, every time.

• ***Single sign-on***: This concept is very similar to the federated Ids concept. Here users possess single ID and a single sign-on to use multiple data services almost across all the systems connected and also on multiple cloud service providers.

• ***Privileged Identity Management*****:** When it comes to the level of IAM at the cloud service providers end, their Administrators are safeguarding so much privileged and valuable information. Access to the consumers data has to be controlled at various levels in tune with the Administrators capabilities and work needs. A Common identity access management frameworks will not suffice to control privileged identities. Hence a specialized privileged identity management is to be put in place to prevent data breaches through the use of privileged accounts.

6.1 Standards and Technologies in IAM standard

Table 2 discusses about various technologies are adapted which provide federated IDs and single sign-on

Table 2: IAM Standard and Technologies. [14]

Protocol/Language	Standard	Services
LDAP(Lightweight Directory Access Protocol)	IETF	Authentication And Authorization
SAML2.0(Security Assertion Markup Language)	XML based OASIS	The exchange of authentication and authorization data between security domain
OAuth 2.0(Authorization framework)	IETF	Authorization flows for web applications, desktop applications, mobile phones, and intelligent devices, which can be used for cloud services
WS-Federation	OASIS standard	WS-Trust standard for the exchange of various tokens

OpenID Connect	API	Mobile Applications
SCIM(System for Cross-domain Identity Management)	IETF	Automation of user provisioning.
Active Directory Federated Services (ADFS2**)**	Microsoft	Single sign-on access to systems and applications located across organizational boundaries

VII. CONCLUSION

Data, in the modern world is being transferred across the globe for storage, processing, business needs. Such data includes valuable personal information, security data and monetary card information. Vast storage of redundant and old data is also taking place for use in data mining and to assess user preferences. In such a scenario, this paper has discussed the various threats to data in cloud infrastructure and the effect of various technologies in use. To conclude, we find that data stored and processed across multi cloud based environment in the hands of efficient Cloud service providers only can provide peace of mind to the user rather than using a single cloud service provider.

REFERENCES

[1]http://www.thesmallbusiness.org/software/benefits-of-cloudcomputing.html

[2]http://www.allthingscrm.com/cloudcoomputing/understanding-cloudcomputing-applications.html

[3] http://en.wikipedia.org/wiki/Cloud_computing

[4] http://www.wikinvest.com/concept/Cloud_Computing

[5]Cloud computing security challenges &solutions a survey https://ieeexplore.ieee.org/document/8301700/ by S Basu- 2018

[6]Cloudcomputing Trends to-prepare-for-in-2018

[7] C. Divya Shaly, R. Anbuselvi, " Multi-Cloud Data Hosting for Protection Optimizationand Security"-International Journal of Computer Science and MobileComputing. April 2016.

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

[9] Mark D. Ryan, "Cloud computing security: The Scientific challenge and aSurvey of solutions". Elsevier 02013.

[10] AlZain, M.A.; Soh, B.; Pardede, E. (2011). MCDB: Using Multi-clouds to Ensure Security in Cloud Computing. Dependable, Autonomic and SecureComputing (DASC). 2011 IEEE Ninth International Conference on , vol., no.,pp.784,791, 12-14.

[11] Chang, V.; Bacigalupo, D.; Wills, G.; De Roure, D. (2010). A Categorisation of Cloud Computing Business Models. Cluster, Cloud and Grid Computing (CCGrid). 2010 10th IEEE/ACM International Conference on , vol., no., pp.509,512, 17-20.

[12] AlZain, M.A.; Pardede, E.; Soh, B.; Thom, J.A. (2012). Cloud Computing Security: From Single to Multi-clouds. System Science (HICSS). 2012 45th Hawaii International Conference on, vol., no., pp.5490, 5499, 4-7.

[13] Barinder Kaur and Sandeep Sharma Parametric Analysis of Various Cloud Computing Security ,ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1499-1506

[14] Cloud standard security council, Cloud Security Standards: What to Expect & What to Negotiate Version 2.0

[15] Ahmed Albugmi,Madini O. Alassafi ,Robert Walters, Gary WillsConference: 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE,, At Luton, UK, Volume: 1

[16] Jeffrey Voas, Jia Zhang,"Cloud Computing: New Wine orJust a New Bottle?", IT Professional, Vol. 11, No. 2, pp. 15-17, Mar./Apr. 2009.

[17]Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres,Maik Lindner,"A Break in the Clouds: Towards a CloudDefinition", ACM SIGCOMM Computer CommunicationReview, 39(1), pp. 50-55, 2009

[18] Mao Wen-Bo (2009),"Cloud computing security, [Online] Available: http://blog.pconline.com.cn/article/334526. html,2010.

[19] Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues, "Towards Trusted Cloud Computing, [Online] Available: http://www.mpi-sws.org/~gummadi/papers/trusted_cloud. pdf,2010.

[20] http://www.nist.gov/itl/csd/cloud-102511.cfm

[21] http://thecloudtutorial.com/related.html

[22] http://thecloudtutorial.com/cloudtypes.html

[23] Learning about Cloud http://www.arcitura.com/

[24]VirtualizationVsCloudcomputing http://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html

[25]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.

[26]https://www.quickstart.com/blog/post/5-benefits-of-virtualization-in-a-cloud-environment/