Chief Editor

Dr. A. Singaraj, M.A., M.Phil., Ph.D.

Editor

Mrs.M.Josephin Immaculate Ruba

EDITORIAL ADVISORS

1. Prof. Dr.Said I.Shalaby, MD,Ph.D.
   Professor & Vice President
   Tropical Medicine,
   Hepatology & Gastroenterology, NRC,
   Academy of Scientific Research and Technology,
   Cairo, Egypt.
2. Dr. Mussie T. Tessema,
   Associate Professor,
   Department of Business Administration,
   Winona State University, MN,
   United States of America,
3. Dr. Mengsteab Tesfayohannes,
   Associate Professor,
   Department of Management,
   Sigmund Weis School of Business,
   Susquehanna University,
   Selinsgrove, PENN,
   United States of America,
4. Dr. Ahmed Sebihi
   Associate Professor
   Islamic Culture and Social Sciences (ICSS),
   Department of General Education (DGE),
   Gulf Medical University (GMU),
   UAE.
5. Dr. Anne Maduka,
   Assistant Professor,
   Department of Economics,
   Anambra State University,
   Igbariam Campus,
   Nigeria.
6. Dr. D.K. Awasthi, M.SC., Ph.D.
   Associate Professor
   Department of Chemistry,
   Sri J.N.P.G. College,
   Charbagh, Lucknow,
   Uttar Pradesh. India
7. Dr. Tirtharaj Bhoi, M.A, Ph.D,
   Assistant Professor,
   School of Social Science,
   University of Jammu,
   Jammu, Jammu & Kashmir, India.
8. Dr. Pradeep Kumar Choudhury,
   Assistant Professor,
   Institute for Studies in Industrial Development,
   An ICSSR Research Institute,
   New Delhi- 110070, India.
9. Dr. Gyanendra Awasthi, M.Sc., Ph.D., NET
   Associate Professor & HOD
   Department of Biochemistry,
   Dolphin (PG) Institute of Biomedical & Natural Sciences,
   Dehradun, Uttarakhand, India.
10. Dr. C. Satapathy,
    Director,
    Amity Humanity Foundation,
    Amity Business School, Bhubaneswar,
    Orissa, India.

ISSN (Online): 2455-7838
SJIF Impact Factor (2017): 5.705

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 3, Issue:10, October 2018

Published By :
EPRA Journals

CC License

BY NC ND

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 10 |October| 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

SECURITY ISSUES IN CLOUD ENVIRONMENT

Mir Abdul Samim Ansari
School of C&IT, Reva University, Bangalore, Karnataka, India

ABSTRACT

Cloud computing has provided software support for various systems from server to service provided. Many challenges for design and delivery of services over different requirements and environments. Growth of cloud computing provides various risks and challenges for system. Devices connected over internet are lead to threats and security risks. Cloud provided different level of abstraction to ensure risk and privacy. Cloud Computing is one in every of the biggest buzzwords in the computer world these days. It lets in useful resource sharing that consists of software, platform and infrastructure by virtualization. Virtualization is the center era behind cloud resource sharing.

Cloud vendors exit of their manner to ensure security. This paper addresses the challenges and security risk and analyze different measures to handle.

KEYWORDS:*Cloud Computing, Distributed Computing, Virtualization, Security*

1. INTRODUCTION

Cloud Computing means computing model which originated from distributed computing, virtualization technology, utility computing and further computer technologies. It is main source for services on virtual machines which is distributed over large physical pool of resources. Scalability and availability for large level of enterprise application. These can be a program for development and deployment of cloud applications. Platform as a service-(PaaS) hardware infrastructure, infrastructure as a service (IaaS) virtualized infrastructure.

Cloud Computing provides convenience, Ubiquitous and demand on network access to shared pool and definitions on computing resources which has efficiency to spread the provisionised and spreaded through fewer service provider interaction or management effort.

Cloud computing can be distributed into four types:

- Distribution Computing- Utility and Grid Computing
- Hardware- Hardware Virtualization Multicore Chips
- Internet Technologies- SOA, Web 2.0, Web Services and Mashups.
- System Management-Automic computing data center Automation.

Cloud computing applications are usually rated under subscription model. The cloud based services not only prohibited for Software applications.

Deployment Models	Essential Characteristics	Service model
Public	On Demand Service	SaaS
Private	Broad Network Access	PaaS
Hybrid	Resource Pooling Rapid Elasticity	IaaS
Community	Measured Services	

Table 1: overview of cloud computing

A) On Demand Self Service:

On demand self Service helps the operators achieve and configure cloud services

automatically; Consumer can provide provision computing capabilities to every service provider.

B) *Broad Network Access:*

Cloud resources and capabilities are provided over the network these are accessed through standard mechanism those are used by thick and thin client platforms, for example Laptops, mobiles, Workstations etc.

C) Resource Pooling:

The user can enter data into cloud from any location at any time. Computing Resources are pooled to help multiple consumers.

D) Rapid Elasticity:

Capabilities provided by cloud which can be elastically

rapidly released or provisioned. Cloud Computing creates

a dilemma of multiple computing resources. The resource

are rated up and down.

2. CLOUD SERVICE MODELS

Virtualized resources include storage, computation and communication. Cloud stack in the down layer such as Amazon EC2, Go Grid, Rack Space Cloud Servers.

a) Platform as a Service:

We can easily program cloud due to high level of abstraction. Platform as a service (PaaS).The users have such a place where they can deploy or develop any application without thinking about the memory and applications Ex: Google App Engine.

b) Software as a Service:

On top of the cloud stack the application falls for the last users there they get the access which are provided by the SaaS from web portals. Ex: Facebook, YouTube.

c) Infrastructure as a Service:

It is a Service that provides APIs to low level network infrastructure like data partitioning, scaling, security, backup etc.

3. CLOUD DEPLOYMENT MODELS

Private Cloud:

It is an internal data which is not for public. Single Organization with many consumers (Ex; Business Units). Private cloud is taken by a third Party.

Public cloud:

The cloud Infrastructure is for public use. The public cloud is operated by any government or business or academic organizations.

Community Cloud:

Cloud Infrastructure is shared to few organizations and able to support a particular community where they have same goals. It may be operated and managed by any organization of a third party Community

Hybrid Cloud:

It is the combination of one or more than two clouds.(Private ,public , Community). This cloud computing which increase the efficiency of control when it is from the public to enterprise cloud. They decreases the chance of errors. Private cloud maintain the security and their data privacy and compliance Quality of service (QoS). Private clouds have higher efficiency to maintain the network bandwidth and implement optimizations.

4. SECURITY CHALLENGES AND THREATS IN CLOUD COMPUTING

Clouds are used in many Applications like collaboration services, business implementations, Online Presence and R & D projects, social networks and business tool. In all this sites they have become most essential due to analysis, estimation, control cloud services gives consumers a hope where they do not face loss of data or theft of data.

Cloud Security:

The Cloud Security deals with all the information related to Security of data. In the Deployment Model they face challenges like copying and sharing of the data and unencrypted data and the identity management and the threats will be believing the data.

Service: In this Model they face challenge like storage and leakage of data and hacking and sharing the technology, the threats involved in service will be the misuse of the security.

The network Model have few challenges like lack of security and more of unnecessary data, and hacking of data. Most of the threats are these networks are hacked by many users due to this there may be huge loss of data.

The Application Model which has the challenges like hacking of many social applications such as Google here we lose the data privacy.

4.1 Information Security Principle

a) Integrity:

This refers to the quality of data. The data should not be remodeled by any user. The data should have its originality.

b) Confidentiality:

This word refers to protection of Particular data. It confirms to maintain the privacy of their data. When there is increase in various application there will be higher risk to access also.

c) Availability:

The Application Should be easy to use whenever it is necessary and for the proper authorized consumers to use at any moment.

5. CLOUD SECURITY REQUIREMENTS

Before even adding the cloud we should check few requirements this needs many requirements except security but for this we can easily trust the robust security.

Robust Security: The robust Security which helps in securing to data to an extend and also protects all the data which falls into this.

Trust and assurance: It maintains the confidence of the entire data and protects the cloud

infrastructure. It includes the hardware and software of all the data centers. It gives the consumers the trust and security about the data.

Monitoring and Governance: It helps the people to check their security environment and their sustainability of how they perform.

Cloud Security Controls:

1. Front End Security
2. Middle Layer
3. Back End Security

Front end security deals with security and process of certification.

6. SECURITY ARCHITECTURE

This Section has the confidential of data and the users from securing the data.

1) **Isolation:** It isolates the multiple data.
2) **Confidentiality:** This particular word describes the security of data from unauthorized access.
3) **Access control and Identity Management**: This can be accessed only by authorized users.

7. CONCLUSION

From so many researches and technology cloud data protection and accessing the cloud data is more used in IT field and for Security.

Cloud Computing security is considered as very Important and it should be added in cloud architecture to make sure security of information.

REFERENCES

1. *http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html.*
2. *Cisco White Paper, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/n s537/white_paper_c11-532553.html, published 2009, pp. 1-6.*
3. *John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.*
4. *George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2009, ISBN 9780596156367, pp. 2-4, 99-118.*
5. *http://en.wikipedia.org/wiki/Cloud_computing.*
6. *http://communication.howstuffworks.com/cloud*
7. *computing1.htm.*
8. *John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing," published on the IEEE Journal on Cloud Computing Security, July/August 2009, Vol. 7, No.4,61-64.*