CHALLENGES OF CLOUD COMPUTING, SECURITY ISSUES AND POTENTIAL OPERATIONAL AREAS IN DATA TRANSPORTABILITY, SEGREGATION, BACKUP, PORTABILITY AND RECOVERY

[1]**DR.D.ARIVAZHAGAN**
Professor,
Department of Information Technology,
AMET University, Chennai, India

[2]**S.SUNDARAM**
Assistant Professor,
Department of Information Technology,
AMET University, Chennai, India

Abstract: ***In Cloud computing virtualization plays a vital role. Now a days Cloud computing gaining more and more attention towards software concerns, individual users and in educational field because of its usage and on-demand access to a shared collection of resources across the network. IT enabled companies have experienced security issues for a decade. Because of security issues, some of the software companies are not familiar to adopt this technology. To facilitate its adoption these existing issues have to be fixed. Though many more countermeasures have been proposed by the scientists for addressing the security issues, still scope exist to model highly secured system. This paper outlines data security architecture, discusses security objectives, traditional and current security related issues and their counter measures.***

Keywords- Cloud Computing, Cloud Security Issues, Data Transportability, Data Segregation, Data backup, Data Portability, Data Recovery.

1. INTRODUCTION

Cloud computing is vastly persistence area that enables universal access to shared pools of configurable system resources, finest performance, quickly provisioned with nominal administration effort. In cloud computing, the data will be stored and retrieved from the database. Still many software concerns afraid to adopt this technology due to lack of privacy awareness. Cloud computing is a booming field due to its performance, availability, cost effective and many application systems [1]. The cloud model consists of five essential characteristics– resources pooling, broad network access, on-demand self-service, rapid elasticity, measured service , three service models – Infrastructure as a service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS); and four deployment models – private cloud, public cloud, hybrid cloud and community cloud [2]. This paper helps to concentrate to spot, identify and rectify the security issues faced in cloud technology. In this paper a detailed analysis of cloud characteristics, service models and deployment models are discussed [3]. The main drawbacks in cloud environment are privacy, content integrity and query of the outsourced information. The complete system is maintained by third party. Information misuse attacks are amplified if the hacker is service provider's accessibility and authorization only to controls aggravate this kind threat attack. Due to security concern, watermarks can be used. Suppose, the user wants to edit the original information then unable maintain privacy of content. For security issues, this paper suggests novel and effective approach to securing the cloud using decoy information technology [1].

2. CLOUD COMPUTING

Cloud computing is a computing prototype, where a huge amount of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, information and file storage. With the dawn of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly [4].

2.1 CLOUD ARCHITECTURE

Cloud computing architecture is the systems design of the software systems contained in the delivery of cloud computing which usually involves multiple cloud mechanisms collaborating with each other over a loose connector mechanism such as a messaging queue [5].

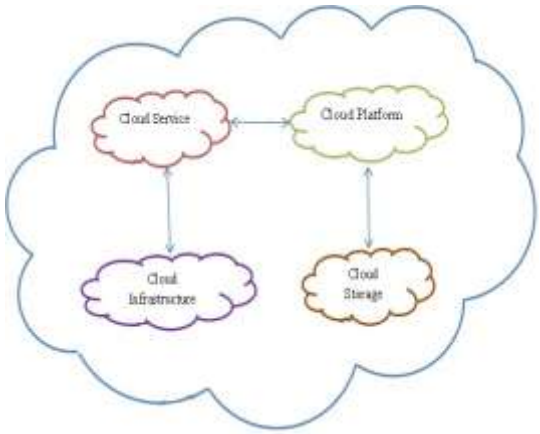

Figure 1: Cloud Architecture

2.2 CLOUD CHARACTERISTICS

On-demand self-service: Users are able to provision cloud computing resources without requiring human interaction, mostly done though a web-based self-service portal (management console).
Broad network access: Cloud computing resources are accessible over the network, supporting heterogeneous client platforms such as mobile devices and workstations.
Resource pooling: Service multiple customers from the same physical resources, by securely separating the resources on logical level.
Rapid elasticity: Resources are provisioned and released on-demand and/or automated based on triggers or parameters. This will make sure your application will have exactly the capacity it needs at any point of time.
Measured service: Resource usage are monitored, measured, and reported (billed) transparently based on utilization. In short, pay for use [6].

2.3 CLOUD SERVICE MODELS

Cloud Providers offer services that can be grouped into three categories.
Software as a Service (SaaS):
In this model, a complete application is offered to the client, as a service on demand. A single instance of the service runs on the cloud and multiple end users are serviced. On the client side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted and maintained.

Platform as a Service (PaaS):
A development environment is encapsulated and offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the providers infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of operating system and application servers.

Infrastructure as a Service (IaaS):
IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The client would typically deploy his own software on the infrastructure [4].

2.4 CLOUD DEPLOYMENT MODELS

The cloud deployment models mentioned below are based on the National Institute of Standards and Technologies. There are four basic cloud deployment models, which are:

Private cloud model
In this system, the cloud infrastructure is set up on the premise for the exclusive use of an organization and its customers. In terms of cost efficiency, this deployment model doesn't bring many benefits. However, many large enterprises choose it because of the security it offers.

Public cloud model
Public cloud is hosted on the premise of the service provider. The service provider than provides cloud services to all of its customers. This deployment is generally adopted by many small to mid-sized organizations for their non-core and some of their core functions.

Community cloud model
Community cloud model is a cloud infrastructure shared by a group of organizations of similar industries and backgrounds with similar requirements i.e. mission, security, compliance and IT policies. It may exist on or off premise and can be managed by a community of these organizations.

Hybrid cloud model

Hybrid cloud is a combination of two or more models, private cloud, public cloud or community cloud. Though these models maintain their separate entities they are amalgamated through a standard technology that enables the portability of data and applications [7].

3. SECURITY

Security is the toughest task in cloud computing. In a Cloud environment, answerability for employing and preserving efficient security methodology are up to the cloud providers. Cloud providers has the responsibility of users information. To maintain confidentiality among cloud users, cloud providers need to resolve all type of security issues. Cloud computing technology consists of hardware infrastructure in that virtual machines and virtual images deployed. Accessing and storing of information in the cloud are done through gateways. Bulk amount of information's are stored in the cloud data centre's. In cloud computing technology many data centre's are available. Processing of information from cloud to other networks is done by Network Operation Centre(NOC). Confidentiality, Integrity, Availability, Authenticity and Accountability are the five major security objectives of cloud computing technology [2].

4. CHALLENGES AND SOLUTIONS

The transferring of private and organizational data to the cloud environment access to share the data with the cloud provider. Due to a lack of established industry standards within the cloud computing environment, public clouds are commonly proprietary to various ranges. For cloud consumers that have custom-built solutions with needs on these proprietary environments, it can be challenging task to move from one cloud provider to another one [9].The main solution is to find the perfect cloud provider. Cloud IT security various from one cloud environment to another. Cloud provider should be well versed with cloud environment and adopt standard security rules and regulations. Contract between Cloud vendor and Cloud provider should be highly confidential and clear, so if any issues occur enterprise can claim the vendor. Efficient recovery tool should be used without loss any data by the cloud vendor. So if data loss or corrupted using recovery tool it can be easily recovered. For safer security efficient firewalls, servers, proxy servers, routers and high end software, operating systems should be used. This hardware and software setup will provide safe and secured environment from cyber-attacks. There should be a chart for flow of data so that it will be easy for the cloud programmers to have a clear knowledge about the users datas available in the cloud environment. [8]

5. CONCLUSION

Though lot of potential gains in cloud environment, there are some limitations and security issues [2]. Security is one of the most vital issue in cloud computing. Most of the security issues and their solutions are elaborately discussed in this paper. Novel security techniques are the accurate one to adopt by all IT concerns for safer and confidential cloud technology in future.

REFERENCES

[1] Rama Krishnan and V.Mathivanan, " Content Based Security Policy in Cloud Environment", International Journal of Applied Engineering Research, *ISSN 0973-4562, Volume 10, Number 14 (2015) pp 34658 – 34663, http://www.ripublication.com*

[2] M.N.Birje, P.S.Challagidad, M.T.Tapale, R.H.Goudar, "Security Issues and Countermeasures in Cloud Computing", International Journal of Applied Engineering Research, *ISSN 0973-4562 Vol.10 No.86 (2015), http://www.ripublication.com*

[3] Rama Krishnan and V.Mathivanan, " An Criticism of Contemporary Cloud computing Productions and Encoventers ",International Journal of Computer Engineering and Technology, *ISSN 0976-6367, Volume 6, Issue 8, Aug 2015, pp.41 – 50*

[4] Cloud Computing – An Overview – Torry Harris

[5 https://www.conceptdraw.com/How-To-Guide/cloud-computing-architecture-diagrams

[6]https://www.ibm.com/blogs/cloud-computing/2014/01/31/cloud-computing-defined-characteristics-service-levels/

[7]https://www.rishabhsoft.com/blog/basics-of-cloud-computing-deployment-and-service-models

[8] Pradeep Kumar Tiwari, Bharat Mishra – "Cloud Computing Security Issues, Challenges and Solution", International Journal of Emerging Technology and Advanced Engineering, *ISSN 2250-2459, Volume 2, Issue 8, August 2012*

[9] Usman Namadi Inuwa, "The Risk and Challenges of Cloud Computing", Usman NAmadi Inuwa International Journal of Engineering Research and Applications, *ISSN: 2248-9622, Vol.5, Issue 12, (Part – 14) December 2015.*