AN ANALYSIS ON SECURITY ISSUES IN CLOUD COMPUTING

Vandana[1], Arti Mishra[2], Meenakshi Pathak[3], Shikha Arya[4]

[1,2,3,4]*Assistant Professor, Computer Science, SRMSWCET, Bareilly, (India)*

ABSTRACT

Cloud computing is an internet-dependent technology and an emerging area that affects IT infrastructure. This technology provides a platform where resources, software and information are provided to user's on-demand. The main objective of cloud computing is to make a perfect internet-based system with powerful computing capability to the users of internet. Cloud computing is also known as utility computing that enables convenient, on-demand network access to a shared computing resources such as networks, servers, storage, applications, services and information that can be easily shared and utilized on cloud with minimum management efforts . The main challenge of cloud computing is to provide a secure-shareable and secure-utility system. Security requirements in cloud computing is very much different from traditional environments. It has many issues related to the security area, since cloud has a dynamic nature, global environment and easy sharing of resources. This paper introduces the detailed analysis on the security issues of cloud computing. It investigates the security issues in layered- architecture of cloud. Each cloud architecture layer has different security issues. Each security issue can be solved at individual layer with minimum efforts to provide a secure and powerful system on cloud.

Keywords: Cloud Computing, Internet, Layered-Architecture And Security Threats.

I. INTRODUCTION

Cloud computing is a merger of known technologies and utilizes internet as a service deliverable network. It provides a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Cloud computing is so named because the resources being accessed is found in the clouds and does not require a user to be in a specific place to gain access to it. The word cloud is a familiar, but when combined with computing, the meaning gets bigger and complex. The real cloud is commonly used in science to describe a large group of objects that visually appear from a distance as a cloud, a visible collection of particles of water. While the technical cloud is an area or space in internet that is utilized and provided by virtual servers on the internet. The functional origin of technical cloud is also taken from the real cloud. As real clouds carry water from one place to another place, similarly the technical clouds provides resources by taking required architecture or space from multiple virtual servers on the internet. The distributed nature of cloud is the key point of security in cloud and also gives the chance to malicious activities to be carried out very easily because of the global environment and easy accessibility.

II. LAYERED – ARCHITECTURE OF CLOUD COMPUTING AND SECURITY ISSUES

The layered -architecture provides the easy and clear working view of the any system. There are numerous security issues for cloud computing as it encompasses many technologies including database, operating systems, network , virtualization, resource scheduling, load balancing, transaction management, concurrency control and memory management. Therefore security issues for many of these systems and technologies are applicable to cloud computing. The cloud environment consists five layers.

These layers are:

1. Client Layer
2. Application Layer
3. Platform Layer
4. Infrastructure Layer
5. Server Layer

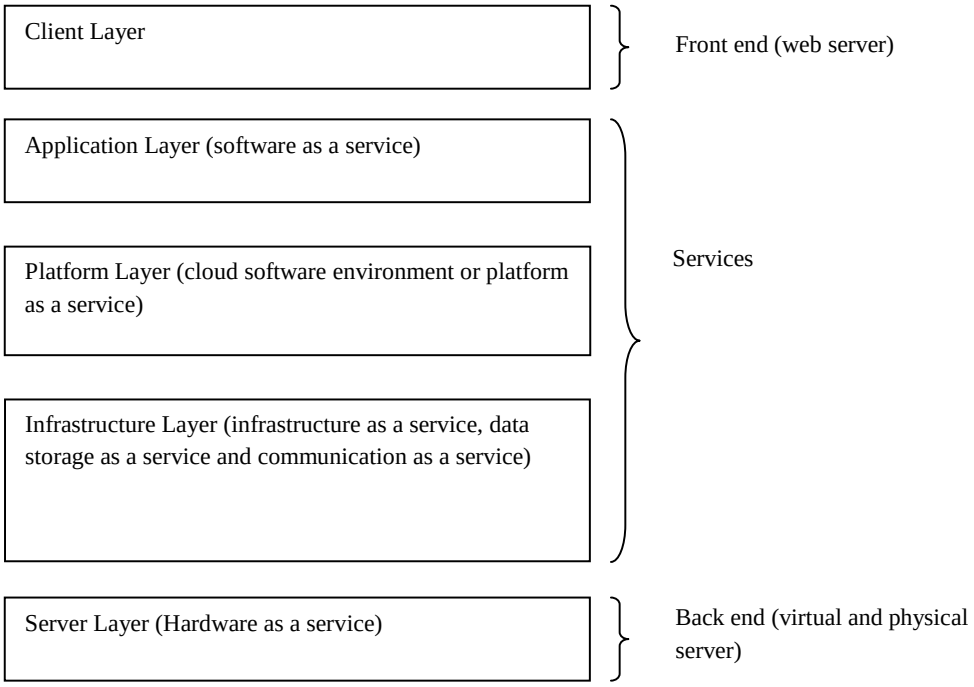

Fig1. Five Layers of Cloud Infrastructure

2.1 Client Cloud Layer

This layer is the most visible layer to the users of the cloud infrastructure. The user uses the services provided by this layer, sometimes user has to pay for the services.

2.1.1 Security Issues of Client Layer The biggest security issues of this layer are selection of sources, as there are many sources available in the cloud that contains multiple resources. It is difficult to identify the accurate and correct resource on the internet. This difficulty arises the problem of legal ownership of the data. The second issue is related to the availability of data on the cloud. As all the services is provided by virtual server and their working is depended on the proper connection of different devices and the service provider. The service provider has the authority of removing information on the internet, so it might be possible that the

required information and services is not available at that time. The concept of authorization is also key issue due to the public nature of the cloud because we cannot trust anything that cloud contains. The content of clouds can easily be modified so we need some security for preventing easy access of the resources.

2.2 Cloud Application Layer

This layer is also known as environment layer. This layer delivers software over the internet and eliminating the needs to install and run the application on customer's own computers. This layer is based on service as a software model and provides services on demand such as email, software and business applications.

2.2.1 Security Issues of Application Layer: With cloud application layer most of the security issues lie with the cloud provider because of the degree of the abstraction and minimal customer control. There are many security issues of application layer as: application security, internet threats, data protection and data backup issues, availability of application and identity issues of application.

2.3. Cloud Platform Layer

This layer provides fundamental and required resources to other highest layers (client and application layer). The user of this layer are cloud application developer, implementing their application for users on the cloud. It provides a platform where the application is written and consumes the cloud resources. This layer is also known as cloud software environment. The layer offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction.

2.3.1 Security Issues of Cloud Platform Layer: This layer is responsible for securing the platform software that includes the run time engine that executes the customer's applications. There are many security issues are as inherit security issues of data and network because this layer combines more than one source element into a single integrated unit that is third party relationships. The security issue is data legal issues as data may be stored on different places with different legal regimes that can compromise its privacy and security. This layer works on PaaS model that offers development tools to create SaaS applications, so application and user's data are also stored in cloud servers which can be security concern and the security of the data while it is being processed, transferred and stored depends on the provider's. Destruction or alteration of configuration information, and physical destruction or alteration of network components and hacking, network security and interconnection complexity issues [1] are other security issues of the platform layer.

2.4 Cloud Infrastructure Layer

This cloud layer provides basic software management for the physical server, computing resources (IaaS), data storage (DaaS) and communication (CaaS) that compose the cloud. Software kernel can be implemented as operating system kernel and virtual machine monitor. It provides a platform virtualization environment. This layer provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet.

2.4.1 Security Issues of Infrastructure Layer: This layer has better control and management compared to the other layers. It control the execution of the application running in their virtual machines and responsible to configure security polices correctly. The underlying compute, network, and storage infrastructure is controlled by cloud providers. Cloud provider consider a required effort to secure their systems in order to minimize threats that results from creation , communication , monitoring, modification and mobility[1]. Security of

virtualized environment is very important consideration in this layer because the environment is vulnerable to all types of attacks. Virtual machine monitoring, sharing of resources, roll baking and virtual machine connectivity are the main security consideration of this layer.

2.5 Cloud Server Layer

This layer provides the actual physical hardware. The user of this layer is big enterprises with huge IT component requirement in need if rented hardware as a service [2]. This layer is also known as server layer.

2.5.1 Security Issues of Server Layer: The cloud server security depends on both the physical and technical security issues, backed up by security policies, procedures and well -trained staff. The data center of a cloud provider is a central repository for valuable data resources and thus an attractive target for malicious hackers. So it is important to consider the physical security of a cloud provider's data centers. These security issues include security policy breach, monitoring issues, data security, physical devices security issues and authorization issues.

Table1. Security Issues of Cloud Layers

S.No	Cloud Layer	Security Issues
1.	Client Layer	Selection of sources
		Ownership of data
		Availability of services
		Authorization and identification issues
		Integrity of data
		Accessibility issues
2.	Application Layer	Application security
		Internet security
		Data protection
		Data backup issues
		Availability of application
		Insecure Interfaces and APIs
		Insecure cloud service for user access
		Identity issues of application[3]
3.	Platform Layer	Network threats
		Data legal issues
		Destruction of configuration information
		Physical destruction
		Hacking
		Alteration of network components
		Interconnection complexity issue
4.	Infrastructure Layer	Virtual machine monitoring
		Resource sharing

		Roll backing
		Virtual machine connectivity
		Configuration issues
5.	Server Layer	Security policies breach
		Virtual machine attacks
		Physical security
		Data security (integrity. confidentiality)
		Monitoring issues
		Authorization
		Incident and disaster recovery
		Easy modification in central repository
		Technical security issues

III. CONCLUSION

Security is a key issue in technology. There are many fields of security as assurance, countermeasures, risk, threats, vulnerability and exploit. If these security areas are analyzed or considered at the time of development, deployment and utilization then the performance of any computing technology can be increased or maximized. This paper is based on the analysis of security issues of the cloud computing so that these issues can be prevented and protected to increase the user's satisfaction. Users confidence can be achieved by providing them a safe and secure environment, which is a crucial issue in cloud computing. This analysis will help us to provide a secure management at the various layers of cloud.

REFERENCES

[1] An analysis of security issues for Cloud Computing by Keilko Hashizume, David G Rosado, Eduardo Fernandez-Medina and Eduardo B Fernandez

[2] Cloud Computing – A Five Layer Model February 3, 2009 by Brian Wolff

[3] Study of Security Issues in Various Layers in Cloud Computing by Divya Rastogi, Nikunj Kumar, Prof.(Dr.) Abhay Bansal

[4] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, and Sagata Sanyal published, "A survey on Security Issues in Cloud Computing in Cornell University, May 2013.

[5] Nidhi Jain Kansal, Inderveer Chana, published ," Cloud Load balancing techniques: A step towards green computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012.

[6] Prashant Rawagd, Yogita Pawar published, " Security Threats –Main Hindrance to the Wide Acceptance of Cloud Computing Service", International Conference in Recent Trends in Information Technology and Computer Science(ICRTITCS)-2012(0975-8887).