Cloud Computing Security Issue and Its Proposed Solution

Rajni Kumari , M.Tech Research Scholar
Center of Cloud Infrastructure and Security
Suresh Gyan Vihar University
Jaipur , Rajasthan.
E-mail-: rmanushendra@gmail.com

Dr. Manish Sharma , HOD
Center of Cloud Infrastructure and Security
Suresh Gyan Vihar University
Jaipur, Rajasthan.
E-mail-:manish.sharma@mygyanvihar.com.

Dr. Rashid Hussian, Associate Prof.,
Suresh Gyan Vihar University
Jaipur, Rajasthan.
E-mail-: rashid.hussian@mygyanvihar.com.

Abstract
In Recent time, cloud computing drastically changes the view of IT infrastructure such as hard-disk, RAM, Software and storage etc. and also perception of everyone. Amazon ,IBM,Google's Application, Microsoft Azure etc., are the provider of cloud service provider that provide the developing applications for user in cloud environment and to access them from anywhere ,any time. Cloud computing includes elements from parallel computing, utility computing, fog computing and grid computing and into an innovative deployment architecture in the virtual environment. The main purpose of this paper is identifying the issue of cloud data storage and its solution.

Keywords: **Cloud Computing, cloud storage and cloud security.**

1. INTRODUCTION

CLOUD COMPUTING: SECURITY -ISSUES

1.1 CLOUD SERVICES

There are different service model is offered by cloud: Software as a Service, Infrastructure as a Service and Platform as a Service respectively also known as SaaS, IaaS and PaaS. All of them have also different types of deployment models, making it important to understand that system of cloud computing is change. The main security concerns, however, keep on the same.

In addition to, with data storage security issues, the moving data over networks is also included by cloud service. The level of network security is required for it and file transfer encryption. The service user and the service provider have responsibility for this. The reliable and trustworthy networks is only chosen by user and use sufficiently secure password and username credentials. The service encryption must be assured by service provider and server-end security for the stored information.

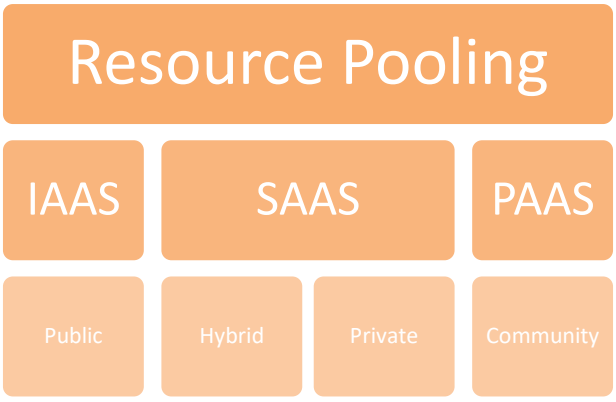

Fig.1 Cloud Computing Model

1.2 KEY SECURITY ISSUES IN CLOUD COMPUTING

Applications, platforms and infrastructure segments are consist in cloud computing. Different products for businesses and individuals around the world have different offer by each segment. Software as a Service (SaaS), Utility Computing, Web Services,

Platform as a Service (PaaS), Service Commerce and Internet Integration are included by business application. Security issues for cloud computing is various are:

- Machine Security
- Virtual Data Transmission
- Access to Servers & Applications
- Network Security
- Data Integrity
- Data Segregation
- Patch management
- Data Privacy
- Data Security
- Data Availability
- Security Policy and Compliance

1.3 VIRTUAL MACHINE SECURITY:

One of the major components of a cloud is Virtualization. It is dynamic i.e. to previous instances, paused and restarted could be lapsed, comparatively easily. Ensuring that on the same physical machine different instances are running and remote from each other is a major task of virtualization. It can also be readily cloned and easily moved between physical servers. VM collapse makes it difficult to achieve and maintain reliable security by this dynamic nature and potential. Vulnerabilities that are found errors may be unintentionally propagated. Also, to maintain an auditable record is difficult of the security state at any given point of a virtual machine in time. There are two type of virtualization, one of them is full Virtualization and other is Para Virtualization in a cloud computing environment.

Complete hardware architecture of computer is replicated virtually in the full virtualization. However, an operating system is modified so that it can be run parallel in para-virtualization with other operating systems. Abstracts the physical resources is abstracted by VMM (Virtual Machine Monitor) that is a software layer used by the numerous virtual machines. A virtual processor and other virtualized versions of system devices like I/O devices, storage, memory, etc are provided by VMM. In all popular VMMs many vulnerability are found that allow avoidance from Virtual machine. It could allow a guest operating system user to execute code on the host or another guest operating system by Vulnerability in Microsoft Virtual PC and Microsoft Virtual Server. It is find that vulnerability in VMware's shared folders mechanism that grants users of a guest system read and writes access to any part of the host's file system including the system folder and other security-sensitive files. Vulnerability in Metasploitable can be broken by users of a guest domain to execute arbitrary commands. On host and guest operating systems is the other issue is the run of administrator. Current perfect isolation is not offered by VMM.

We have taken virtual box of oracle and create a virtual machine of metasploitable and it is easily accessible by root user.

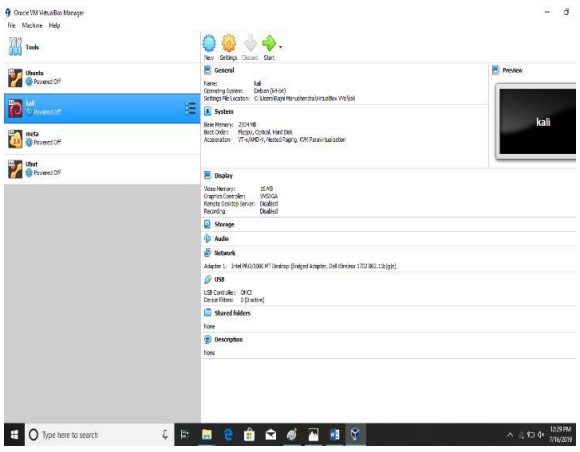

Fig 2: Virtual Box

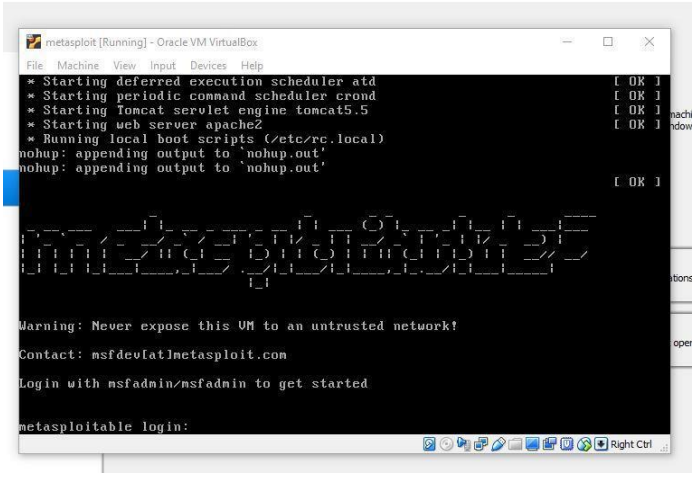

Fig 3: Virtual Machine

1.4 DATA SECURITY:

The service of cloud computing that offer for user is easy to find possible storage. Hypertext Transfer Protocol (HTTP) is communication protocol that is used to achieve the service of cloud computing. Data integrity and information security are assured by it, the most common adoption are Hypertext Transfer Protocol. Secure (HTTPS) and Secure Shell (SSH). In a traditional on evidence application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, the enterprise data is stored outside the enterprise boundary, at the Service provider end in cloud computing. So, the service provider must adopt additional security checks to ensure data security and prevent holes due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party.

SOLUTIONS TO DATA SECURITY ISSUE

To secure information it is better solution to encryption. It is better to encrypt data before storing data in cloud server. Permission can be given by data owner to particular group member such that data can be easily accessed. Data access control is provided by data centric security. To improve the data security over cloud is design data security model that include data encryption, data integrity and authentication. Data protection can be used as a service for ensuring privacy. Applying encryption on data to avoid access of data from other users. Before uploading data into the cloud the users are recommended to verify whether the data is stored on backup drives and the keywords in files remain unchanged. The hash of the file is calculated before uploading to cloud servers will ensure that the data is not changed. It can be used for data integrity but it is very difficult to maintain it. To combining identity based cryptography and RSA Signature can be provided to check by RSA based data integrity. Both at the physical level and application level to keep apart data from different users and must be clear boundaries that ensure by SaaS. In cloud computing, distributed access control architecture can be used for access management.

Reference

[1]. Data Security Challenges and Its Solutions in Cloud Computing R. Velumadhava Raoa,*, K. Selvamanib,* *aDepartment of Computer Science & Engineering, RIT, Chennai,indi bDepartment of Computer Science & Engineering, Anna University, Chennai, India*

[2]. Future Generation Computer Systems Addressing cloud computing security issues Dimitrios Zissis ∗, Dimitrios Lekkas Department of Product and Systems Design Engineering, University of the Aegean, Syros 84100, Greece

[3]. State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions
Farrukh Shahzada *aKing Fahd University of Petroleum and Minerals, Dhahran, KSA*

[4]. A Study on Data Storage Security Issues in Cloud Computing Naresh vurukonda1, B.Thirumala Rao2 1,2Department of CSE, KLUniversity, Vijayawada, A.P, INDIA 1 naresh.vurukonda@gamil.com, 2 drbtrao@kluniversity.in

[5]. "Security Guidance for Critical Areas of Focus in Cloud computing", April 2009, presented by Cloud Security Alliance (CSA).

[6]. Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 20l3 l0.5l2l/ijnsa.20l3.5502 ll.

[7]. Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," CloudComputing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. l, No.2, December 20l1.