Cloud Computing Security Challenges

Mr. Bhushan Talekar, Miss Sonali Chaudhari, Mr. Balmukund Dubey
Computer Engineering, Computer Engineering, Computer Engineering
Mumbai University, Mumbai University, Mumbai University
Mumbai India, Mumbai India, Mumbai India
Bhushi.27@gmail.com
sonali27891@gmail.com
balmukunddubey1989@gmail.com

Abstract- **Cloud computing has generated a lot of interest in the industry and it is recognize as one of the top 10 technologies [1]. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care & government. This paper analyzes different types of clouds and the security challenges that. Cloud security is becoming a key differentiator and competitive edge between cloud providers. This paper focuses the security issues arising in different type of clouds.**

Keywords— **Cloud, Security, Security challenges, Cloud computing**

I. INTRODUCTION

Cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. [1] Cloud computing allows consumers to access resources online through the internet.Cloud computing is independent and is totally different from grid and utility computing. Cloud computing is cheaper than other computing models; zero maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines. Due to this feature, cloud computing is also known as utility computing, or IT on demand.The diagram shows the three distinct categories within Cloud Computing:

I. Software as a Service,
II. Platform as a Service and
III. Infrastructure as a Service. [2]

Fig.1 Cloud computing stack

SaaS -applications are delivered over the web, for end-users.
PaaS -is the set of tools to make coding and deploying those applications quick and efficient.
IaaS -is the hardware and software that powers it all – servers, storage, networks, operating systems.[2]

II. VARIOUS TYPES OF CLOUDS

Clouds are broadly classified as:

A. *Personal clouds*: Such clouds are especially operated by single organization or single institute provide a broad range of office and enterprise computing services. It supports the applications for online collaboration, email and calendaring such as ERP software. Conventional approaches to computing have constraint our ability to meet the needs. Personal clouds provide a new architecture for improving efficiency. It includes a hosting platform, interfacing unit and infrastructure services.[6]

B. *General clouds:* These clouds are providing services to common people. A general cloud in which a service provider makes resources such as applications and storage is available to the general public over the internet. General cloud services are

Scalability to meet needs and economic for general public. [6]

C. *Domain-specific clouds:* These clouds are maintained for specific requirements by a group of organizations. [6]

D. *Mixed clouds or hybrid cloud:* These clouds are combination of above said three clouds which can share data to achieve fulfill a specific requirement. A hybrid cloud is mostly a combination of at least one private cloud and at least one general cloud. Mainly provides scalability and cost effectiveness.[6]

III. CLOUDS SECURITY CHALLENGES

A. *Personal Cloud Security Challenges]*

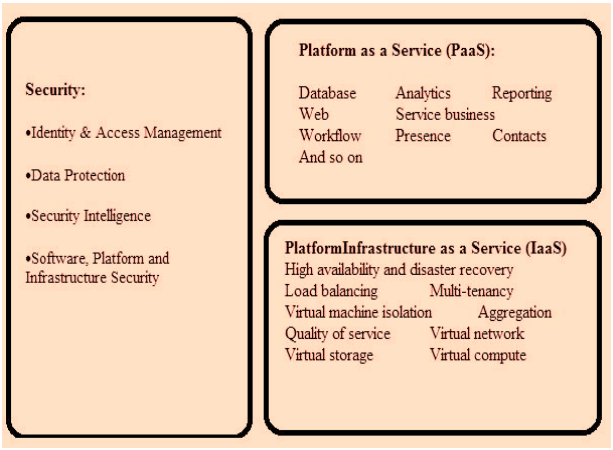

Fig. 2 Personal Cloud Security challenges.

1) *Identify & Access Management :*
Managing identities and access control for enterprise applications remains one of the greatest challenges in personal cloud. Identify & access management mainly contains the identity provisioning, authentication, federation, authorization and user profile management.

2) *Data Protection:*
Protection of data from the unauthorized site is the issue face by personal cloud. The data protection issues are the same, whatever version of the cloud a data controller wishes to us. The key issue is the security of the data. The second issue is the location of the data

3) *Security Intelligence :*
Personal cloud face many security issues related to the cloud adopters, regardless of their infrastructure of choice one of the biggest issues facing Cloud users is data residency.

4) *Software Platform And Infrastructure Security*
Cloud Infrastructure related with both hardware and software. The platform security is deal with database, report, web, contacts and so on. Where Infrastructure Security deal with load balancing, multi tendency, Virtual machine isolation and so on

B. *General Cloud Security Challenges:*

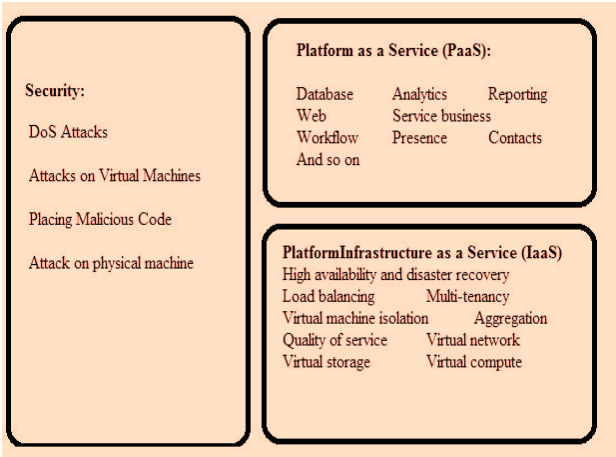

Fig. 3 General Cloud Security challenges.

1) *DoS Attack:*
Denial of service means making the resources unavailable for the users. Usually this type of attack temporarily or infinitely stops a service of the host. This will be shown in figure5.In the cloud system the hacker attack on the server by simply sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly.[4]

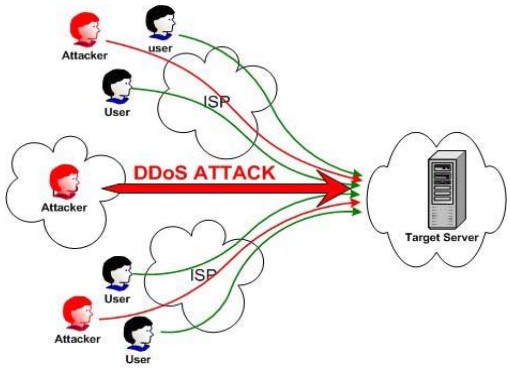

Fig 4. DoS attack [1]

2) *Attack On Virtual Machine:*
Virtual Machine (VM) escape is an exploit in which the attacker runs code on a VM to gain access on the host operating systems. It is considered to be the most serious threat to virtual machine security.[4]

3) *Placing Malicious Code:*
Malicious code is code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content. Malicious code is used in general cloud to unauthorized access or to crack the system.

4) *Attack On Physical Machine:*
Attack on Physical machine lead to the attack on the electronic devices such as computer, mobile devices, PDAs, Laptops etc.[5]

C. Domain Specific Cloud Security Challenges::

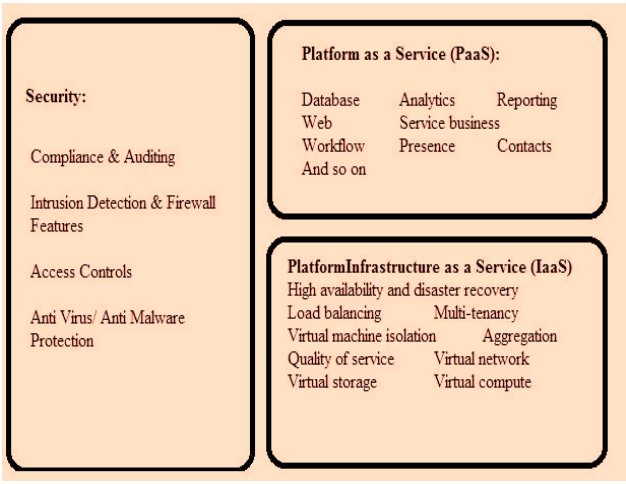

Fig.5 Domain Specific Cloud Security Challenges*:*

1) *Compliance & Auditing:*
Cloud providers have to make sure that the customer's data won't be disclose by any organization even when they left the organization.[1]

2) *Intrusion Detection & Firewall:*
Intrusion Detection & Firewall is required to protect data but sometimes it not apply on every model of cloud therefore it is access by third party

3) *Access Controls:*
Domain Specific Cloud is collection of various groups so there is always issue of access control. Access control is deal with to who give access and for what purpose.

4) *Anti Virus/ Anti Malware Protection:*
Domain Specific Cloud is collection of various groups so if any group is not protected from Anti Virus or Anti Malware Protection then the attacker can easily access the confidential data.

D. Hybrid Cloud Security Challenges::

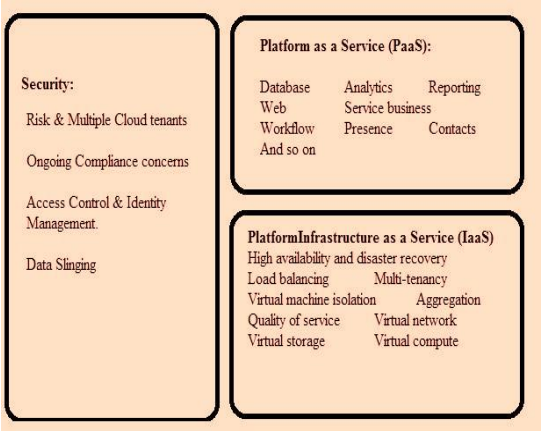

Fig 6 . Hybrid Cloud Security Challenges

1) *Risk & Multiple Cloud tenants:*
Hybrid Cloud or mix cloud is the combination of multiple various types clouds therefore t is difficult to manage and the risk of attacker is more

2) *Ongoing Compliance Concerns:*
Cloud required to keep the track of all organization work with them and who was left.

3) *Access Control $ Identity Management:*
Is the main issue in hybrid cloud because multiple cloud work under same cloud so it is difficult to provide access to particular organization.

4) *Data Slinging:*
It refers to the data loading and cleaning process. Also contain all information about data migration.

IV. CONCLUSIONS

Cloud computing offers great potential to improve productivity and reduces costs. It also poses many new security risks**.** In this paper much of the work has been focused on types of clouds and their security challenges. .

ACKNOWLEDGMENT

Thanks to Prof. Harshada Nemade for providing excellent guidance, encouragement and inspiration throughout the paper work. Without her invaluable guidance, this work would never have been a successful one. Due to the complexity of cloud system, it is very difficult to achieve security. New security techniques need to be developed and older security techniques needed to be radically twisted to be able to work with the clouds architecture

REFERENCES

1. RohitBhaduria,SugataSugal, "Survey on Security Issues in Cloud Computing andAssociated Mitigation Techniques" ,*InternationalJournal of computer applications*, Vol: 47,No:18,June 2012, pp:47-66

2. UNDERSTANDING The Cloud Computing Stack SaaS, Paas, IaaS, © Diversity Limited, 2011 Non-commercial reuse with attribution permitted.

3. Laura Smith on " A health care community cloud takes shape" http://searchcio.techtarget.com/news/2240026119/a-health-care-community-cloud-takes-shape

4. Ulrich Rührmair, Frank Sehnke, Jan Sölter Modeling Attacks on Physical Unclonable Functions

5. K.l.neela, Dr.v.kavitha. "A Survey on Security Issues andVulnerabilities on Cloud Computing". *ISSN : 2229-3345 Vol. 4 No. 07 Jul 2013*

6. Maneesha Sharma, Himani Bansal, Amit Kumar Sharma., "Cloud Computing: Different Approach & Security Challenge" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012

