Chapter 79
Recent Trends in Cloud Computing Security Issues and Their Mitigation

G. M. Siddesh
M. S. Ramaiah Institute of Technology, India

K. G. Srinivasa
M. S. Ramaiah Institute of Technology, India

L. Tejaswini
M. S. Ramaiah Institute of Technology, India

ABSTRACT

Security in cloud is to be increased to strengthen the confidence and trust of cloud service consumers. In the upcoming years, the scientific research and education teams will have to investigate finding new ways to handle the issue of cloud security. This chapter discusses the major threats and their impact on clouds, security measures to handle the attacks in clouds, security as a service in research and education, and steps to enhance security feature in clouds.

1. INTRODUCTION

These days cloud seems to be in every bodies mind and everyone are starting to tend towards cloud computing, now the question that arises is, how secure is cloud computing and what are the advantages and disadvantages of cloud computing. Hence people have started to scratch their heads on scientific ways on how to provide security to the cloud which will make life simpler and easier. As though using cloud computing will surely bring down cost of infrastructure and will also make feel that the business is at ease, but still the major concerns which is cribbing everyone's mind is that, since security is the major threat, so what all steps need to be taken to implement cloud technologies in their companies. Some of the challenges that we face as of today is, when cloud technology is implemented the threats like data loss, infrastructure and compliance issues might arise and what way will they have an impact on the organizations matters a lot (Behl & Behl, 2012).

DOI: 10.4018/978-1-5225-5634-3.ch079

To secure the data, new technologies and different kinds of researches, study and approaches are needed. We need to create Polices, technologies and a set of newly designed controls to protect the clients, data and infrastructure from attacks. For this the researchers have found a best way to secure data that is to create a technology that is layered, since we know that security will be more effective when we stack each of the layers. Cloud technology comes in different types of delivery system that is Private, Public and Hybrid. Security must be provided at both the ends that are at the provider's level as well as the consumer level. Cloud computing has become the hottest topic for research, study, considerations and suggestions that is regarding protecting hardware and platform technologies in the data center to enable regulatory compliances and controlling cloud assess at different end points (Liu, 2012).

2. MAJOR FACTORS THAT IMPACT CLOUD SECURITY

Some of the major factors that have an impact on Cloud security are listed below:

- **Attackers and Threats:** Beware, cybercrime is on the rise. Hackers not only create threats but also are targeting attacks on software and platform technologies for their personal gains.
- **IT Consumerized:** Since the IT sector is consumerized, employees tend to use their personally owned devices such as mobiles and laptops to access applications, data and cloud services. This might make a dent on the security system.
- **Architectural Technologies:** With virtualization growth and use of public cloud perimeter and their controls within the data center are no longer easily constrained or physically isolated nor protected.
- **Dynamic and Challenging Regulatory Environment:** Since organization face a lot of burden of legal and regulatory compliance which are prescriptive demands and face very high penalties for non-compliances and breaches.

2.1 Major Threats to Cloud Computing

Abuse and Nefarious, insider's threat, interfaces and their API's, technologies that are being shared, loss of data and services hijacking are some of the factors affecting Cloud computing which are explained below (Green, 2013; Bouayad, Blilat, Mejhed & Ghazi, 2012).

- **Abuse and Nefarious:** Here two models of services are being used IAAS and PAAS. While both the service providers deliver unlimited network and storage capabilities, wherein anyone with a credit card can easily register and start using the cloud services. Because of this hackers are able to do their works by creating treats and attacks with ease. The areas of concerns are password, DDOS, launching dynamic attacks, malicious data. These providers have become an easy prey for hackers, since with the use of latest technologies the hackers are not detectable and the fraudulent activities are increasing. To avoid this, registration process should be stricter and credit card fraud monitoring system must be implemented.
- **Insider's Threat:** The insider's threat is commonly faced problems in any companies. The IT services and the customers are converged under a single domain. Because of this there is no transparency between the provider, process and the procedures. Since the cloud service providers will