CHAPTER 3

PROBLEM STATEMENT

This problem is explained from Cloud Service Provider perspective, because the problems to the virtual machines raises at Cloud service providers site and it may affect both cloud service providers as well as cloud service users.

Most of the existing approaches does not satisfy requirements of virtualization environments, means that most of them are to identify the problems not for healing, some of them to tolerate the problems to some extent not for to overcome out of it.

Some of the Existing approaches are:

1. “A Virtualization Intrusion Tolerance based system” is proposed by Yuesheng Tan, Dengliang Luo and Jingyu Wang, which is mainly concentrates on how to withstand even in the case when virtual environment is affected by malwares, threats or intrusions. That too it is up to some extent, after that the environment may collapse.

2. “A Security monitoring appliance for virtual machines in IaaS cloud model” is proposed by Amani S Ibrahim, James Hamlyn-Harris, John Grundy and Mohamed Almorsy, whose main intention is to just monitor the environment for identifying the problems, especially in case of one of the cloud service models ie., Infrastructure as a service. It will not fulfill the need of all service models and deployment models.

3. “A Multilevel security model for virtualization” is proposed by Hui Zhu, Yingfang Xue, Xiaofeng Chen, Hui Li and Ximeng Liu, whose main intention is to avoid the problems of virtualization environment which are faced by some organizations and IT companies in China. This approach mainly concentrates on the problems of those particular organizations and IT companies. They won’t reflect the problems of all situations and models.

4. “Secure virtualization for cloud environment using Hypervisor based technology” is proposed by Farzad Sabahi, mainly concentrates on introducing the security measure only at hypervisor layer. It won’t targets the problems of virtual machines
which are infected who interact with hypervisor. The system removes the problems of hypervisor not virtual machines.

5. “Checking running and dormant virtual machines for the necessity of security updates in cloud environments” is proposed by Roland Schwarzkopf, Matthias Schmidt, Christian Strack and Bernd Freisleben mainly concentrates on infected virtual machines which behaves abnormally. This system just checks whether they are normal or dormant and look for security updates in the environment. This system will not target the problems of Hypervisor and also the interactions between Hypervisor and virtual machines.

In our system all these problems are considered and concentrate to identify and heal the virtual machines environment in all type of cloud models and situations.

When the virtual resources are formed out of available actual physical resources, those virtual resources may face the problems from intruders, malwares or sometimes the virtual machines themselves corrupted and in turn they trouble the other virtual machines, and also make those virtual machines to consume more resources like processing power, memory and bandwidth etc. than they actually required. Sometimes the virtual machines may get troubled in such a way that, they cannot do any processing based on user requirements. In some cases, the virtual machines may behave in such a way that, they try to access the resources such as Computing power, RAM etc., allocated to other virtual machines and trouble them. In some instances the misbehaving virtual machines may try to corrupt the data or operating systems of other virtual machines. The currently available security mechanisms may not fulfill the needs of security of the virtualized resources in cloud computing especially for the Virtual machines. Here we concentrate on difficulties of virtualization security, weaknesses, effect of virtualization on cloud benefits and recommend some approaches to defeat these issues.