CHAPTER 6

CONCLUSIONS

In this work, a set of security vulnerabilities are discussed in cloud virtualization. Then we proposed different approaches to overcome the problems of Virtual Machines with respect to security. Performance of the proposed approach in management of virtual machine resources facilitates security of performed operations on the platform. It distinguishes between valid and invalid (malicious) virtual machines. It is advisable to the IT infrastructures that, they mainly concentrate on investing on secured virtualization mechanisms since similar type of security challenges exists between both virtual and physical execution environments. Adopting the combined approach with security software provides required level of protection, immediate application of solutions and make sure that minimum level of security to all the virtual instances with no more overheads and problems.

We have simulated all the proposed approaches except the last one using the simulator tool called cloudsim. In the first approach, we can observe that when Virtual Machine is infected, it may affect other Virtual Machines, it may consume more memory and try to access the data and other resources of other Virtual Machines, which is shown in the result analysis. In the second and third approach, we introduced Security Supervisor component by which we can reduce the effect of infected Virtual Machine on other Virtual Machines and also avoid the functioning of infected Virtual Machine. Inclusion of IDS/IPS system to each Virtual Machine avoids the external threats to the Virtual Machines. In fourth and fifth approaches, we have duplication mechanism by which we can create the instances of Virtual Machines and allow them to work instead of Virtual Machines, if something happens to one of the instances, then other instance can continue the function of infected instance without disturbing the work. This enables the system to have Fault tolerance capability so that it will stop its work even in case of failure of Virtual Machine instances with adequate security mechanisms. In all the approaches, when Security supervisor in included, it provides the security to all Virtual Machines, but the drawback of that part is, it increases the response time of the Virtual Machine Monitor with Virtual Machines. This is because it has to check each and every request from all the Virtual Machines for authentication, authorization and resource access control policies. It is shown in the result
analysis.

All the scenarios have its own set of values and graphs which are shown in the Result analysis chapter.

The comparison chart for different scenarios are given. It shows different parameters such as Overall Response Time in milliseconds, VMM processing time in milliseconds, VM request servicing time in milliseconds and Memory consumption in MBs.