CHAPTER 5

ENHANCING CLOUD SECURITY THROUGH POLICY MONITORING TECHNIQUES

5.1 INTRODUCTION

Cloud Service providers are helping companies to reduce the high cost infrastructure installation and maintenance. To adopt the cloud services on a wide scale by business and individuals, it is necessary for cloud providers to provide adequate accountability and policy monitoring techniques to protect against an increasing number of threats, since security is a predominant issue of cloud services. There is no widely accepted methodology or toolset for achieving security in Cloud.

This chapter highlights the importance of policy monitoring techniques and the positive effects they enforce in terms of security. This chapter also provides effective ways in which the policy monitoring techniques can be used to enhance security in the cloud environment.

5.2 ENHANCING CLOUD SECURITY THROUGH POLICY MONITORING TECHNIQUE

Cloud Computing, besides containing a lot of nice features, also has some issues. The advantages of cloud computing includes scalability, availability, performance, cost-effective, acquire resources on demand, release resources when no longer needed, pay for what you use, leverage
other’s core competencies, turn fixed cost into variable cost, security is the major issue.

Absence or inadequate security leads to some of the major problems in a cloud environment. So enhancing security in cloud is of paramount importance. Figure 5.1 shows the proposed security architecture of a cloud.

**Figure 5.1  Layered architecture with Cloud Security Model (CSM)**

First layer is composed of resources managing the hardware, software, basic resources along with storage and networks. The second layer is the virtual management layer that keeps track of the virtual machines and their deployment. The third layer manages infrastructure details and the delegation details, the fourth and the fifth layer manages software and the platform and top layer is where the end user connects with the cloud.

Cloud Resources includes hardware, software, legacy application and network resources. Virtual management layer consists of virtual
machines, VM management and deployment and a hypervisor. Topmost layer is the application layer that runs the user applications. Security and compliances will be applicable to all the layers. Cloud Security Model will monitor the resources and virtualization layer and other layers based on policy.

5.3 POLICY MONITORING TECHNIQUES

Cloud Services are services provided to the end user/subscriber. In order to achieve this, a Service Level Agreement between the Cloud Provider and the user should be available. Since, security and compliances are applicable to all the layers; each layer has its own security measures. The application layer occupies the top most area, when it comes to the topmost layer will contain most of the security features including firewall and service vulnerability monitoring, risk assessment and control management.

Policy Monitoring is a continuous process based on regulatory compliance, information risk, based on service requirements, cloud business requirement, etc. E.g. giving access permission to service deployed in cloud, whether it is based on authentication, or open access, or giving only for restricted users alone. Since it is a continual process, it has to be maintained through security policy manager.

Based on the cloud business requirement, policy has to be developed and maintained in a set of documents, which has to be monitored through policy manager. It has to be developed in such a way as to protect entire organization resources as well as not to violate user privacy, by monitoring risks and threats.
Policy monitoring not only monitors the service level agreement of services provided by the cloud providers, but also, it gives secured protection to assets/resources of the organization; it shows how the performance will be monitored. Monitoring the service in turn indirectly provides reliability of the cloud service.

Here reliability of the service means cloud services are available for the user 24 x 7; availability of the service is also one of the important criteria here, especially in cloud service, since service is deployed in third party resources. So maintaining policy, in turn maintains the reliable, secured cloud services.

Security Policy encompasses a set of rules and regulations. The Policy implies how these rules and regulations are implemented and enforced. The triad Confidentiality, Integrity, Authentication is the basic for measuring any Cloud Service Policy.

Security policies are the foundation of a sound security implementation. For Effective Security Control, policies, standards, guidelines, and procedures, are to be developed and consistent with the appropriate standards, such as International Organization for Standardization (ISO) 27001 and ISO 27002. Developing and deploying a well written policy is vital for Sound Security of the Cloud Service Management.

All aspects of cloud application security should be captured from development to operation. Actually policy is manually documented and approved by regulations. To implement Policies, standards, procedures, and guidelines are to be followed and adopted.
Policies should include things such as Access controls, (i.e. only authorized user can access and have connection to the system), Data Protection, Confidentiality, Integrity, Identification and Authentication and Accountability. Policies should be carefully generated for cloud services keeping in mind that services are running in cloud. Only authenticated user can access the service at the same time preventing unauthorized access; further based on the user privilege level it must allow the access, modification, deletion of the service. It should protect the data at rest as well data at transit. Cloud provider must periodically monitor to ensure the security of the service and can take the authoritative back up of the service based on the service policy.

This research work mainly concentrates on achieving Enhanced Security of the Cloud Application. To achieve hundred percent security is not possible. Through properly devising the Security Policy, risks can be mitigated by adopting standard strategies and methods that are to be implemented.

Cloud Application Security is one of the significant criteria which have to be included in Service Level Agreement (SLA). SLA is nothing but the mutual agreement and commitment between the cloud user and the cloud service provider. Assuring Security to the application which is running on the cloud is a critical success factor of the Cloud. Application Security varies with the type of Cloud Service Model, whether responsibility is on the shoulder of cloud service provider (CSP) or application developer. Policy Monitoring Technique is as shown in Figure.5.2
This technique makes it certain that all the services are monitored continuously. It helps in the vulnerability monitoring and risk assessment. Based on the risk assessment appropriate counter measures are applied to overcome the security problem. By using Java Authentication and Authorization Service (JAAS) the administrator can verify the identity of the user and their authorization towards accessing the service as per the defined SLA.

Authentication module checks for the identity of the user accessing the service regardless of the service type and nature. Authorization module checks for the user’s authorization to access the service based on Service Level Agreement. Policy is generated based on the
SLA agreement between the user and the provider. Here policy varies with price and other factors. Security manager will monitor for vulnerability issues and risk assessment is made and based on the results and appropriate countermeasures are applied.

In the case of PaaS, Application developers are fully responsible for the coding, but underlying resources are owned by CSP. In the case of IaaS, developer is responsible for the security of the application. But in SaaS, CSP is responsible. Whatever might be the type of Service Model, while developing and deploying the application on cloud, the developer should follow the standards such as OWASP’s guidelines and adopt Secure Software Development Life Cycle (SDLC) for developing the Secured Application.

By adopting the SecSDLC, Cloud Security Policies to be implemented are discussed, finalized, approved, and documented, implemented, tested, counter measures and control management are kept up to date for the current changing threats.

Based an end user’s requirement, which might be IaaS, PaaS or SaaS, a single Virtual Machine is allotted for the user. Creation of Virtual Machine and its images are performed based on their policy requirement. If vulnerability has been detected, appropriate steps can be taken in order to solve the issue. Isolating Virtual Machines of each user is important which can be done with the help of the hypervisor.

Virtual machines have the provision to take snapshots. Hence in case of intrusion, necessary steps such as forwarding request to the next VM can be taken for recovery. Snapshots that were taken can be used for
creating the new virtual machine. At worst case, the entire virtual machine can be destroyed and can be reconstructed immediately with the help of the snapshots without affecting the regular workload of the user. Many Virtual Machines can be run on a single host machine. Proper updating of VMs Operating system, installing and updating the firewalls in VMs is important to ensure the security of the service. Based on the policy based risk assessment report generated, maintenance of the Virtual Machine can be achieved.

5.4 SUMMARY

This chapter describes the policy monitoring techniques, which is used for monitoring security in cloud architecture. A Cloud Security Model (CSM) is proposed, which works with the well known cloud layered structure. A policy monitoring technique is proposed with various parameters such as authentication and authorization, security audit, risk assessment and counter measures and control management. The proposed architecture exhibits an effective security solution for usage in cloud architecture. The usage of policy monitoring has enabled enhanced security, by which the user’s data and their services are kept secure. Next chapter 6 discusses about the security enhancement is brought about by combining virtualization and policy monitoring techniques.