PRIVACY AND SECURITY IN CLOUD COMPUTING

By

Nasir Raza

Submitted to the Faculty of Department of Information Security,
Military College of Signals, National University of Sciences and Technology, Rawalpindi,
in partial fulfillment of the requirements for the degree of MS in Information Security

June 2016

SUPERVISOR CERTIFICATE

It is certified that the Final Copy of the Thesis has been evaluated by me, found as per specified format and error free.

Dated: ________________

____
(Col Dr. Imran Rashid)

ABSTRACT

Cloud Computing has achieved broad acceptance in the market and academia in a very short period of time, as evident from its broad deployment in the information technology industry. On the other hand, the service providers and clients of cloud have experienced concerns over security and privacy of the data and applications running in cloud architecture. Entirely new dimensions of security vulnerabilities, threats and attacks have been witnessed with adoption of cloud model, in contrary to traditional security systems. Clients may resultantly suffer through un bearable loss if undue importance is rendered towards the security and privacy issues in cloud model. Any organization that is migrating towards cloud, or already operating in cloud environment, needs to refer towards a complete security and management framework. Security audit of the system is an important aspect, so the organization should also look into certain challenges posed to network forensics in cloud environment.

This thesis work initially evaluates cloud architecture and security vulnerabilities and threats posed to it. A security feasibility has been conducted and a comprehensive security and management framework has been proposed for a sensitive organization operative in the cloud architecture. The thesis includes implementation of the proposal for which virtualized environment was setup as proof of concept. The framework, a layered security / management model, covers all essential security and management aspects for a sensitive organization to function in cloud environment. The stakeholders of cloud architecture need to know their roles and responsibilities in the model. The proposed framework is a guideline for both the clients and the cloud service providers towards their roles in the cloud computing model. The proposed framework, to the end, is compared with the existing security guidelines recommended by well recognized standard bodies in the area of cloud computing including CSCC, ISO/IEC and PCI-DSS.

Dedicated to:

My Supervisor,

My Committee Members,
My Family members,

My Teachers and Colleagues

for their unconditional support all the way.

ACKNOWLEDGEMENTS

First of all, I am immensely grateful to my supervisor Col Dr. Imran Rashid for his worthy supervision and support that enabled me to complete my thesis work. I would also like to thank my committee members, Lt Col Dr. Mohammad Babar Aslam and Lecturer Mian Muhammad Waseem Iqbal for their valuable technical support and worthy guidance. Further I am obliged to all my teachers and colleagues for their endless support.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AD	Active Directory
CIA	Confidentiality, Integrity, Availability
CPU	Central Processing Unit
CSP	Cloud Service Provider
CSCC	Cloud Standards Customer Council
DB	Database
DoS	Denial of Service
DDoS	Distributed Denial of Service
HA	High Availability
HIPS	Host Intrusion Prevention System
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
ILOM	Integrated Lights Out Management
IP	Internet Protocol
IS	Information Security
ISO	International Standardization Organization
IT	Information Technology
ITU-T	International Telecommunication union – Telecom Standardization Sector
MAC	Media Access Control
NMS	Network Management System
OS	Operating System
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry – Data Security Standards
PoC	Proof of Concept
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks

SaaS	Software as a Service
SAN	Storage Area Network
Snmp	Simple Network Management Protocol
Subnet	Subnetwork
VLAN ID	Virtual Local Area Network Identification
VM	Virtual Machine
vROM	vRealize Operations Manager

Chapter 1

INTRODUCTION

Cloud is an architecture where an aggregated pool of flexible computation, processing and storage resources is made available to clients through the internet as per their elastic requirements [1-4]. The cloud model significantly liberates its client from worries of consuming critical resources like time and expertise for provision of services in all the phases including planning, design, deployment, maintenance and extension of infrastructure. Resultantly there can be seen a significant reduction in investment by the client / user, not only in financial terms but also in terms of worthy time and critical resources. The model allows client to get services through latest technology, both in terms of software and hardware, despite relatively low investment. The customer is in capacity to rent the anticipated resources instantly, with minimum interaction with the cloud service provider (CSP), for the specified duration of his own choice as per his requirements [4].

There are certain substantial features of cloud model, including remote storage of data leading to loss of control over data, virtualization of the resources and remote hosting of applications, that raises security concerns of the clients [5, 6]. The security terminology in the cloud environment not only focusses on the security of the data, but it is equally important for the security of applications and computations [4]. The client does not require to have detailed technical knowledge of the underlying infrastructure and technologies being used for provision of services in the cloud model [7]. The cloud being revolutionary technology in the field of service provisioning has entirely changed the people's view on the architecture of service provision [8].

1.1 Cloud Architecture

The users of cloud have been relieved from the setup and maintenance of infrastructure (hardware and software) complexities for provision of required services [8]. The client can place his data and applications off site and will be able to access them as and when he wants, irrespective of his location, through the underlying infrastructure of internet [9]. The technologists of various technical domains have been fascinated by overwhelming features of cloud model to consider it as a suitable solution for them in handling of their data, applications and infrastructure [10]. Basing on the service model, there exists a total of three independent layers in the stack of cloud model [7]. Each of these layer is an entirely complete model of service autonomously. Infrastructure-as-a-service (IaaS), witnessed in the place of bottom layer in the format of the Cloud architecture, serves through a set of certain resources collectively made available that can help provision of services like processing / computational power, storage requirements and services related to network. The services can be provided in the form of virtual machines, physical server machines, dedicated / shared storage, security devices like firewalls etc. These services can be utilized by the clients as they will be installing their specific softwares (operating systems or applications) on to hardware for customized usage. Platform-as-a-service (PaaS) takes the central position as a layer in the stack of cloud model. At this layer, user gets services in the form of a platform or environment for some specific simulation or programming tools. Software-as-a-Service (SaaS) lies at the top of the model where from the clients are provided with the applications / softwares for their usage [1]. Management suite is considered as an additional layer that fulfills requirement of management of entire cloud stack.

1.2 Cloud Models and Characteristics

Any deployment architecture scenario of cloud can be categorized as either of Private, Public, Community or Hybrid model on the basis of deployment models [7]. Private Cloud model is the one where entire resources of the cloud architecture are absolutely for the organization owning (rented) the cloud. Public Cloud model is the one where slices of resources are sold to various organizations, in other words resources are shared. The Community model is the one where the sharing of resources is held only among the closed community members. Hybrid cloud is the one which is formed through combination of either of two previously discussed cloud models with an aim to meet additional requirements of the clients.

There are certain characteristics that are considered essentials in Cloud model [1], described as under: -

- Resource Pooling
- Broad Network Access
- On Demand Self Services
- Rapid Elasticity
- Measured Services

1.3 Security Challenges in Cloud Environment

The broad acceptance of cloud led to wide deployment of the model in the industry, however the relevant technologist witnessed new-fangled security and privacy issues with time. This forced concerned technical people to reevaluate the prevailing mechanisms of security for cloud architecture. The actual deployment of the cloud is not considered as secure as the security claims exists in the papers [11]. The user is generally not allowed to monitor the granular details of the cloud architecture [12], that helps the users to maintain its emphasis on the real tasks instead of spending time and resources on deployment and maintenance of the architecture for service provisioning. New dimensions of attacks are revealed in the cloud architecture besides traditional security threats. Security model that has been adopted by the CSP is the one and only for the client to work with and rely on [6]. The primary and most discussed challenge in the cloud model which has proved to be the only accepted barrier in the deployment of cloud is security [9]. Multi-tenancy, outsourcing of data and intensive data computations are few prime security challenges in cloud environment.

1.4 Identification of the Problem Area

An organization with sensitive data and applications, when functioning in cloud environment, comes across critical security and privacy challenges that must be addressed in an appropriate manner. The precise identification of security vulnerabilities and threats is mandatory for appropriate handling of security issues. The process of evaluating new security threats and vulnerabilities should be continuous once the organization has moved into cloud model by migrating its data and applications in cloud architecture. There is a dire need of a comprehensive security and management framework for an organization functioning in cloud environment. The framework should cover all aspects related to security and management of the organizational data, applications, services and infrastructure.

1.5 Problem Statement

To carry out detailed analysis of cloud architecture, review the existing security challenges and threats in the environment and present a comprehensive security and management framework for an organization operating in cloud environment.

1.6 Thesis Goals

The thesis initially discusses cloud architecture, its characteristics and security challenges relevant to cloud environment. The discussion is followed by proposal of a security and management framework in the cloud architecture for sensitive organization which is operating in cloud environment. The proposed framework is based on the concept of defense in depth security which is achieved through various tiers of security and management in the framework. A virtualized environment is setup to serve as the proof of concept (PoC) for the implementation of the proposed framework. The challenges to network forensics in cloud environment are also discussed in thesis that also includes the grouping of these challenges into certain clusters. The splitting up of challenges posed by network forensic to cloud environment into various groups is aimed to indicate the relevancy of the problem to one of the appropriate sector out of CSP, Forensic expert, Forensic tools unless it is considered as beyond control of these. Proposed framework is compared to certain recognized frameworks by standard bodies in cloud domain.

1.7 Thesis Layout

The presented thesis is composed of six chapters. Second chapter reviews general architecture of cloud, characteristics of cloud, security issues related to cloud environment and challenges to network forensics in cloud computing environment particularly. A complete framework of security and management for the organization operational in cloud environment is presented in chapter 3 followed by the implementation and analysis of proposed framework in a virtualized environment in chapter 4. Chapter 5 compares proposed framework to certain international security architectures proposed by CSCC, ISO/IEC and PCI-DSS followed by chapter 6 including conclusions and recommendation for future work.

Chapter 2

CLOUD ARCHITECUTRE AND SECURITY ASPECTS

2.1 Cloud Characteristics

Cloud is among the most talked technology at the present however there are certain privacy and security threats to its clients that needs to be addressed timely. Industry is witnessing continuous growth in deployment of the cloud model for which the credit should be given to its elastic deployment techniques and notable features in either of the deployment or service model.

2.1.1 Resource Pooling

Customized services are rendered to the clients as per their flexible and changing requirements by virtue of cloud that holds an aggregated pool of resources comprising of computational processing, applications and storage by the CSP [3]. The cost involved in the provision of these flexible pool of resources is very economical in comparison to the establishment of infrastructure by the organization itself [5].

2.1.2 Broad Network Access

There is a broad range of computing devices / machines that can be used by clients to access the services offered by the cloud. These machines include personal laptops, thin clients, mobiles, tablets or personal digital assistants etc.

2.1.3 On Demand Self Service

The user enjoys the privilege of consuming customized set of services for as long as he desires. Provision of services can be acquired through little or no interaction with CSP.

2.1.4 Rapid Elasticity

The elasticity is a remarkable feature provided by CSP which ensures rapidly changing service set at any point of time. The client handles himself scaling up or scaling down of service set for any time frame of his own choice [3].

2.1.5 Measured Services

The billing of the services being utilized by user on cloud network holds user and CSP both accountable. The payment to be made by user is specifically for utilization of the services offered by the CSP.

2.2 Cloud Service Models

There exists a total of three layers of service models in the cloud environment that are available for the purpose of service provisioning to the clients of the cloud model [7]. These service models comprise of the Infrastructure-as-a-service (IaaS) model, Software-as-a-service (SaaS) model and Platform-as-a-service (PaaS) model. Either of these layers is an entirely complete entity for service provision. IaaS, the bottom layer, is the one in which a set of services is pooled up that includes infrastructure of hardware for processing, network, and storage for the user [13]. IaaS may include either of media for data storage, server machines (physical or virtual) or security devices etc. Clients can later on install their own software / applications as per their specific practical requirements [14]. PaaS is middle layer in the hierarchy that creates an installation platform to be used by the client for his specific application or environment [3]. The underlying network, generally internet, helps the cloud user to access and use development tools [6]. This layer provides service to the cloud users in the form of application software [3]. The central cloud server is presenting certain services that are being accessed and used remotely by the user of cloud network

[14]. The billing, metering and relevant management issues in cloud environment are handled by the management stack.

2.3 Cloud Deployment Models

The deployment of Cloud can be carried out as either of the Private cloud model, Public cloud model, Community or Hybrid cloud model. Private cloud is the model where all resources are dedicated to the only organization that rents the services from the CSP. Public cloud is the model where set of services is shared among the multiple organizations who are acquiring services from the CSP. In Community cloud model, the members of the cloud are generally selected on some common grounds and then cloud infrastructure is shared among them as public cloud model. Hybrid cloud model comprises of either of the two previously discussed models, where the aim is particularly to manage the additional requirements of the cloud users. The service models of cloud architecture, the deployment models and vital cloud characteristics are shown in Fig. 2.1: -

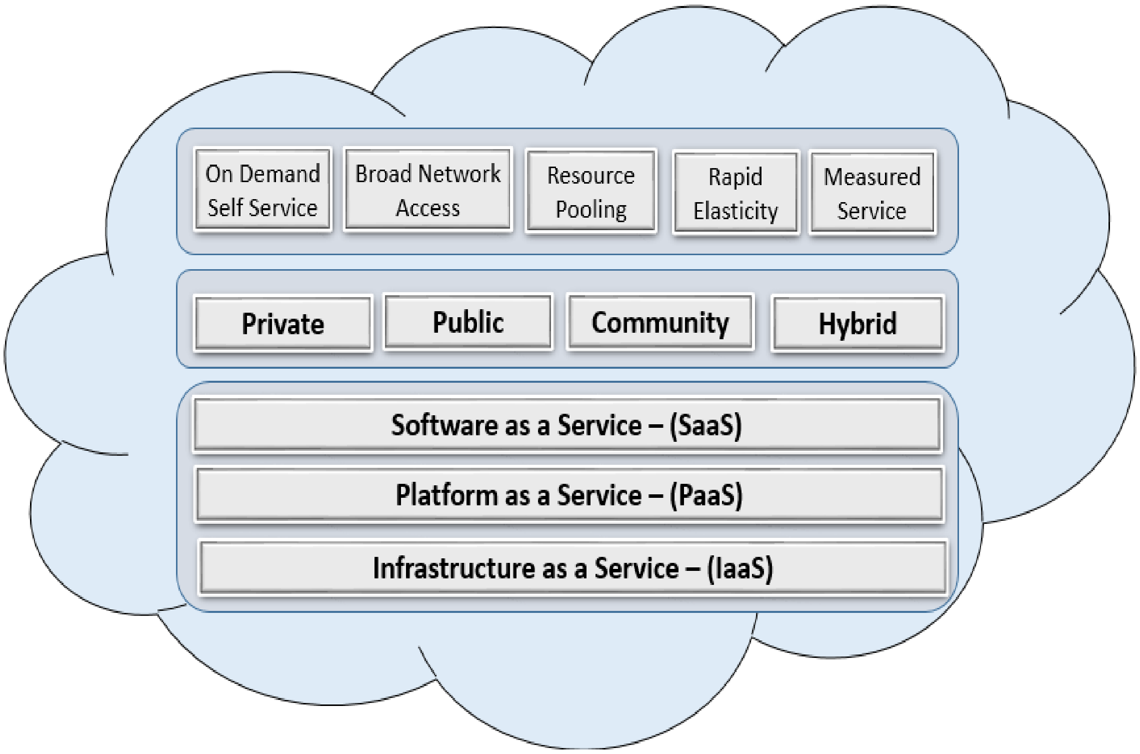


Fig-2.1 Cloud Computing Architecture

2.4 Security Challenges to Cloud

A large number of severe impacts of security threats and challenges exists for the clients using cloud model mainly owing to offsite storage of client's highly valued asset – its data [14]. The security threats posed by cloud environment is acting as the main resisting feature that is holding back a large number of organizations and clients from moving towards cloud architecture [8].

2.4.1 Main Reasons of Security Issues in Cloud

There are certain factors that lead to security related issues in cloud environment, discussed as under: -

2.4.1.1 Outsourcing

The critical data and applications of user are held with the CSP. Resultantly the user has no control on its data, referred as prime security concern of the user in cloud environment [3]. Client might not be having knowledge of the exact physical site where data is placed, in most of the cases [6], [8]. A conflict may arise at the moment when there is a dispute between client and CSP. The conflict may be more severe since varying policies may exist for the CSP and the country hosting the client's data and applications [7]. CSP should be in capacity to achieve the parameters of the Confidentiality, Integrity and Availability (CIA) with respect to data. The sub-contractors employed by the CSP provide certain services, that should also be considered as a possible cause of security breech for client's data in cloud environment.

2.4.1.2 Multitenancy

CSP may be sharing its infrastructure among multiple users of cloud. Particularly in a virtualized environment, a single physical server machine may be holding applications and data of various cloud users. Virtualization leads to an interesting scenario where security needs to be evaluated in new dimensions. The possibility of attack launched from some legitimate users cannot be even ruled out in case of virtualized environment. This shared data of client may be exposed to unauthorized users in a multi-tenant environment, leading to breach of confidentiality aspect at least out of CIA triad.

2.4.1.3 Massive Data and Intensive Computation

There are numerous intensive computations going on simultaneously in the cloud environment besides massive data handling [3]. This situation can only be handled by superior strategies at security layer in contrary to traditional security systems. Critical data of clients can be protected only by using high end devices (security oriented) in the cloud environment. CSP may adopt approach of carrying out lesser computations for the tasks in contrary to what he claims to achieve economy in terms of cost and effort [4]. The margin of achieving such approach by the CSP is because of lesser visibility in the data flow and processes at application layer. Interoperability among various clouds can only be achieved through standardization [7].

2.4.2 Review of Cloud under Key Security Attributes

The adoption of Cloud is on continuous increase in line with its popularity. Broad acceptance and rising deployment of cloud model has revealed more concerns of security forcing technologists and researchers to reevaluate conventional mechanisms related to security. Although certain CSPs have claimed their cloud environment to be secure enough to handle all security concerns, real time cloud deployment has not been witnessed in line with these claims [11]. Additional dimensions of attacks are to be handled in cloud environment besides certain conventional security concerns that exist in the traditional systems. It is security, that has been rated as top most barrier to be overwhelmed for successful growth of cloud model in industry [9]. Table-1 presents summary of certain challenges faced by cloud environment that can be reviewed under certain important parameters of security including CIA triad, privacy and accountability, as shown under: -

General Security Parameter	**Reason causing Security Issues**	**Security Threat**
Confidentiality	Outsourcing	Loss of Control over data
		Data Leakage from storage
	Multi-tenancy	Cross virtual machine attack (through side channels)
		Malicious System Administrator attack
		Access to Residual data
		Third party mishandling data
Integrity	Data Auditing by third party	Data exposure to third party
	Computational Transparency from client	Violation of certain policies / procedures
Availability	Sharing of Cloud Infrastructure	Denial of Service (DoS) Bandwidth Starvation Fraudulent resource Consumption Fault Isolation Distributed Denial of Service (DDoS)
	Outsourcing	Discontinuity of services
		Data Loss
		Non availability of data owing to dispute
	Cloud Interoperability	Inability to use data
Privacy	Outsourcing	User's Profiling
		Sharing of client's personal data (with third party)
Accountability	Identity Secrecy	Inability to track activity
		Identity Spoofing

Table 2.1 Security Issues and Threats in Cloud Computing Environment

2.4.2.1 <u>Confidentiality</u>

A system is said to ensure Confidentiality if no un authorized person is allowed to gain access to data of a user, applications or system that is considered protected [8]. The protection of data is not only to be ensured form other clients or attackers, but also from the CSP staff / employees. The authorized persons only should be having access to the documents of a client [6]. There are more chances in breach of confidentiality as the system grows or the number and type of devices increase that can be connected to the network [8]. Public cloud model, since shares data among its various clients / organizations, is more prone to attack on confidentiality when compared to private cloud model [9]. Once data is deleted on storage by the client, the attacker can try to access residual data in order to recover the original data. Cross virtual machine (VM) attack which is launched through side channels exploits the multi-tenancy feature of cloud to breach confidentiality of the system. CSP administrator has rights at a level higher than normal user, hence can access the storage area of the customer, hence breaching confidentiality.

2.4.2.2 Integrity

Integrity of data implies that there should not be any modification in the data by any person who is unauthorized to do so. Integrity terminology applies to both data and applications. It is not only data that should be protected from unauthorized modification, but also the applications or programs of the user should be protected from integrity breach. No unauthorized person should have access rights to modify a data or applications for which he is not entitled, to ensure integrity [8]. There can be malicious intent to compromise the integrity of the data / applications, or maybe it can happen by some other cloud user unintentionally because of inappropriate access rights mechanism. A weak access control mechanism or insufficient protection measures on data can lead to breach of data or applications integrity in cloud environment. The client of cloud may not be able to monitor such changes all the time owing to off storage that reduces control of client on data or transparency of operations form client in cloud model.

2.4.2.3 Availability

Availability, one of the most acute feature in effort to provide smooth services to the client, implies the data and applications of the client should be accessible to him round the clock, as and when he desires, without any un necessary delay. A system is said to be available to the client if its availability is around 99.999% [7]. The authorized user should be able to access its data, applications and hardware all the time as per his requirement. To achiever availability, some sort of backup approach needs to be adopted at hardware and software level. The backup technique is not applicable to data only, but also to infrastructure, hardware, network, storage, server machines, software applications and to an extent that power arrangements are also included in this context. The enterprises working at multinational level, even provide the feature of redundancy at geographical level to maintain highest level of availability [9].

There are certain attacks that may be launched to compromise availability of a system, particularly in the context of cloud architecture these attacks may prove to be disastrous since cloud is offering services to various clients / users / organizations across the globe. These attacks may include particularly denial of service (DoS), direct or indirect, or Distributed DoS (DDoS). A large number of fake requests are flooded from the attacker to the target server with an aim to exhaust resources of the target machine, so as it is unable to provide services to its legitimate users smoothly. The threshold plays an important role in attempts to block such an attack. If the attacker plays intelligently and keeps on launching this attack on and off with a flood that does not reach the threshold, it may not be even detected and may prove to be more fatal for the system. The attack can be prevented by first monitoring the activity and then migrating the victim to some other subnet, attacker being unaware of new subnet fails to relaunch attack. There can be discontinuity in provision of services because of some dispute with the CSP, affecting availability [9]. Whatever the reason be for discontinuity of services, the damage of reputation and finances will be borne by the client primarily, most of the times.

2.4.2.4 Accountability

Accountability implies to conduct tracing of any activity on the system and relate it with the evidence. The tracing of an activity is more difficult once we are dealing with the cloud in comparison to system otherwise [7]. The secrecy of clients on cloud network demands from CSPs not to disclose their identity in tracking mechanisms, however it brings up certain security issues. This creates certain cushion for the attacker to launch malicious activity without disclosing his identity. The dynamic and complex nature of cloud architecture makes it difficult to conveniently isolate the compromised resource physically [11].

2.4.2.5 Privacy

Privacy focusses particularly on the personal data of the client that should not be disclosed to irrelevant personnel [6]. The privacy of users on cloud network can be compromised if significant weightage is not given to the security of the cloud environment by CSPs. The level of risk increases when Cloud Service Provider hides the fact from client to safeguard its reputation. Generally, the vulnerabilities, threats, security challenges and counter measures to achieve security are same as applied in the Confidentiality parameter. Auditing of data gives a solution to client to verify data integrity, yet auditing by a third party brings confidentiality of data at risk. Some technique needs to be improvised to protect confidentiality of data under public auditing by third party. The integrity check should be carried out for the data stored on cloud site and data should be scrutinized before its utilization. The traditional approach used for this purpose can work by downloading all the data from the cloud to the client, and then checking integrity of entire data through verification of some hash value or signatures. However, the efficiency of adopting traditional approach is a big question mark. First of all, the volume of entire data is quite huge, downloading this will consume large no of computations and network resources. These problems force to find some technique to audit the data to verify integrity without downloading it from the site.

Clients' profiling is another serious outcome of the privacy breach, which is more relevant to cloud environment. The personal information of client might be sold to third party for commercial purpose, or might be even misused with malicious intentions. The administration of certain social media websites may have gathered specific details about an individual, this information may be even more than that held with the client's colleagues [3]. Client's personal details including his religious beliefs, ethnic ideas, personal / political affiliations may be shared with third party.

2.5 Challenges to Network Forensics in Cloud Computing

Digital Forensics is the field where scientific techniques are applied in carrying out investigation of an incident to carefully extract the evidence. The extracted evidence is then correlated with the events that can assist in validation of the activity. Network forensics deals particularly with the network traffic in the architecture and is considered branch of digital forensics [15]. The traffic on the network is captured for analysis and further investigation so that the suspected activity can be referred to the originator with support of evidence [16]. Reconstruction of activities is necessary to reach the authenticated conclusion. The correlation must validate the user performing certain activities with certain time stamps. The framework or procedure adopted in network forensics is composed of several phases including preparation for carrying out investigation, extraction of evidence and its preservation followed by detailed analysis of the evidence [16]. The final conclusion is in the light of examination and analysis carried out on the extracted evidence and correlation of the evidence to the suspect.

Cloud model provides pool of aggregated resources to its clients on flexible terms through the underlying infrastructure of internet [15]. The data stored by the client on the cloud site is placed with other organizations / clients [17]. The forensic expert need to be more skilled and knowledgeable when moving into cloud environment. The processes and procedures of forensic investigation are required to be extended to the domain of Cloud environment too [18]. Network forensics problems rise even further in the cloud computing environment. While conducting forensic investigation, analysis of network traffic has assisted the investigation process [16], although managing capturing and analysis of huge amount of traffic has always been a serious concern. Segregating challenges to network forensics in to certain groups is considered very useful for appropriate handling of the issues by the relevant domain.

2.5.1 Network Forensics

The evidence, point of interest for the forensic expert, may exist in static form, moving state or under execution [19]. A systematic procedure is followed by digital forensics to extract the evidence, surely an authentic evidence. Main difference between digital and network forensics is about handling of data, where the digital forensics generally handles static data only whereas data handled by network forensics can be in rest or in motion. The application of the digital forensics particularly in the domain of the IT networks is the science known as Network forensics [16]. It is the network traffic and logs of the machines that is monitored and examined to identify some incident [19]. The examination is aimed to trace and track the incident to attribute it to the originating source finally by validating the involvement of the suspect in the activity [20]. This involves path tracing to the source of the activity. Network forensics may be considered as typically further extension of the features of security system employed on the network. The major difference between security system of the network and network forensics is that security is aimed to protect from incident happening whereas network forensics is not specifically aimed to protect the assets of the network but only to track the incident later on. The network forensics procedure can be assisted by certain intelligent technique like implementation of honey pots in the network [21]. Tracing back to the source of the incident in other words implies tracing back to the IP address of the device that originated the activity / attack [22].

The attack needs to be investigated, irrespective of the fact that attack caused damages to the network or not. Network forensics is a systematic procedure that adopts scientific techniques including identification and extraction of evidence, analysis of evidence, correlation of evidence to other known facts and reporting on the incident. Reporting ultimately either denies or validates involvement of a certain suspect in the activity [16]. Manual analysis of captured traffic can be held although use of scientific tools is preferable as it achieves efficiency, accuracy and boost performance. The relevant monitoring and regularly capturing network traffic, capturing of pertinent traffic can be helpful in the process of network forensics. The approaches generally adopted for forensic investigation can be either of “Catch it as you can” or “Stop, look and listen” [23].

2.5.2 Network Forensics Framework

It is considered that Network forensics is further extension or branch of digital forensics, hence follows generally same principles and guidelines as followed by digital forensics [23]. There is a well-defined framework for network forensics having certain mandatory steps as shown in Fig.2.1 [16] as under: -

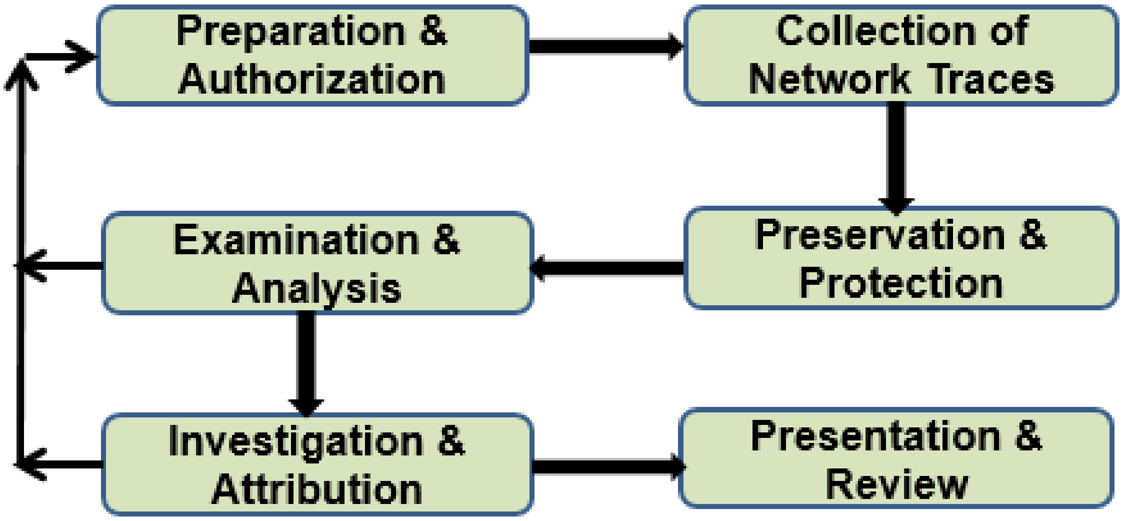

Preparation & Authorization
Collection of Network Traces
Examination & Analysis
Preservation & Protection
Investigation & Attribution
Presentation & Review

Fig-2.2 Framework for Network Forensics

The complete framework for network forensics includes following steps in a sequence: -

- Preparation and Authorization to conduct network forensics activity
- Collection of incident traces from the network
- Preservation of the evidence and its protection
- Analysis of evidence
- Investigation of incident and referring it to attacker
- Demonstration of the results and review by experts / legal body

2.5.3 <u>Tools used for Network Forensics</u>

The activity conducted on the network leaves its traces in the network traffic most of the times, which is point of interest for the forensic expert investigating the incident [23]. There is a requirement of a packet sniffer tool that can capture these packets from network traffic. A large number of such tools, both in hardware and software, are available in the industry that are helpful to the network forensic expert [16], e.g. Wireshark, Tcpdump, Ethereal, CapAnalysis, E-detective, NetDetector, ipfix etc. The tools are capable of capturing traffic from the network and conduct the analysis of the traffic afterwards. The feature of off line analysis in other words enables the administrator to travel back in time which is remarkably strong and helpful feature of the tools. Advanced techniques need to be adopted by forensic experts since attackers are also getting more and more knowledgeable and technically sound in the present era of IT. Finally, the report generated by the forensic expert is a valuable document, since this document is containing the extract of the evidence. The document should contain complete and authentic evidences that can support the content of the report and attribution of the incident towards some source. The selection of an appropriate tool for forensic activity is very important since report generated by a non-standardized will not be of much help in the court.

The tools used for network forensics procedure are only meant for investigative purposes and should not be considered at all as the security system for the network. The network forensic tools will not be replacing the security measures taken in the form of firewalls or IDPS [21]. There are certain mandatory characteristics expected from network forensic tools [23], mentioned as under: -

- Ease of use and management
- Efficient performance / High speed search
- Network traffic capturing for deep off line analysis
- Memory, File and Disk forensics capability

2.5.4 <u>Network Forensics Challenges Categorization in Cloud Environment</u>

Network forensics incorporates a devoted monitoring layer in the network that can collect relevant traffic / evidence for future analysis [15]. This layer boosts the entire security model and assists in monitoring and intercepting any malicious activity form outside or inside. Development of out of the box and effective techniques by CSPs is needed to handle the intricate model of cloud from network forensics point of view [24]. It is challenging to carry out investigation in cloud architecture owing to certain reasons including vast magnitude of network traffic / data [25]. It is challenging for the forensic expert to get access to the data / network traffic and extract evidence from it particularly in cloud environment [26]. The handling of network forensics issues particularly in cloud domain can be optimized by segregating it into certain categories including Forensic experts, Forensics tools, CSP and remaining declared beyond control of former three spheres, shown in Fig. 2.3 as under: -

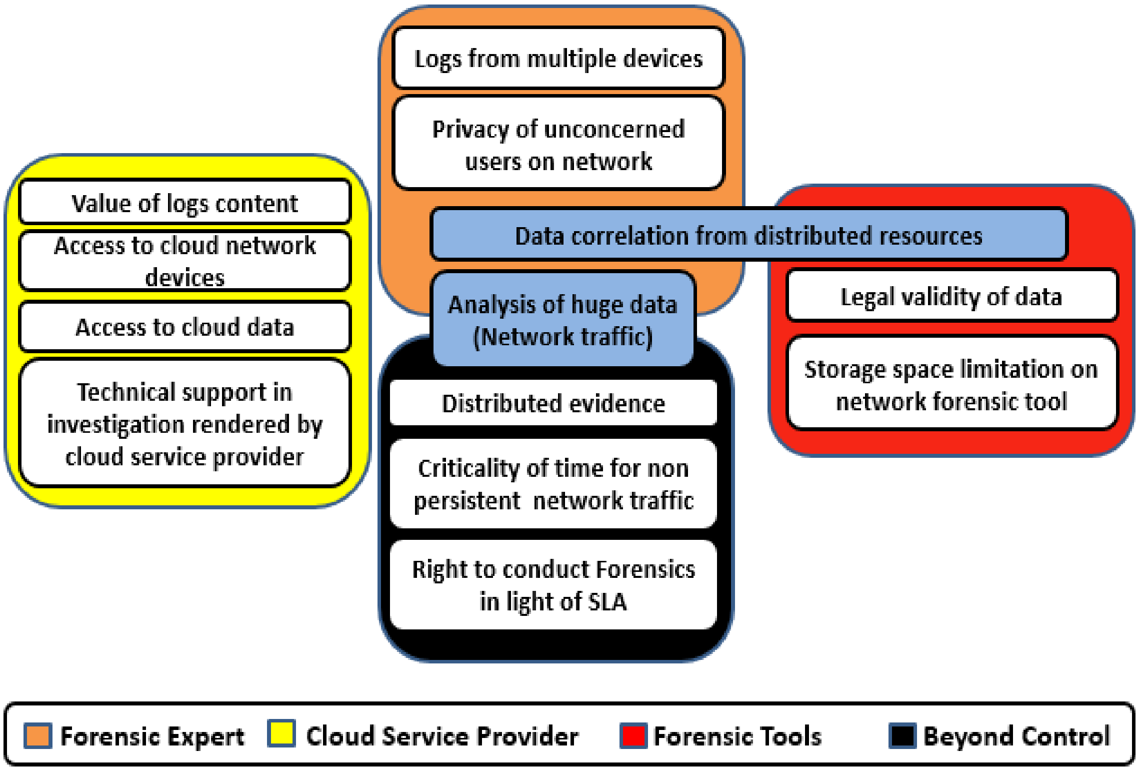

Logs from multiple devices
Privacy of unconcerned users on network
Value of logs content
Access to cloud network devices
Access to cloud data
Technical support in investigation rendered by cloud service provider
Data correlation from distributed resources
Analysis of huge data (Network traffic)
Legal validity of data
Storage space limitation on network forensic tool
Distributed evidence
Criticality of time for non persistent network traffic
Right to conduct Forensics in light of SLA
Forensic Expert
Cloud Service Provider
Forensic Tools
Beyond Control

Fig-2.3 Network Forensics Challenges Categorization in Cloud Environment

2.6 **Summary**

In this chapter, I have shortly mentioned about the architecture of cloud environment including its deployment and service models along with essential characteristics. The discussion continues with the description of security issues relevant to the cloud environment. The cloud environment has been reviewed under certain key security parameters to analyze the possible impact of potential security threats in cloud environment. Further Network Forensics concept has been described briefly. Certain challenges that are presented to network forensics particularly in cloud computing environment have been highlighted. Segregation of these challenges into various groups has been explained. The challenges have been segregated into categories of Forensic expert, Forensic tools or CSP for appropriate handling whereas few challenges are considered beyond the control of either of these groups.

Chapter 3

SECURITY AND MANAGEMENT FRAMEWORK FOR A SENSITIVE ORGANIZATION OPERATING IN CLOUD ENVIRONMENT

3.1 Introduction

The data held with a sensitive organization is its most valued asset and is given top most priority. The loss of such highly sensitive data can be disastrous for the particular organization. The moment a sensitive organization is linked up in cloud environment, the stakes for security of data and applications rise manifold. A wide range of vulnerabilities and threats appear to the organization in cloud environment, to handle which the organization should follow a well thought framework. A comprehensive security and management framework for a sensitive organization operating in cloud environment will be presented and discussed in this section of thesis. The proposed framework focusses on all security and management aspects that needs to be worked upon between client and the vendor providing cloud services. The most valued and critical asset of the sensitive organization is data, resultantly must be handled with highest level of security [13].

The multi-layered approach of defense in depth, adopted in proposed framework, ensures protection from wide range of security threats. This multi layered ensures if a layer of security has been compromised by the attacker, there are other security barriers in way that will protect the system from being compromised. Resultantly the layered defense architecture reduces the probability of threats penetrating a secure system. The efficiency and optimization of system resources will have finally positive impacts once the environment has been secured by the CSP [14].

3.2 Proposed Security and Management Framework

A conceptual framework is proposed for sensitive organization functioning in cloud environment. The security has been implemented at various tiers in the proposed framework, keeping defense in depth approach for security as the ideal approach to achieve highest security level. Security and management parameters are implemented at each tier of the proposed framework independently as per concept of the layered model.

The tiers in the proposed security and management framework are under: -

- Physical Security tier
- Implementation tier
- Service Availability tier
- Management tier
- Monitoring tier

The proposed security and management framework is shown Fig. 4.1 as under: -

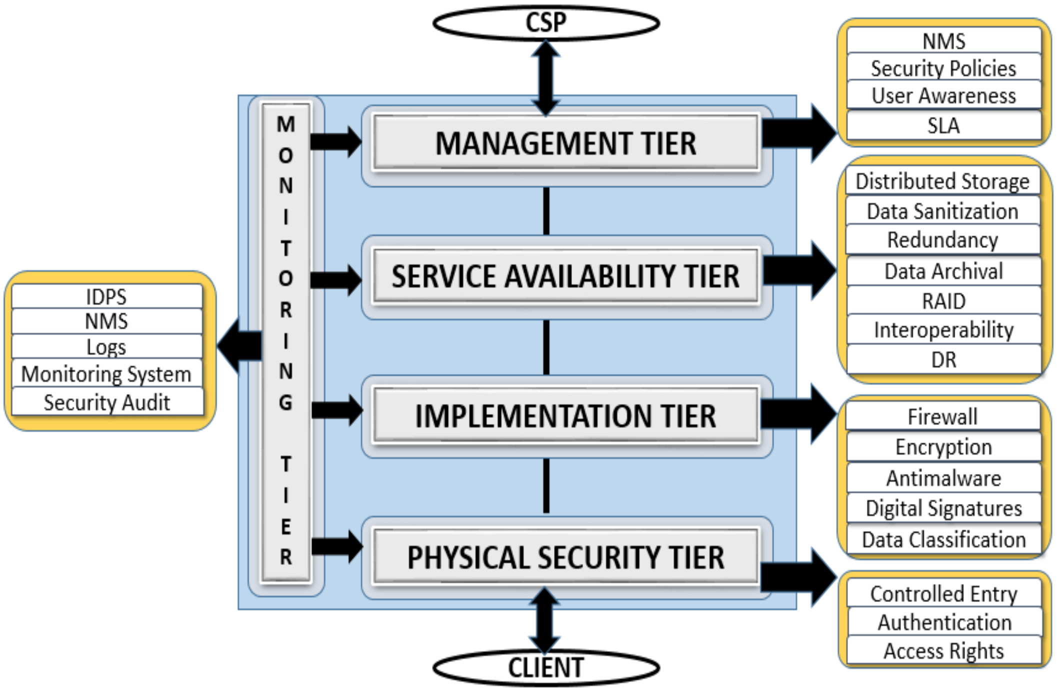


Fig-3.1. Conceptual Diagram of Security and Management Framework for organization operating in cloud environment

3.2.1 Physical Security Tier

3.2.1.1 Controlled Entry

The first layer of security model is related to the Physical security and deserves prime attention. Controlled entry needs to be designed and implemented to achieve physical layer security that should include approaches like authentication through smart cards provided by organization, biometric system including finger prints of the clients and retina scan. The physical inspection of the individuals and scanning of their belongings should be assisted by authentication of client's smart cards and vehicular stickers through wireless tag readers. A monitoring system should be installed at all entry / exit points and critical locations and must be monitored all the time.

3.2.1.2 Authentication

The users should be authenticated prior to provisioning of access to the resources as shown in the proposed framework. A dedicated centralized server for authentication purpose is preferable when the user base is increasing. In addition to users, entry of individual machines / end systems should also be controlled on the network. This can be achieved by media access control (MAC) address binding and spoofing techniques that will allow the only permitted devices to join the network and restrict connection to network otherwise.

3.2.1.3 Access Rights

Once the authentication of the users has been carried out, the level of access rights provided to the users need to be controlled through implementation of access rights mechanism. There should be constant monitoring of effectiveness of access rights by the CSP and changes may be incorporated in the system if desired since entities are dynamic in cloud architecture. The document or configuration file of access rights deserves extra ordinary protection through encryption while it is being stored [27]. Access rights can be controlled conveniently by making groups of the users at OS level or through configuring and implementation of access control lists (ACLs) on the network devices. ACLs are rules that specifically allow / deny certain clients or machines to communicate with other clients or machines on basis of their IP addresses and services being used. The permission criteria include a set of IP addresses with combination of certain IT services to be used.

3.2.2 Implementation Tier

3.2.2.1 Firewall Protection

The firewall needs to be installed at the gateway of traffic so as it can monitor all the incoming and outgoing traffic thoroughly. Entire infrastructure of cloud network, including cloud storage, database machines, server machines and networking equipment should be protected from a firewall. Hardware firewalls should be installed at ingress and egress traffic points whereas software firewalls should be configured on the server machines and end systems as an additional layer of defense. Hardware firewall is surely a preference over software firewall in the network for monitoring of entire ingress and egress traffic and certain other critical points. However, the selection of hardware firewall is a trade-off with the cost, complexity and cost to achieve skills required for configuration and maintenance.

3.2.2.2 Encryption

The security level for data, may it be static or in transit, can be increased manifold using encryption techniques [28]. Encryption is a trade-off between degrading performance and increasing security levels, resultantly selection of type and variant of encryption depends upon the criticality of applications and data. It is secrecy of the key which decide how strong the algorithm is, although importance of a sophisticated algorithm cannot be denied. Here comes in the issue of key management that demands a careful, optimized and secure handling approach [29-30]. The performance of the system is severely affected once encryption is used on large size of data and traffic, as can be seen particularly in cloud environment [2]. There is a limitation of implementing computations on the data once it has been encrypted. To protect data in case of theft of storage, it is recommended to use technique of full disk encryption, although for cloud it is questionable owing to uncommon probability of such incidents [14]. The processing on encrypted data without deciphering it can be achieved using homomorphic encryption technique. The results of operations are same in homomorphic encryption on encrypted text as it would be on plain text. It saves time on decrypting the cipher text and processing involved in deciphering it before processing and ciphering later on [5].

3.2.2.3 Antimalware Protection

Protection from all kinds of malwares, including viruses, spyware, adware, Trojan horses and worms etc., is necessary for data and applications in cloud architecture. In addition to viruses and worms, attacks like phishing are also potential threats for cloud environment [31]. The system is scanned by the antimalware time to time to spot the infected files and programs and handle them accordingly. Constant updates of antimalware are necessary to handle zero day exploits since attackers are coming up with new virus every other day.

3.2.2.4 Digital Signatures

The modification or tampering of client's data can be ensured through some advanced technique like digital signatures. Digital signature provides feature of sender authentication in the system so as the sender or receiver cannot question the sanctity of the document. The issue of impersonation, modification of the documents and non-repudiation are quite common in the IT communication that can be best handled by use of digital signatures. The digital signature is so common by now that they carry a proper legal standing to support their client.

3.2.2.5 Data Classification

The value of data, its criticality or the potential risk linked to it defines the sensitivity of data. The sensitivity or criticality of data is the key factor that can be used to classify the data in to numerous classes [32]. Data can be classified to numerous classes and there is a set of rules applicable to each class as per the sensitivity level of the data.

3.2.3 Service Availability Tier

3.2.3.1 Distributed Storage

Confidentiality is achieved through Distributed Storage concept by dividing data into numerous chunks and storing these chunks at multiple storage locations [13]. There are certain algorithms that are followed for the partitioning of data into chunks, the same algorithm makes it convenient to retrieve the data from either of the site. Distributed storage increases the data protection resultantly raising standard of confidentiality. Synchronization of data and events is one of few issues related to distributed storage that needs due attention.

3.2.3.2 Data Sanitization

The data which has been deleted by the client from the cloud storage should not be recoverable. Confidentiality of offsite stored data may be breached if it is not permanently deleted from the storage media [3]. Although the general approach followed may store copies of the client’s data on cloud to ensure recovery of data in case of disaster incident, however same feature of data redundancy can cause compromise over confidentiality. There are certain recovery tools in the market that help to reconstruct data and recover the data files that have been even deleted by the user [11]. Encryption of data is one useful technique in this scenario which converts data into useless cipher text which is of no use to the attacker who has recovered such data files from backup copies or residual of deleted data. It is essential to conduct data sanitization once the cloud agreement terminates with the client for provision of data storage services, otherwise the remnants of data can be mishandled by the attacker [10]. Entire data including backup files of original data must be removed properly.

3.2.3.3 Redundancy in Critical Resources

Redundancy is the most important factor that assists in providing 99.999% of availability in the system. Redundancy is not only for data but primarily it is achieved for infrastructure, network, hardware, software, storage, server machines, database instance and power arrangements etc. Redundancy is always a tradeoff between reliability of data and services with cost, hence selection of appropriate level of redundancy is significant.

3.2.3.4 Data Archival

The most valued asset of the user in a system and particularly in cloud environment is his personal / organization's data. The data can be protected well by archiving it on a remote site, resultantly improving security of data as well [11]. The selection of point of time for archiving the data and its backup duration is both adjustable and delicate. There is a certain amount of traffic generated on each archiving activity, hence suitable frequency of data archiving should be set through consultation with experts in the field. Generally, off hours are selected mostly for such activities instead of working hours or peak hours. To protect archived data from natural calamity or disaster, it should be even placed at some distant location from the original data site. Consistency of data and applications is vital factor that should be given due consideration in archiving process.

3.2.3.5 Redundant Array of Independent Disks (RAID)

More than one physical disk can be used in certain arrangement to achieve the RAID. RAID is a technique which further improves upon data availability in the cloud environment. Certain levels of RAID are available in the industry, either of these can be conveniently used by the cloud user provided CSP is elastic in provision of variety options to the cloud user. The selection of certain RAID level by the user should logically depend upon the criticality of data, budget available with the organization / client and desired performance metrics etc.

3.2.3.6 Cloud Services Interoperability

Interoperability ensures reusability of the data and applications once it is shifted from one cloud setup to another. The interoperability of cloud services needs to be ensured by the CSP. Migration of data, applications or services between clouds should be transparent and preferably seamless to the cloud user. CSP can achieve interoperability by adopting certain well recognized standards at international level and common standards being followed by the main stream vendors. Failure in compliance to well recognized standards by the CSP may lead client to interoperability issues at later stage. Till date, it is a valid security concern of the vendors and cloud that standard protocols do not exist in the domain of cloud computing as these are available for the IT otherwise [33]. Virtualization is an advocated approach to achieve interoperability in the cloud architecture. Interoperability helps to gather clients and various vendors of cloud computing to a single common grid. Security is prime concern in the process of interoperability of data and services in the cloud architecture.

3.2.3.7 Disaster Recovery (DR)

DR implies bringing back operations of the organizations alive and provision of un interrupted services to the clients again at the earliest in case of some disaster. Aims should be achieved with minimum interaction with the technical support team and least utility of the resources, may it be technical or physical resources. DR planning is an entirely complete field, that demands systematic study of certain factors at the time of designing and planning phase in cloud computing architecture. One of the important factors in the

DR planning is suitable selection of datacenter location from calamities point of view [34]. Disasters can be natural calamities or sometimes manmade or artificial as well, e.g. disaster as a result of a cyber-attack is an example of man-made disaster. Handling of disaster incident should be properly formulated and highlighted by CSP [35]. The DR plan is a phased program where the emphasis is primarily restoration of business critical services whereas remaining services are focused in phases to follow. DR is not only taking backup of data, but it includes reactivation of entire services for the client of cloud as it was before the disaster incident [36].

3.2.4 Management Tier

3.2.4.1 Network Monitoring System (NMS)

NMS is a software / management suite used by the CSP on the entire cloud network to continuously monitor the devices on the network. The monitoring and management feature of NMS makes it part of the Management tier in the proposed framework. Devices may be all type of hardware on the cloud network including server machines, networking equipment, storage machines etc. NMS does not only monitor the liveliness of the network device but also continuously monitors the health status and performance of each device on the network. Agents are installed on the devices on the network that are to become part of NMS. These agents keep passing health and performance status of machines to the centralized management server. Generally, simple network management protocol (snmp) is the protocol being used in the industry by the technologists for network management. It immediately highlights if any unusual incident occurs on the machine as an alert, warning or error. Different levels are set for incidents to declare them as warning, alert or error basing on some thresholds that can be customized by the administrators.

3.2.4.2 Security Policies

Security experts of the organization are responsible to draft security policies for their organization, although same are to be approved by the top level management in the organization. The security policies can never be implemented practically unless top level management itself takes interest. A security policy is meant to put certain restrictions on the clients while accessing the resources and allowing access to specific resources, data or applications. Certain security policies should focus on the disaster management and recovery in the cloud architecture. Security policies should not be affecting the data flow at any level. An audit of security policies is essential to validate the implementation and effectiveness of the security policies. A periodic review of security policies will help to improve the security for the organization in cloud architecture.

3.2.4.3 User Awareness

The security policies can never be implemented in true spirit unless users are educated how important these security policies are for the security of data and applications of the organization in the cloud architecture. Users should be given awareness on the criticality of situation if security policies are violated. Users should realize importance of security in the organization and take on the security measures at their will. The user awareness should be made part of the training program of the organization for its effective implementation. The users should be formally educated on procedures to be adopted so they can abide by the security policies. In addition to user awareness, system should enforce certain security parameters on the users so users don’t have choice to avoid security measures at certain places.

3.2.4.4 Comprehensive Service Level Agreement (SLA)

Availability of services to the users in the cloud architecture can be greatly improved through implementation of a wisely drafted SLA. SLA should be a reflection of the security policies of the organization. While drafting of SLA, client faces certain problems like he may not be well aware of the complex security terminologies used in the draft of SLA [37]. SLA should be tactfully drafted so as its not only the client who has to ensure all aspects of security rather CSP should also be given certain responsibilities to implement security measures in the architecture. SLA is the only document that imposes certain limitations on the vendor. CSP should be bound in SLA for provision of services to the cloud clients round the clock. SLA should include terms and conditions to bound CSP to provide security at certain desired level that can be proved with evidence [38]. It is SLA that legally ensures confidentiality, privacy, reliability and availability in the provisioning of the services by the CSP.

3.2.5 Monitoring Tier

3.2.5.1 Intrusion Detection and Prevention System (IDPS) Protection

IDS is only capable of identifying any sort of malicious traffic passing through the device whereas IPS has the capability to even prevent any such malicious traffic. Entire inbound and outbound traffic of the cloud should be monitored by the IDPS for which IDPS should be incorporated in the network at a point where from all traffic is entering and exiting the network. The IDPS should be capable to spot on the traces of attack in the system. The attackers are getting more and more knowledgeable nowadays, hence adopting intelligent techniques to attack the network, accordingly the IDPS system should have capabilities to trace wide range of attacks. There can be certain ways adopted by the IDS to intimate about the presence of malicious traffic including logging, generation of alert as message or email to the system administrator etc. The IPS in addition to generating alert will also stop the attack by blocking the traffic from the malicious source or blocking certain type of traffic. The setting of threshold for taking a certain decision by the IDPS is very critical. IDPS is particularly implemented for entire network at critical points, whereas same technique can be employed on certain hosts / end systems or server machines in the form of Host Intrusion Protection System (HIPS). HIPS monitors all traffic, to identify malicious code, associated with the client only on which it is installed.

3.2.5.2 Access to System Logs

Any malicious traffic should not only be blocked but there should be a mechanism to store all malicious traffic with necessary details to assist in tracking later on [10]. The timestamp is very critical among the details to be stored in the log entries. Entries of the log file are very sensitive to the time synchronization element. Correlation of logs cannot be done correctly without precise time synchronization of devices. The client should be given access by the CSP to look into the stored logs at any point of time in order to track down certain incident. The investigation or forensic activity cannot produce any fruitful results without access to the system logs. The details associated with the logs of incident should be sufficient to trace the originator of the incident from certain device / internet protocol (IP) address at the actual time [14]. Logs should be stored with certain severity level and displayed in order of priority basing on severity level of the incident. The severity levels of log entries will help to achieve optimum utilization of logs. The protection of log file from deletion and modification needs to be ensured.

3.2.5.3 Monitoring System

The monitoring system should include monitoring of all the traffic entering and exiting the network. Monitoring of traffic is aimed to ensure that the flow of traffic across the network remains regulated and anomalies, if any, are identified instantly. The monitoring should be carried out primarily on the ingress and egress traffic point. Monitoring of employees of the organization is also critical in this context. A unified security management system is preferable to work on the entire network to have centralized management of all the networking devices and end hosts / machines. The unified system performs centralized logging, correlation of information from different resources and is capable of generating precise reports of the security events.

3.2.5.4 Security Audit

A security audit in an organization is always helpful to measure the on ground implementation and analyze the effectiveness of the proposed security controls. Security audit should be held regularly and periodically as it is the only criteria that can help to evaluate the implementation and efficacy of the security policies for the organization in the cloud environment. The security audit highlights if there are any vulnerabilities in the security system so action can be taken to eliminate the security loop holes in the cloud architecture. The security audit should be conducted on the entire network including most of the networking devices, server machines and host systems. Feedback of the audit is critical to bring improvement in the security of the organization.

3.3 Summary

The proposed security and management framework has been described in this chapter. The discussion starts with introduction to the conceptual framework proposed that consists of five main levels. Each tier is described in detail later on including various parameters that are part of each layer.

Chapter 4

IMPLEMENTATION AND ANALYSIS OF PROPOSED SECURITY AND MANAGEMENT FRAMEWORK

4.1 Introduction

A setup of virtualized environment was deployed, as pre requisite base for deployment of cloud architecture. The proposed security and management framework was implemented on top of the virtualized environment as proof of concept (PoC). Two physical machines / servers of Huawei RH series (RH2288H V2), each having two 2.5 GHz processors and 128 GB RAM, were configured as hypervisor with ESXi-6. An ESXi server is a hypervisor that actually provides an abstraction layer of hardware for the purpose of virtualization. Certain VMs were installed on each of these host servers / nodes. A centralized management suite of vCenter-6 appliance was installed on another windows VM for the purpose of management of both host server machines and all the VMs. The storage was provided to all the virtual machines primarily from a centralized storage on the network (SAN), although the storage from server machines was also available and could be used for certain VMs.

The virtualized datacenter may comprise of certain VMs including management server, database instance, windows active directory component and various application / web servers. vCloud-6 suite was installed on VMs as the cloud architecture for PoC. The deployment of vCloud-6 in the environment included installation of Identity appliance – Single Sign On (SSO), vRealize Automation center and IaaS component. The NMS tools in the virtualized cloud environment was implemented as vRealize Operation Manager (vROM). The vROM centrally monitors all the server machines, VMs and vCloud-6 appliance suite. The centralized monitoring and reporting is a remarkable feature of the vROM that eliminates need of some other monitoring system in the environment. The deployment of the complete virtualized cloud environment is shown as in Fig 4.1. under: -

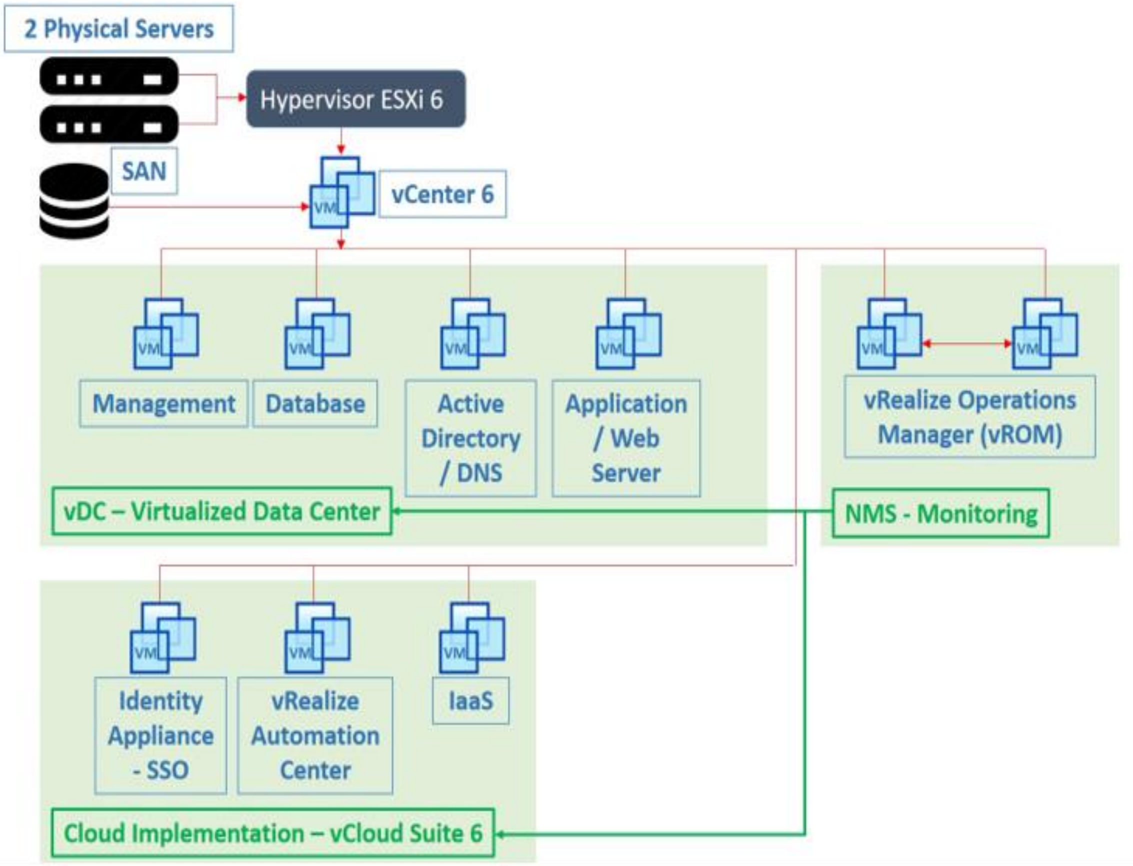
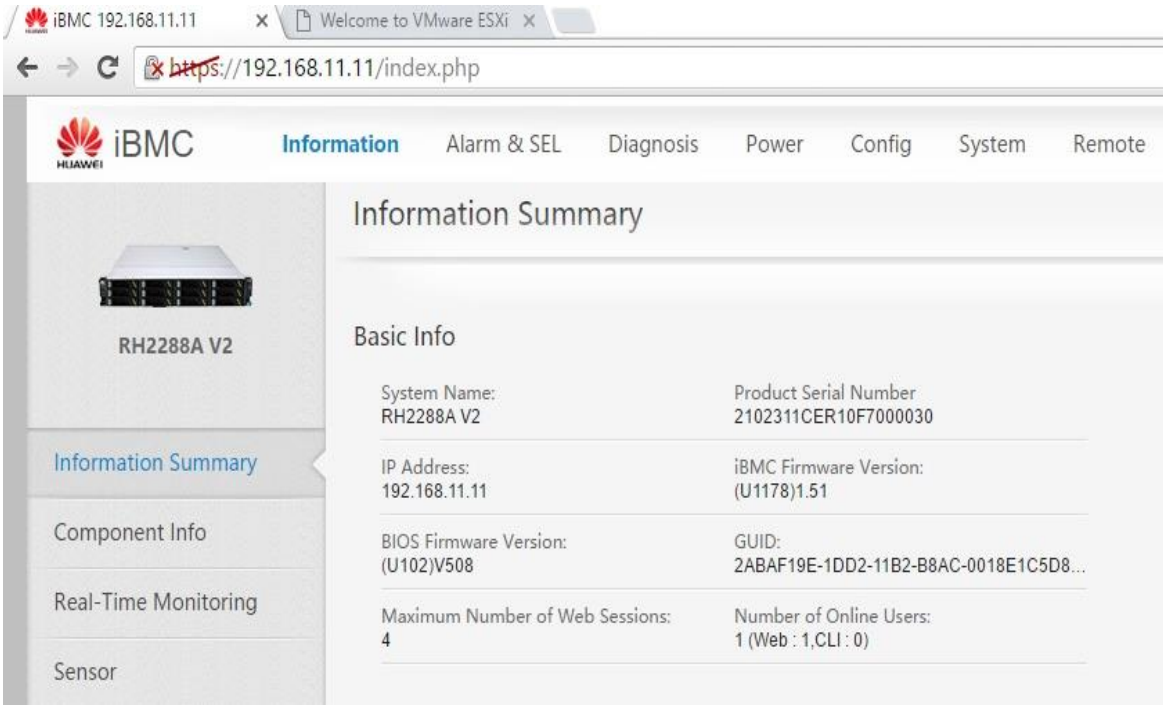


Fig-4.1. Overview of Virtualized Cloud Environment Architecture

4.2 Virtualized Environment Setup

VMware ESXi-6 has been installed as hypervisor in the virtualized environment on 2 server machines (Fig. 4.2.a), each physical machine with 2 processors having processing speed of 2.5 GHz, having 4 Cores per socket and support of multiple (8) logical processors, as shown in Fig. 4.2.b. A cluster was established comprising of these ESXi-6 machines to achieve redundancy at physical level. The feature of redundancy and HA at the hardware layer is a magnificent feature that helps achieve highest level of availability in the provisioning of services to the cloud customer.



Information Summary

Basic Info

System Name: RH2288A V2

Product Serial Number 2102311CER10F7000030

IP Address: 192.168.11.11

iBMC Firmware Version: (U1178)1.51

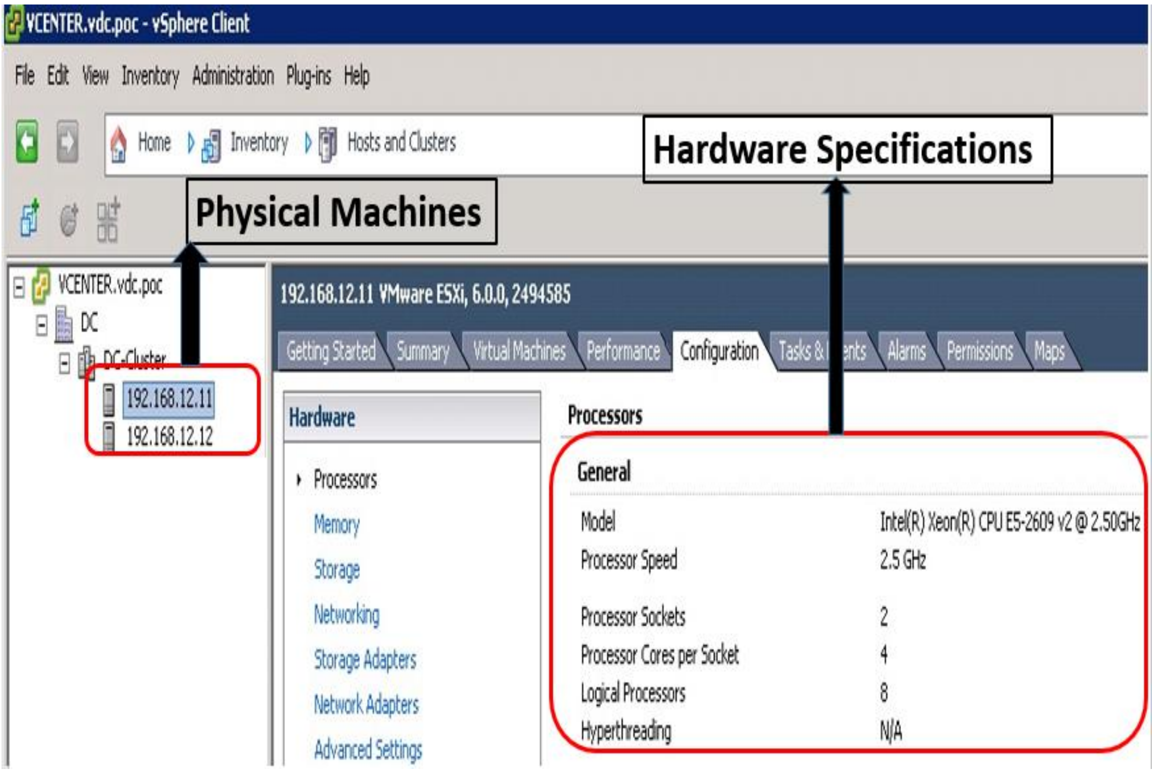
BIOS Firmware Version: (U102)V508

GUID: 2ABAF19E-1DD2-11B2-B8AC-0018E1C5D8...

Maximum Number of Web Sessions: 4

Number of Online Users: 1 (Web : 1,CLI : 0)

Fig-4.2. a. Hardware Details for Virtualized Environment



Processors

General

Model	Intel(R) Xeon(R) CPU E5-2609 v2 @ 2.50GHz
Processor Speed	2.5 GHz
Processor Sockets	2
Processor Cores per Socket	4
Logical Processors	8
Hyperthreading	N/A

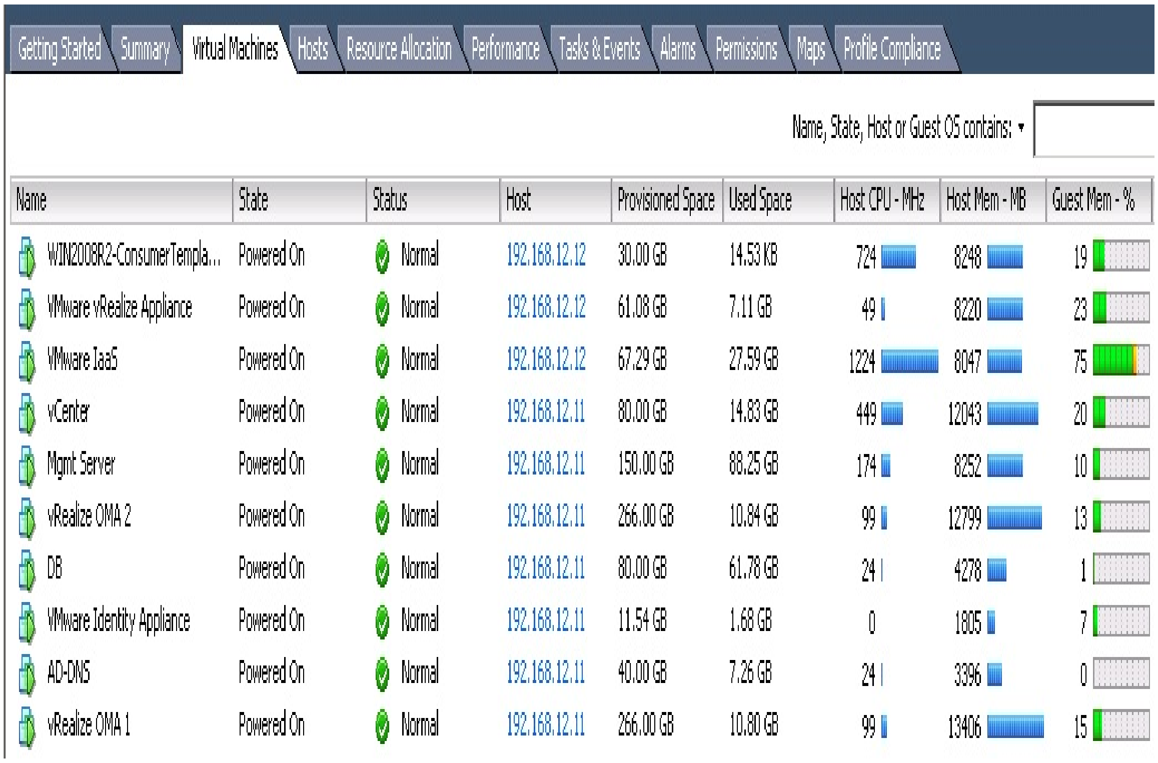
Fig-4.2. b. Specifications of Servers installed with ESXi-6

The subnet used for IP addressing of machines / devices in virtualized environment was selected from the range of private IP addresses, the specific subnet used was 192.168.0.0/16. Different subnets were used for each type of devices / VMs and segregated VLAN ID was assigned to each of them for segregation of traffic. Separate VLANs used to maintain traffic segregation among various subnets at data link layer. VLANs also help to reduce broadcast and collision domain at data link layer. IP addressing scheme used for the virtualized environment is as shown in Table 4.1 as under: -

Subnet	**Machines**	**VLAN ID**
192.168.10.0/24	Management server / machine	10
192.168.11.0/24	ILOM	11
192.168.12.0/24	ESXi-6 Servers	12
192.168.13.0/24	AD	13
192.168.14.0/24	Windows Machines, vCenter-6, vCloud-6	14
192.168.15.0/24	Consumer VMs	15
192.168.16.0/24	DB	16
192.168.17.0/24	SAN	17

Table 4.1 IP addressing scheme used for Virtualized Environment – Proof of Concept

While establishing virtualized environment for PoC, a Datacenter setup was established first of all comprising of various VMs on two physical machines. Certain VMs deployed as part of Datacenter included Windows 2008 Server machines Management server, Database machine (DB), Active Directory component of Windows Operating System (OS), vCenter appliance for management of server nodes and all VMs, Consumer template machine and vRealize Operation Manger appliance to play role of NMS. RAID was implemented at each server machine level. Storage was made available from SAN for all VMs. The status of VMs including the host server machine from which it is getting processing resources at a particular point of time, available / utilized storage and performance metrics are all available for view centrally as shown in Fig. 4.3a, whereas usage of processor on each VM can be seen in Fig 4.3.b as under: -



Name	State	Status	Host	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB	Guest Mem - %
WIN2008R2-ConsumerTempla...	Powered On	✓ Normal	192.168.12.12	30.00 GB	14.53 KB	724	8248	19
VMware vRealize Appliance	Powered On	✓ Normal	192.168.12.12	61.08 GB	7.11 GB	49	8220	23
VMware IaaS	Powered On	✓ Normal	192.168.12.12	67.29 GB	27.59 GB	1224	8047	75
vCenter	Powered On	✓ Normal	192.168.12.11	80.00 GB	14.83 GB	449	12043	20
Mgmt Server	Powered On	✓ Normal	192.168.12.11	150.00 GB	88.25 GB	174	8252	10
vRealize OMA 2	Powered On	✓ Normal	192.168.12.11	266.00 GB	10.84 GB	99	12799	13
DB	Powered On	✓ Normal	192.168.12.11	80.00 GB	61.78 GB	24	4278	1
VMware Identity Appliance	Powered On	✓ Normal	192.168.12.11	11.54 GB	1.68 GB	0	1805	7
AD-DNS	Powered On	✓ Normal	192.168.12.11	40.00 GB	7.26 GB	24	3396	0
vRealize OMA 1	Powered On	✓ Normal	192.168.12.11	266.00 GB	10.80 GB	99	13406	15

Fig-4.3. a. Virtual Machines Status

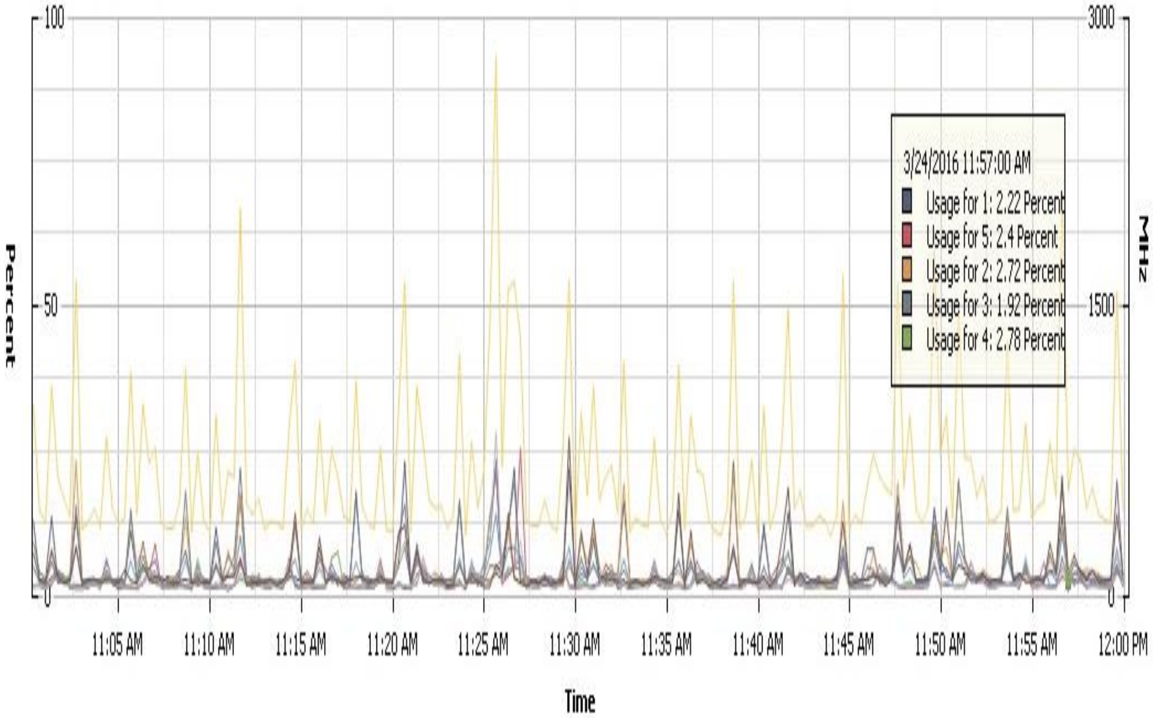


Fig-4.3. b. Virtual Machines Processor Usage Statistics

The centralized management appliance for the entire cluster including multiple server machines / ESXi hosts and all VMs is vCenter-6. A vSphere Client (installed on a windows machine / VM) or vSphere Web Client (browser based interface) can be used to access the vCenter management suite through which further all the ESXi servers connected in the network are accessible and can be managed conveniently. vCenter-6 was installed on a dedicated VM as shown in Fig. 4.4: -

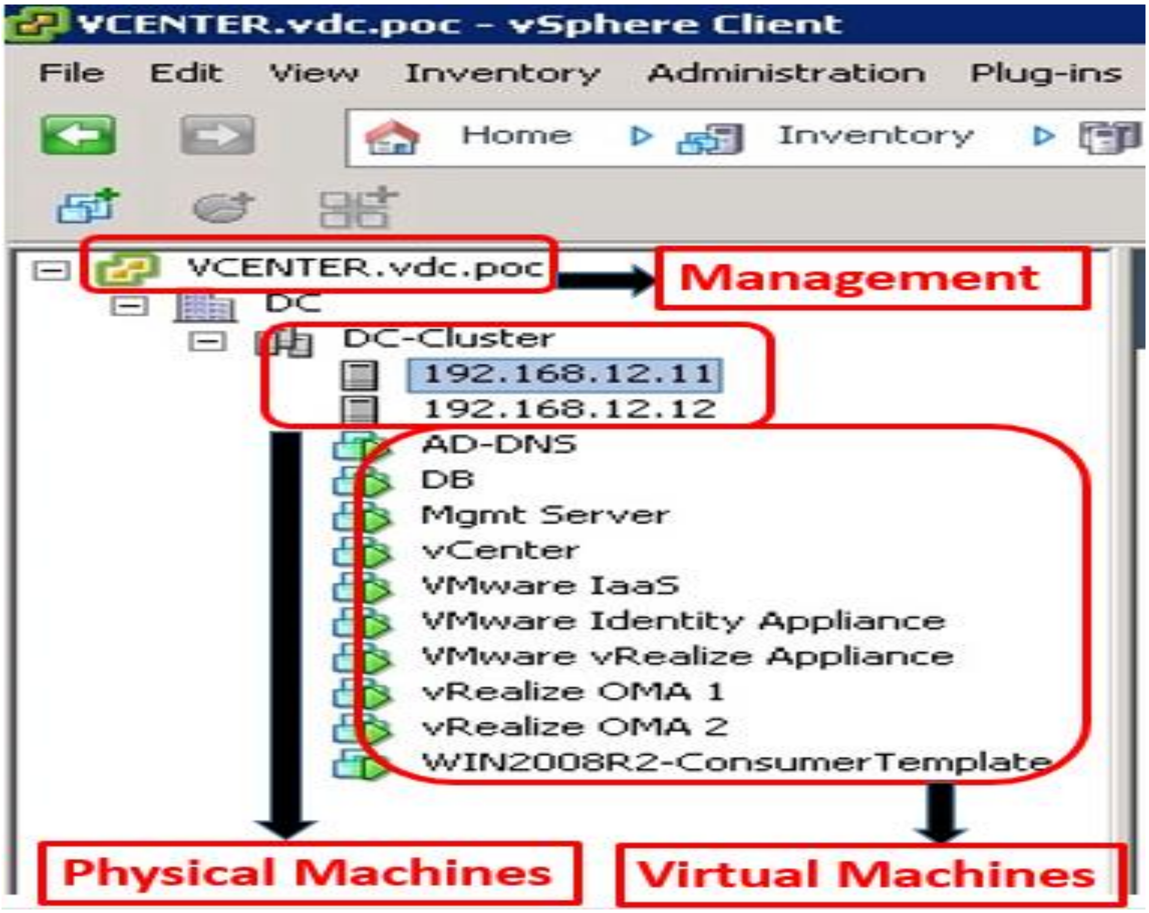
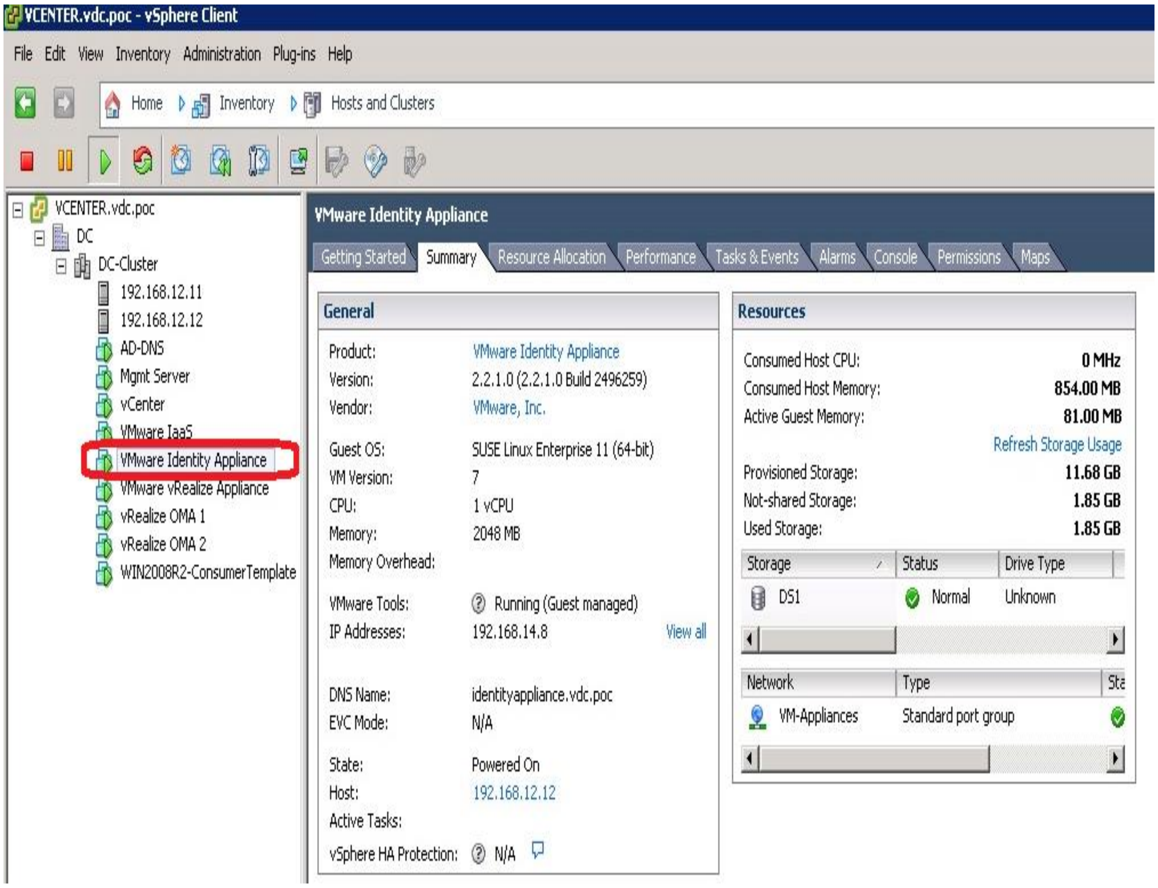


Fig-4.4. vCenter Appliance for VMs Management

4.3 Cloud Deployment

The deployment of cloud environment required development of a virtualized environment as a pre requisite (already covered in previous section). vCloud-6 was installed as cloud architecture to provide services to its users. vCloud-6 is not a single VM or appliance, it’s a complete suite containing various integrated components. The remarkable improvement in efficiency and responsiveness of provision of services for the client are prime features of virtualized cloud. The installation phase of vCloud-6 deployment, after prior installation of ESXi servers and vCenter server / appliance to manage them, included deployment of VMware Identity Appliance and vRealize Appliance for further installation of vCloud IaaS architecture on it. VMware Identity Appliance is a virtual machine, as shown in Fig 4.5, that has been installed as a virtual appliance.



General

Product: VMware Identity Appliance
Version: 2.2.1.0 (2.2.1.0 Build 2496259)
Vendor: VMware, Inc.

Guest OS: SUSE Linux Enterprise 11 (64-bit)
VM Version: 7
CPU: 1 vCPU
Memory: 2048 MB
Memory Overhead:

VMware Tools: Running (Guest managed)
IP Addresses: 192.168.14.8

DNS Name: identityappliance.vdc.poc
EVC Mode: N/A

State: Powered On
Host: 192.168.12.12
Active Tasks:
vSphere HA Protection: N/A

Resources

Consumed Host CPU: 0 MHz
Consumed Host Memory: 854.00 MB
Active Guest Memory: 81.00 MB

Provisioned Storage: 11.68 GB
Not-shared Storage: 1.85 GB
Used Storage: 1.85 GB

Storage	Status	Drive Type
DS1	Normal	Unknown

Network	Type	Sta
VM-Appliances	Standard port group	✓

Fig-4.5. VMware Identity Appliance

VMware vRealize Appliance supports installation of IaaS cloud installation features as shown in Fig. 4.6.a. The administrators gain access to the system through vRealize automation center for the purpose of managing cloud IT resources. The administrators of the cloud can create catalogs of services or resources, to be provided to the cloud clients, and maintain them. Different users on cloud have different roles and different access rights on to the resources. Certain templates of services to be provided for the user were created that could be provided to cloud user on his request, e.g. consumer template machine of Windows OS is ready to be made available to the client in the cloud environment, as shown in Fig. 4.6.b: -

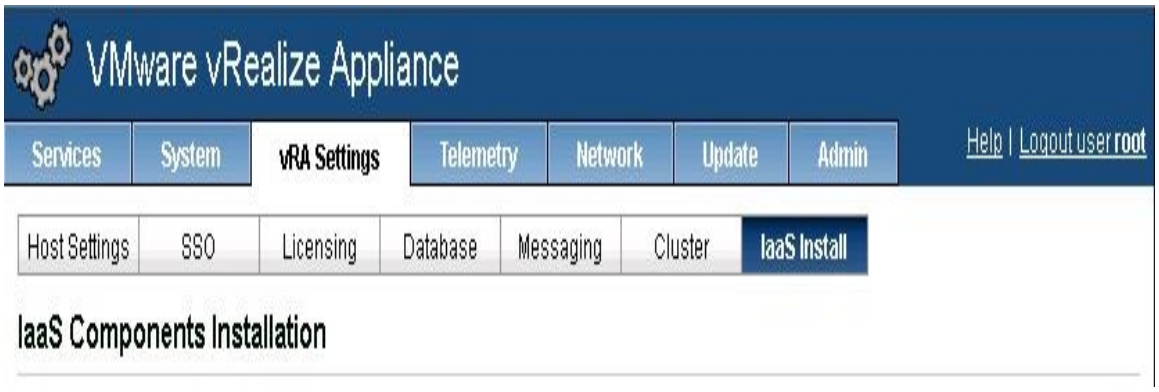
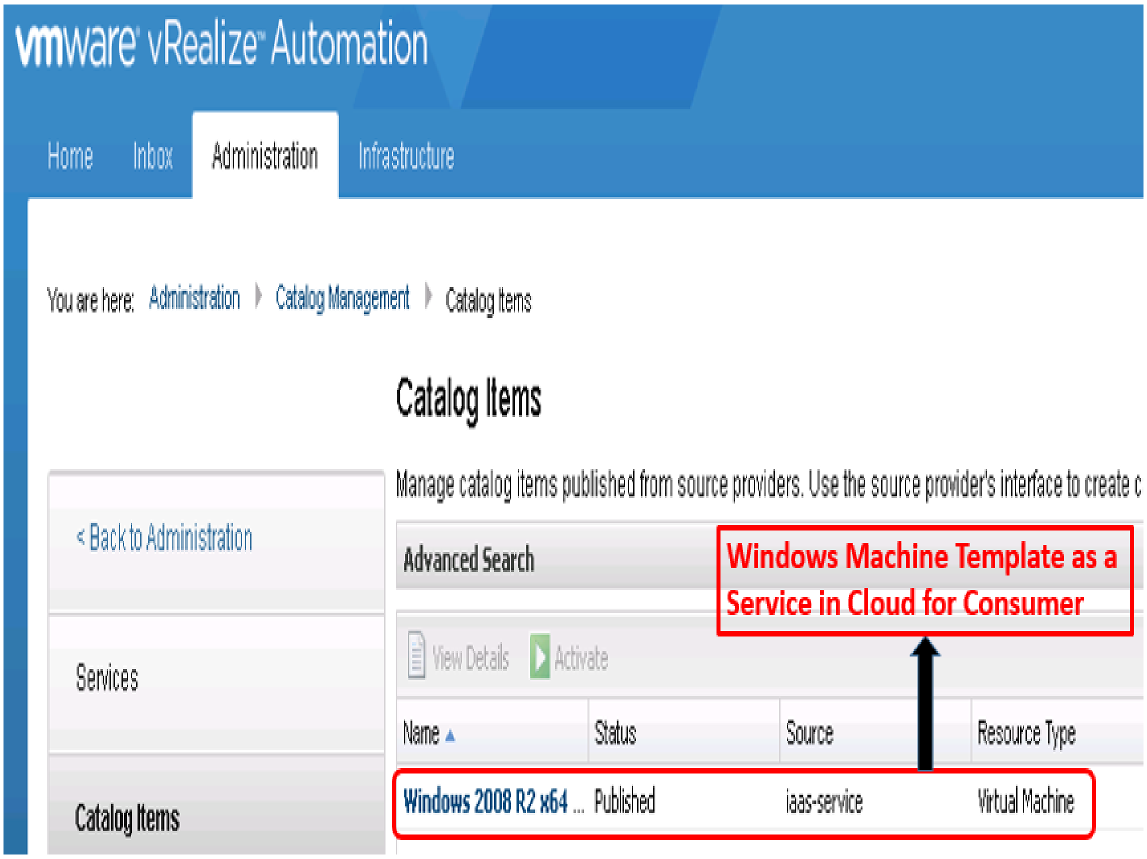


Fig-4.6. a. VMware vRealize IaaS Installation



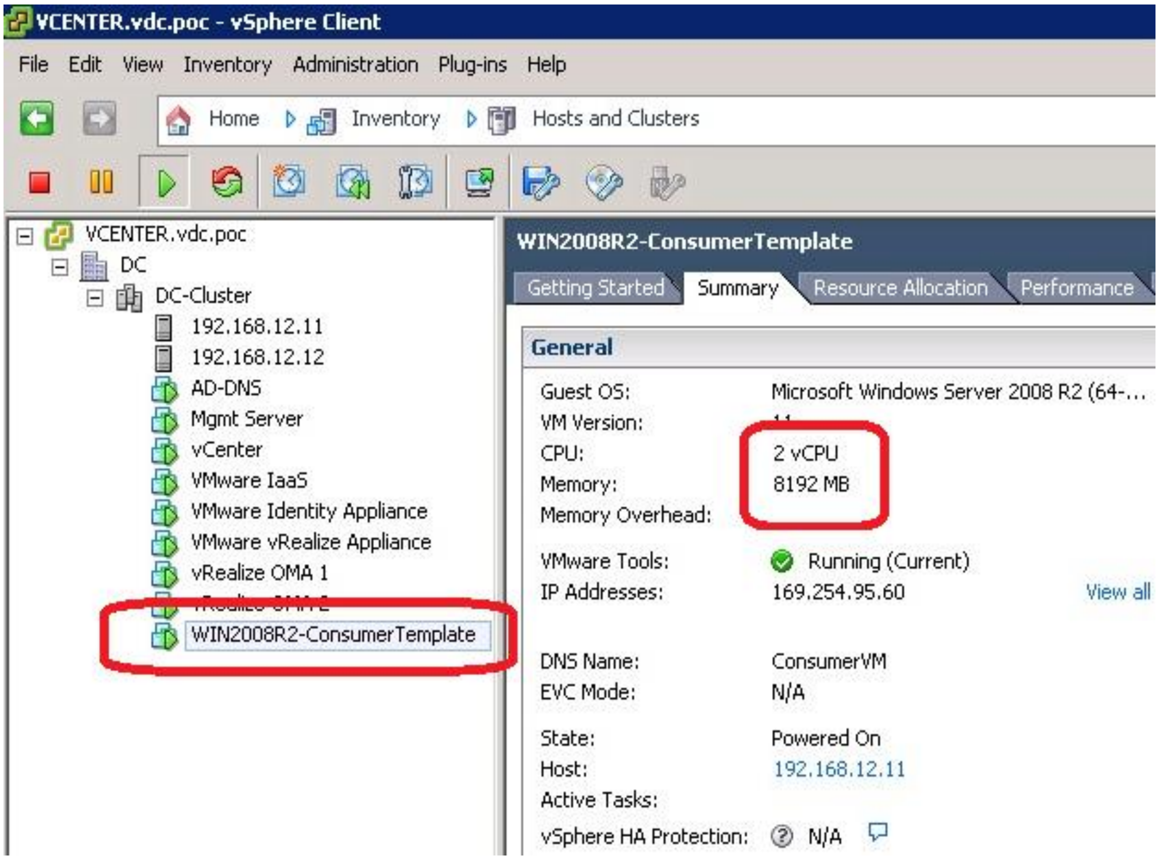
Manage catalog items published from source providers. Use the source provider's interface to create c

Name ▲	Status	Source	Resource Type
Windows 2008 R2 x64 ...	Published	iaas-service	Virtual Machine

Windows Machine Template as a Service in Cloud for Consumer

Fig-4.6. b. Catalog Items Template for Virtual Machine

The consumer template is a VM in the virtualized environment of the PoC which has been assigned with certain resources (2 CPUs and 8 GB RAM in this case). The consumer template can be provided to an authorized user of the cloud architecture as a VM resource on his request for service provisioning. The consumer template VM in the virtualized environment is as shown in Fig-4.7: -



WIN2008R2-ConsumerTemplate

General

Guest OS: Microsoft Windows Server 2008 R2 (64-…
VM Version: 11
CPU: 2 vCPU
Memory: 8192 MB
Memory Overhead:

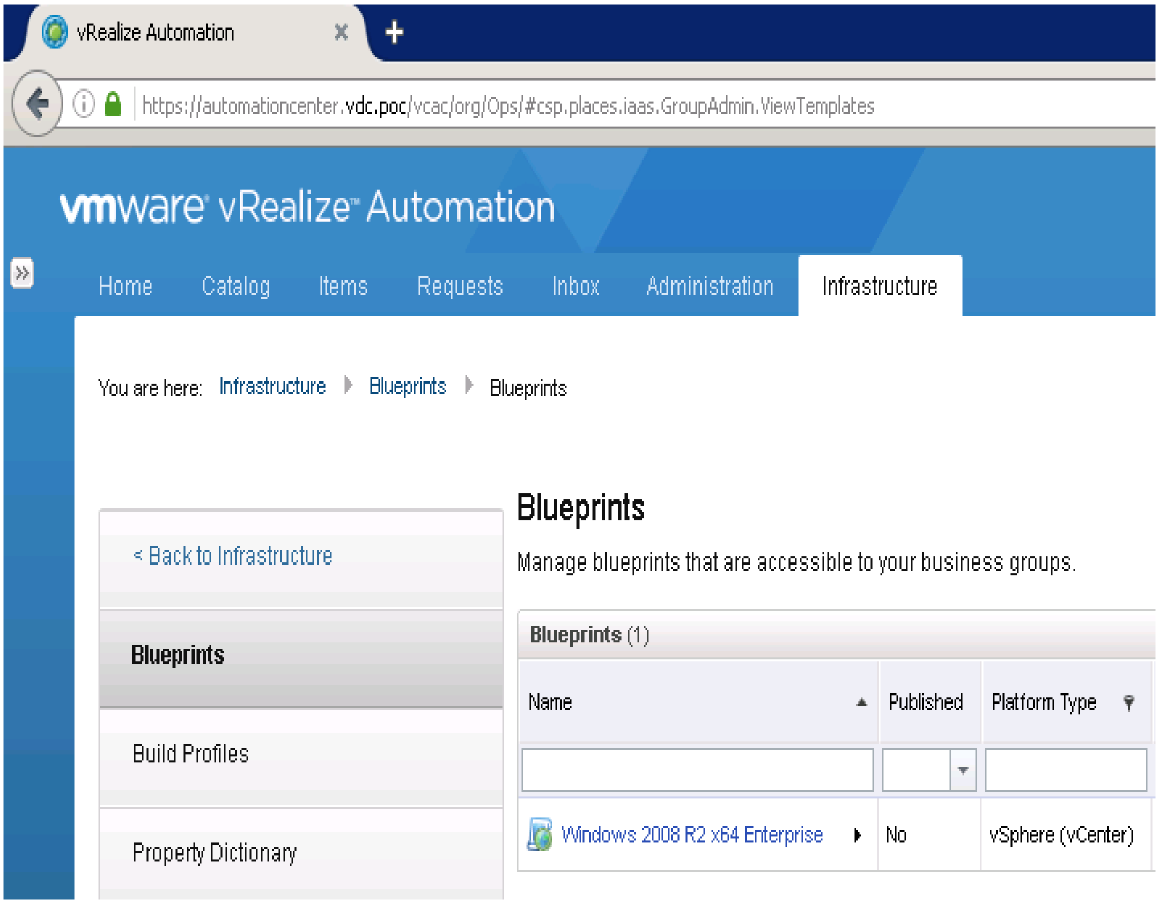
VMware Tools: Running (Current)
IP Addresses: 169.254.95.60

DNS Name: ConsumerVM
EVC Mode: N/A

State: Powered On
Host: 192.168.12.11
Active Tasks:
vSphere HA Protection: N/A

Fig-4.7. Virtual Machine Consumer Template

The consumer template is a blue print now that will be used later for provision as a service to the client as shown in Fig. 4.8. The administrator can manage this blueprint as an infrastructure using certain settings like for how many days this machine will be leased to the user / client, if it can be further copied or not etc.



https://automationcenter.vdc.poc/vcac/org/Ops/#csp.places.iaas.GroupAdmin.ViewTemplates

You are here: Infrastructure ▸ Blueprints ▸ Blueprints

Blueprints

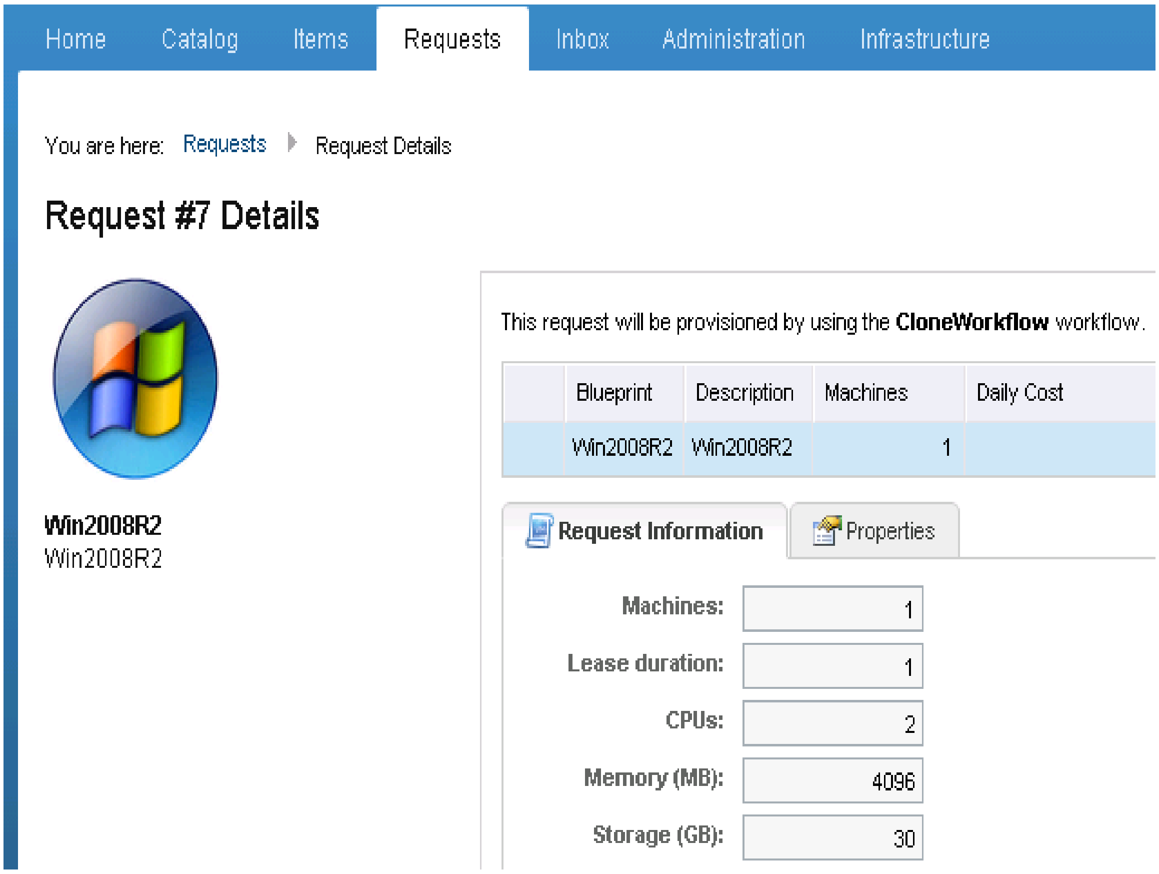
Manage blueprints that are accessible to your business groups.

Blueprints (1)

Name	Published	Platform Type
Windows 2008 R2 x64 Enterprise	No	vSphere (vCenter)

Fig-4.8. Virtual Machine Infrastructure Blueprint

The client / user of cloud services can request provision of VM Windows 2008 server machine (or any other VM if available as template in the service catalog). The administrator allows the client of the cloud to customize his requirements, while requesting for provisioning of services, including number of machines, duration of lease, processing and storage details. The lease duration implies for how long the machine will remain usable for the client of cloud model. At the termination of lease model, the VM machines provided to the client will expire and will not be usable any longer. The machine will be provided from the already available VM template on request of client as shown in Fig 4.9 as under: -



Request #7 Details

Win2008R2
Win2008R2

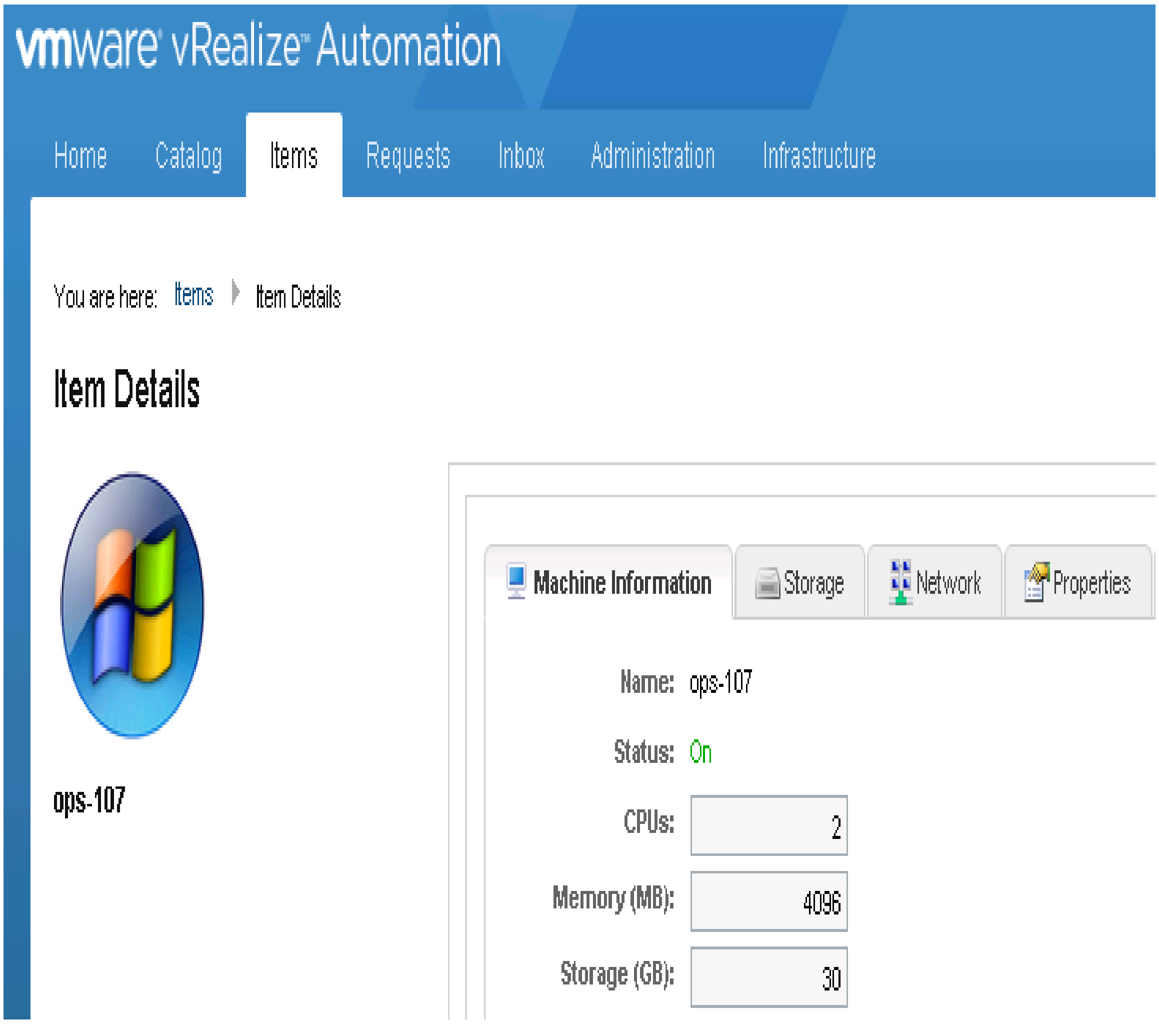
This request will be provisioned by using the **CloneWorkflow** workflow.

	Blueprint	Description	Machines	Daily Cost
	Win2008R2	Win2008R2	1	

Machines:	1
Lease duration:	1
CPUs:	2
Memory (MB):	4096
Storage (GB):	30

Fig-4.9 Client's Request for consumer Virtual Machine Template

The windows machine requested by client is now ready to be used as shown in Fig-4.10 and can be connected by the client. Certain configurations can be done on the VM by the administrator including setting up number of CPUs allotted to the template machine, RAM assigned for usage, storage allocated on the VM for the client with the template and specific network settings. Once the machine is ready and available, the client can access the machine through console or remote desktop connection.



Item Details

ops-107

Name: ops-107

Status: On

CPUs: 2

Memory (MB): 4096

Storage (GB): 30

Fig-4.10 Virtual Machine Configurations

The requirement of NMS suite in the cloud architecture for all VMs / appliances has been fulfilled by vROM appliance. The appliance enables provision of health and connectivity status for all the appliances and VMs on the network. vRealize Operation Manager acts as NMS for cloud environment. It provides functionality to monitor health status, processor usage, memory usage status, heat map and various other important performance and usage metrics for server nodes and VMs graphically shown in Fig. 4.11.a and statistically shown in Fig. 4.11.b as under. The views can also be customized as per requirements of client.

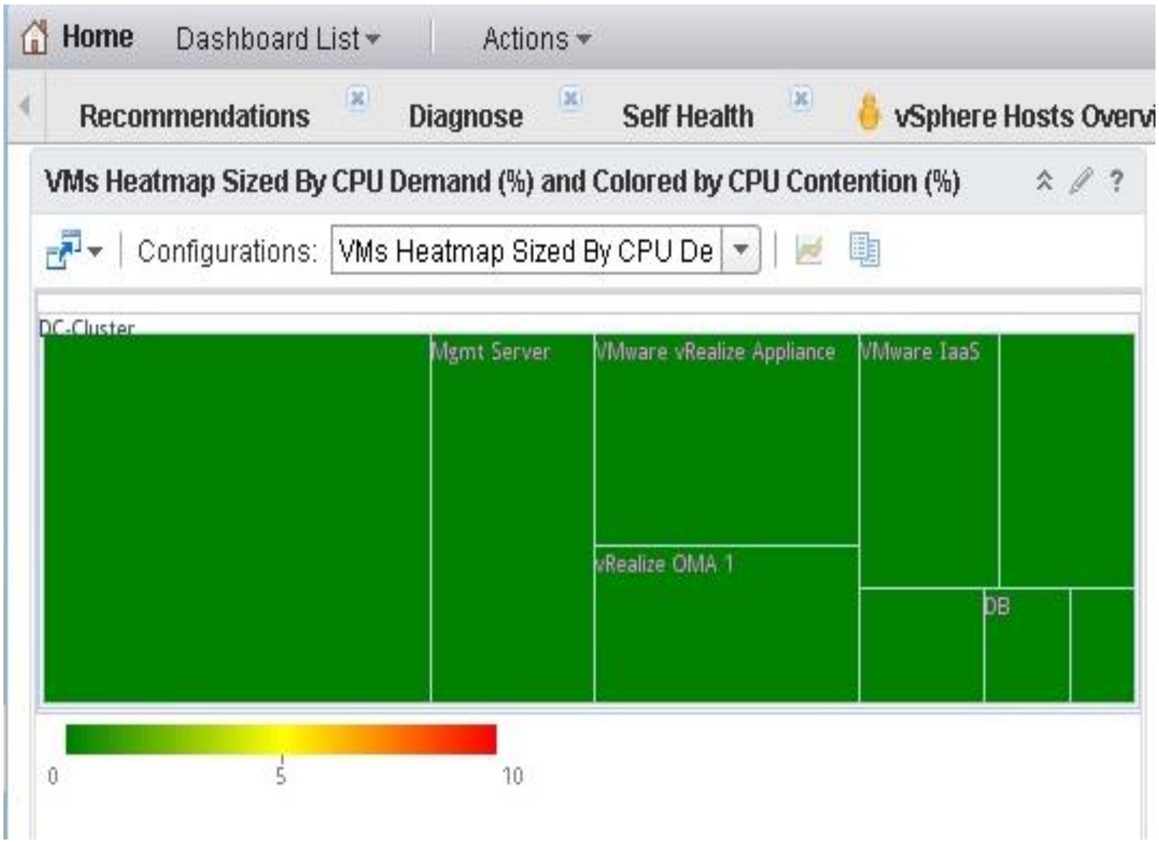
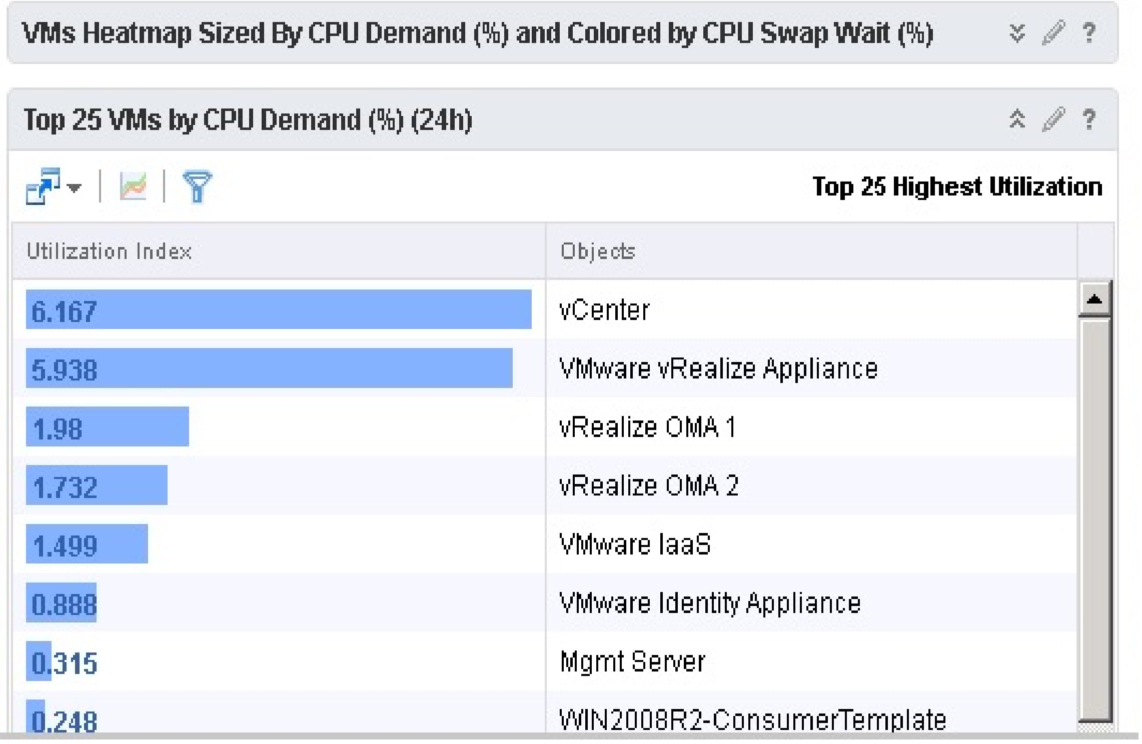

Home
Dashboard List
Actions
Recommendations
Diagnose
Self Health
vSphere Hosts Overvi
VMs Heatmap Sized By CPU Demand (%) and Colored by CPU Contention (%)
Configurations: VMs Heatmap Sized By CPU De
DC-Cluster
Mgmt Server
VMware vRealize Appliance
VMware IaaS
vRealize OMA 1
DB
0
5
10

Fig-4.11. a. vRealize Operation Manager Graphical View


VMs Heatmap Sized By CPU Demand (%) and Colored by CPU Swap Wait (%)
Top 25 VMs by CPU Demand (%) (24h)
Top 25 Highest Utilization

Utilization Index	Objects
6.167	vCenter
5.938	VMware vRealize Appliance
1.98	vRealize OMA 1
1.732	vRealize OMA 2
1.499	VMware IaaS
0.888	VMware Identity Appliance
0.315	Mgmt Server
0.248	WIN2008R2-ConsumerTemplate

Fig-4.11. b. vRealize Operation Manager Statistical View

4.4 Analysis of Proposed Security Framework

The security and management framework proposed in the preceding sections has been analyzed to validate the effectiveness of the framework. This framework provides a set of baseline security measures to be ensured by a sensitive organization that is operating in cloud environment. All key security threats and risks will be properly handled by adoption of the proposed framework in the organization. The organization should adopt all these security measures as a strategic policy once it has decided to adopt the cloud architecture for its future working. The essential security baseline proposed in the framework serves as a checklist for the sensitive organization to operate in cloud model. The implementation of the framework is in certain phases including its implementation on the physical server machines followed by implementation on virtualized environment of cloud architecture. Fig. 4.12.a depicts implementation of the proposed framework along with legends used as shown under in the Fig. 4.12.b: -

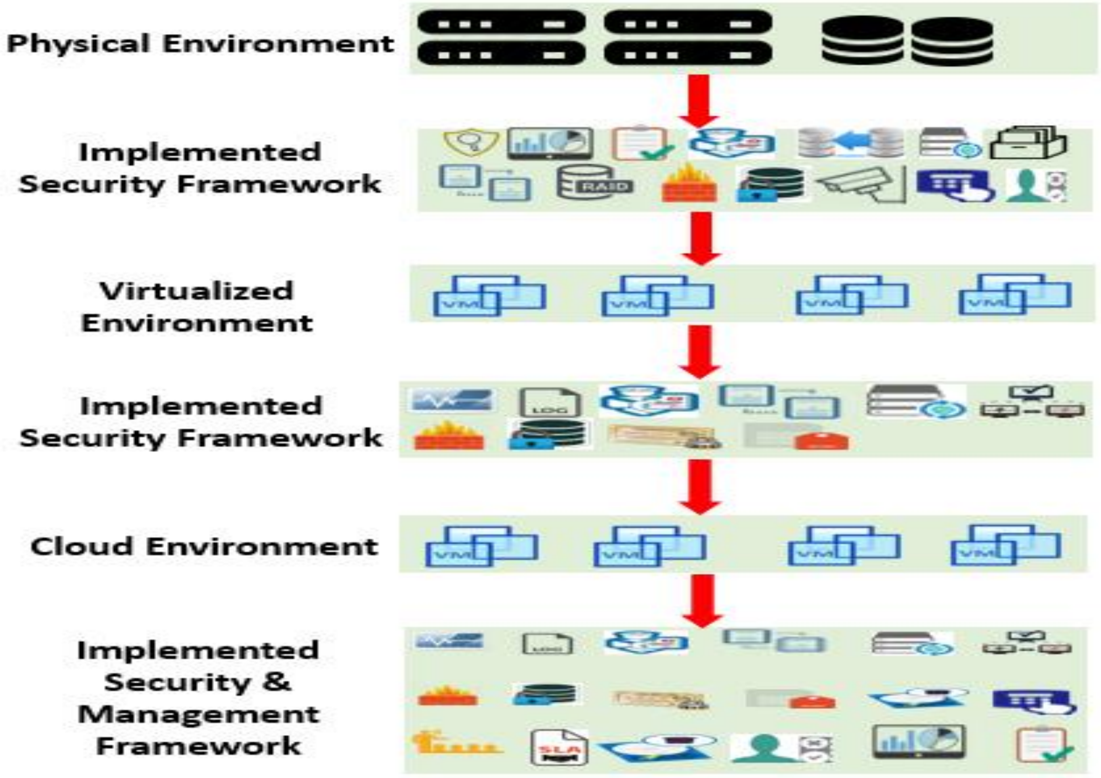

Physical Environment
Implemented Security Framework
Virtualized Environment
Implemented Security Framework
Cloud Environment
Implemented Security & Management Framework

Fig-4.12. a Security and Management Framework implementation

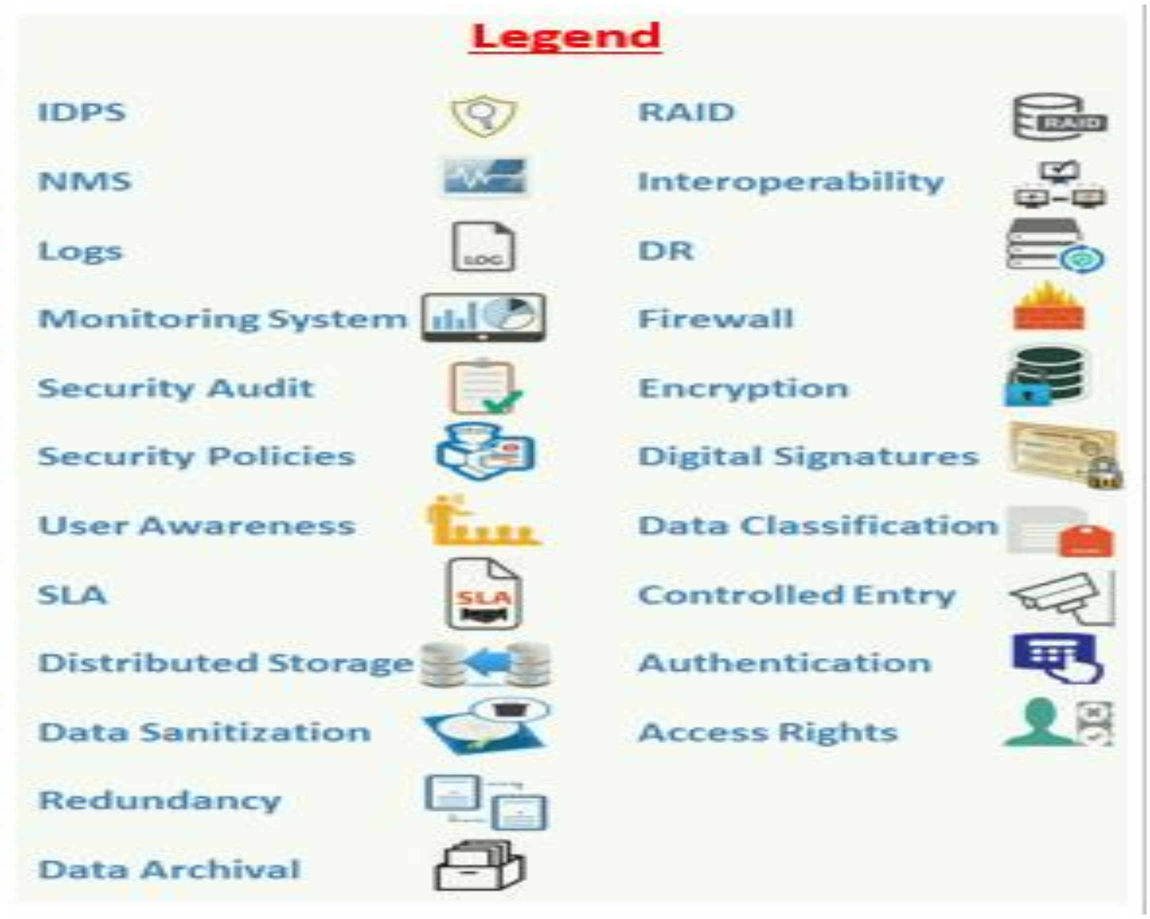


Fig-4.12. b Legends for security and management framework

Virtualized environment itself has certain key advantages including economy of resources in design, implementation and maintenance phase. The flexible control on IT resources is a substantial feature of virtualization. Virtualization, owing to its revolutionized features and capabilities, is future of the IT and particularly virtualized cloud is the direction the technologists are moving owing to its magnificent benefits.

4.5 **Summary**

In this chapter, Implementation phase for the deployment of vCloud was covered. Complete process of environment development including hardware and software details has been discussed and summarized. The discussion starts from installation of VMware hypervisor ESXi-6 on bare metal hardware (two server machines) followed by creation of an entire Datacenter including two server machines as nodes of cluster. The cluster architecture was used to achieve redundancy and high availability features in the system. Certain VMs were built on top of which various cloud and its management components are installed. vCenter-6 was installed for centralized management and control of the entire hardware nodes and numerous VMs. vCloud-6 was installed as cloud model and vROM deployment was meant to work as NMS. Various security and management features of the proposed framework were deployed during the installation of the cloud architecture.

Chapter 5

COMPARISON OF PROPOSED FRAMEWORK WITH INDUSTRY STANDARDS

5.1 Introduction

The proposed framework for security and management of cloud will be compared with certain frameworks / guidelines / security architectures suggested by few internationally well recognized standard bodies. The aim of these organizations is to provide a road map to facilitate the client and the CSP by securing the cloud services for the clients. All stakeholders have to play their role in cloud computing environment in context of security and management of the cloud model. The standard bodies or agencies have formulated certain reference framework for the cloud architecture to help clients and CSP in realizing and following their roles and duties. The client, in adoption of cloud environment in his organization, can follow and fulfill the security requirements to the extent the model adopted allows him to do so.

A thorough understanding of the mechanism that various cloud models follow, in deployment and inter model communication, will be helpful to understand the threats, vulnerabilities, weaknesses in the cloud model and also to identify the risks associated with the adoption of cloud model. Although only client cannot be exclusively held responsible for entire security of the cloud, however it is client who should indicate what security controls are essential and ensure that CSP is implementing the desired or agreed security controls on the cloud architecture. In this section, the proposed framework has been studied in line with the security frameworks for cloud environment proposed by CSCC, ISO/IEC and PCI-DSS.

5.2 CSCC

The CSCC (Cloud Standards Customer Council) is an organization that is working to present standards that can help customers to adopt the cloud model. The organization facilitates clients by formulating their requirements into standards and guides them in the form of documents containing best practices to be followed while adopting the cloud model. CSCC has presented a security standard highlighting the requirements of information security relevant to the deployment of cloud model, focusing on salient concerns that a client should expect or negotiate in cloud model [39]. There are certain types of standards including advisory standards, security frameworks and standards specifications. Advisory standards highlight controls that are applicable to most of the organizations. Security frameworks can be referred as best practices for an organization that helps client to ensure adaptation in light of certain security policies through some procedures or check lists. Standard specifications are the security standards that needs to be implemented to follow a certain standard. There are certain key elements that can help clients in evaluating the security standard adopted by their organization in cloud environment [39]. It is essential to ensure that following features exists in the cloud environment: -

- Essential processes for good governance, risk management
- Audit of processes
- Management of individuals, their roles and user identities
- Data protection
- Policies regarding privacy of users
- Applications security
- Network security
- Physical security

- SLA covering security
- Requirements of exit

5.3 ISO / IEC

The ISO has collaborated with IEC with an aim to present standards in the field of IT. ISO/IEC 27017 is a security framework for cloud architecture proposed by a joint technical committee formed by ISO and IEC that worked in collaboration with ITU-T. ISO/IEC 27018, an extension of ISO/IEC 27017, provides a framework as a set of security controls for the cloud environment to protect its client's or organizational data [40]. The guidelines and security controls are generally applicable to the public model of cloud deployment. The security controls in the framework assist the client on various issues particularly including physical security of the environment, user authentication, access rights, data protection, data backup, confidentiality matters, logging and monitoring. The document describes how policies regarding information security are applicable to the data protection. There are certain responsibilities of the CSP and its subcontractors regarding protection of client's data in relevance to the respective cloud service model. The document assists the client to understand the segregation of roles and responsibilities of the client and the CSP to secure the cloud environment and suggests the cloud user to follow the specified controls in the organization working under cloud model.

5.4 PCI-DSS

The data of a payment card may be stored in cloud environment, retrieved or processed form there, hence PCI DSS requirements are also concerned with the cloud security parameters. The responsibility of security controls in cloud environment is generally segregated between client and the CSP, however this does not relieve the client from the concern that cloud environment is securing his data in compliance with the requirements highlighted by PCI DSS [41]. There is a requirement to define a distinct framework encompassing clear security and management policies highlighting the responsibilities of client and CSP, that must be mutually agreed between both as a prerequisite. The PCI Security Standards Council has issued / published “Information Supplement: PCI DSS Cloud Computing Guidelines” [41], as a framework on cloud security to work as baseline for implementation of security controls on card holder data in relevance to PCI DSS requirements. The document presents essential guidelines for the client and CSP working in cloud environment in the light of security controls relevant to PCI DSS. The guidelines are specific to the users and CSP of cloud environment that are concerned with the card data storage, transmission or processing.

There may be a possibility that at a certain layer where CSP will be held responsible in cloud environment for security of data and applications, but still client should not remain absolutely isolated, instead has to be aware and in position to negotiate on security controls as per his specific requirement. Further in case of card data handling, client has to get involved at a larger scale in the CSP domain of finalizing and implementing security controls in cloud environment. Requirements of PCI DSS are to be viewed under the scope of specific cloud service model and then assigned to either of client or CSP. The outlining of roles and responsibilities between CSP and client for PCI DSS controls management relies generally on certain factors [41], briefly highlighted as under: -

- Client’s purpose to acquire services from cloud
- PCI DSS requirements scope being outsourced to CSP by client
- Certain components / services endorsed by CSP in its own operations
- Service model adopted by the client
- Additional security services provided by CSP

5.5 Comparison of Proposed Framework with CSCC, ISO/IEC and PCI-DSS Standards

There are certain security controls and management aspects proposed in the suggested security and management framework. The proposed framework is an entire conceptual charter that is recommended to be followed by an organization who is migrating or functioning in cloud environment. Certain standards bodies including CSCC, ISO/IEC and PCI-DSS have also proposed relevant frameworks or models for security in cloud environment, as discussed in previous section of the thesis. Table 5.1 presents a comparison, drawn among proposed framework and standards offered by CSCC, ISO/IEC and PIC-DSS, by highlighting if a certain feature has been focused by either of standards:-

PROPOSED FRAMEWORK	CSCC	ISO/IEC	PCI-DSS
Controlled Entry	Yes	Yes	Yes
Authentication	Yes	Yes	Yes
Access Rights	Yes	Yes	Yes
Firewall Protection	Yes	Yes	Yes
Encryption	Yes	Yes	Yes
Antimalware Protection	Yes	Yes	Yes
Digital Signatures	No	No	No
Data Classification	No	No	Yes
Distributed Storage	No	No	No
Data Sanitization	No	No	Yes
Redundancy in Critical Resources	Yes	No	Yes
Data Archival	Yes	Yes	Yes
RAID	Yes	Yes	No
Cloud Service Interoperability	Yes	No	No
DR	Yes	Yes	Yes
NMS	No	Yes	Yes
Security Policies	Yes	Yes	Yes
User Awareness	No	No	No
Comprehensive SLA	Yes	No	Yes
IDPS Protection	Yes	Yes	Yes
Access to System Logs	Yes	Yes	Yes
Monitoring System	No	Yes	Yes
Security Audit	Yes	No	Yes

Table 5.1 Comparison of Proposed Framework with CSCC, ISO/IEC and PCI DSS

5.6 Summary

There are certain standard bodies / agencies recognized internationally that present standards, framework or guidelines to be followed by the clients to operate in the cloud environment. These standards work as guidelines for Client and CSP both in handling cloud security and management related issues. In this chapter, the security and management features of the proposed framework in cloud environment have been compared with certain frameworks / standards / guidelines proposed by world known standards including CSCC, ISO/IEC and PCI DSS.

Chapter 6

CONCLUSIONS AND FUTURE WORK

The research has primarily emphasized on identifying security vulnerabilities, threats and challenges faced by users / organizations in cloud environment. Prior to adoption of cloud model by an organization for which sensitivity of data is very critical, a conceptual framework is required to work as security and management guideline. The discussion on privacy and security issues in cloud architecture follows proposing a systematic framework that encompasses both security and management aspects for a sensitive organization that is part of a cloud architecture. Mainly security concerns in cloud owe to the offsite storage of client's data besides certain other reasons. The cloud architecture adoption for a sensitive organization should be aligned with the proposed security framework. The proposed framework is a layered model that incorporates security and management at various tiers. The framework has been presented after thoroughly studying and reviewing security challenges in cloud environment.

The research work is planned to be extended as under: -

- Exploring optimized ways to carry out security audit of data and applications while keeping in view protection of data from the third party from integrity point of view.
- Exploring and Implementing latest techniques of centralized user authentication, e.g. from a RADIUS, be reviewed and integrated in to cloud model to avoid any confidentiality and integrity breech.
- Exploring latest techniques to handle residual data, remnants of data left on storage once the client has deleted the data, particularly in cloud environment.

- Exploring techniques to further optimize efficiency and performance of the architecture on top of proposed security and management framework as the baseline.
- Study and Evaluation of security features provided by certain well recognized international websites and service providers including Amazon, Google, iPhone etc. to their clients.

BIBLOGRAPHY

[1] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing”, IEEE Communications Surveys & Tutorials, Vol 15, No2, Second Quarter, 2013-843.

[2] Boyang Wang, Baochun Li, Hui Li, “Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE Transaction on Cloud Computing, Vol 2, No 1, Jan-Mar 2014.

[3] Daniel W.K. TSE, “Challenges on Privacy and Reliability in Cloud Computing Security”, 978-1-4799-3197-2/14/31 2014 IEEE.

[4] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanosios, Vasilakos, “Security and Privacy for storage and computation in cloud computation”, Elsevier, Information Sciences, 258 (2014).

[5] Mark D.Ryabn, “Cloud Computing Security: The scientific challenge and survey of solutions”, Elsevier, Journal of Systems and Software 86 (2013).

[6] Sara Hamouda, “Security and Privacy in Cloud Computing”, Proceedings of 2012 International Conference on Cloud Computing, Technologies, Applications & Management 978-1-4673-4416-6/12 IEEE, 2012.

[7] Chunming Rong, Son T. Nguyen, Martin Gilje Jaatun, “Beyond Lightning: A Survey on Security Challenges in Cloud Computing”, Elsevier, Computer & Electrical Engineering 39 (2013) 47-54.

[8] Dimitrios Zissis, Dimitrios Lekkas, “Addressing Cloud Computing Security Issues”, Elsevier, Future Generation Computer Systems, 28(2012)583-592.

[9] Mingqi Zhou, Rong Zhang, Wei Xei, Weining Qian, Aoying Zhou, “Security and Privacy in Cloud Computing: A Survey”, 2010 Sixth International Conference on Semantics, Knowledge and Grids.
978-0-7695-4189-1/10, 2010 IEEE.

[10] Abdullah Abuhussein, Harkeerat Bedi, Sajjan Shiva, “Evaluating Security and Security and Privacy in Cloud Computing Services: A Stakeholder’s Perspective”, The 7th International conference for Internet Technology and Secured Transactions (ICTIST-2012), 978-1-908320-08/7, 2012-IEEE.

[11] Deyan Chen, Hong Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, 2012 International Conference on Computer Sciences and Electronics Engineering, 978-0-76954647-6/12, 2012-IEEE.

[12] Farzad Sabahi, “Cloud Computing Security Threats and Responses”, 978-1-61284-486-2/11, 2011-IEEE.

[13] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, Hindawi Publication Corporation, International Journal of Distributed Sensor Networks, Article ID 190903, Volume 2014.

[14] Dawn Song, Elaine Shi, Ian Fischer, “Cloud Data Protection for the Masses”, 0018-9162-/12 – 2012 IEEE.

[15] Ahmad Almulhem, “Network Forensics: Notions and challenges”, Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium, p.463-466, 2009.

[16] Atul Kant Kaushik, Emmanuel S.Pilli, R.C Joshi, “Network Forensic System for Port Scanning Attack”, Advanced Computing Conference (IACC), 2010 IEEE 2nd International, p.310-315-2010.

[17] Stephen Biggs, Stilianos Vidalis, “Cloud Computing: The Impact on Digital Forensics Investigation”, Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference, p. 1-6, 2009.

[18] Hong Guo, Bo Jin, Ting Shang, “Forensics Investigation in Cloud Environments”, 2012 International Conference on Computer Science and Information Processing, 978-1-4673-1411-4/12, 2012 IEEE.

[19] Dominik Birk, Christoph Wegener, “Technical Issues of Forensic Investigations in Cloud Computing Environments”, Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop, p. 1-10, 2011.

[20] Elias Raftopoulos, Xenofontas Dimitropoulos, “Understanding Network Forensic Analysis in an Operational Environment”, SPW ’13 Proceedings of the 2013 IEEE Security and Privacy workshops, p. 111-118, 2013.

[21] Qassim Nasir, Zahra A.Al-Mousa, “Honey pots aiding network forensics: Challenges and Notions”, Journal of Communications Vol 8, No 11, November 2013, p. 700-707, 2013.

[22] Bo-Chao Cheng, Guao-Tan Liao, Hsu-Chen Huang, Ping-Hai Hsu, “Cheetah: A space-efficient HNB-based NFAT approach to supporting network forensics”, Annals of telecommunications, Springer, volume 69, Issue 7, p. 379-389, 2013.

[23] Hong-Ming Wang, Chung-Huang Yang, “Design and Implementation of a Network Forensics system for Linux”, Computer Symposium (ICS), 2010 IEEE international, p. 390-395, 2010.

[24] Asou Aminnezhad, Ali Dehghantanha, Mohd Taufiq Abdullah, Mohsen Damshenas, “Cloud Forensics Issues and Opportunities”, International Journal of Information Processing and Management. Volume 4, Number 4, June 2013, p. 76-85, 2013.

[25] Farid Daryabar, Ali Dehghantanaha, Nur Izura Udzir, Nor Fazlida, binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh, “A survey about impacts of cloud computing on digital forensics”, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2), The Society of Digital Information and Wireless Communication, p. 77-94, 2013.

[26] Ashish Badiye, Neeti Kapoor, Pooja Shelke, “Some Forensics and Security Issues of Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.

[27] Arjit Ukil, Debasish Jana, Ajanta De Sarkar, “A Secret Framework in Cloud Computing Infrastructure”, International Journal of Network Security & Its Applications, Vol.5, No.5, September 2013.

[28] Tao Sun, Xinjun Wang, “Research of Data Security Model in Cloud Computing Platform for SME”, International Journal of Security and its Applications, Vol 7, No 6, 2013.

[29] Zhen Mo, Qingjun Xiao, Yian Zhou, Shigang Zhang, “On Deletion of Outsourced Data in Cloud Computing”, 2014, IEEE International Conference on Cloud Computing.

[30] Mazhar Ali, Revathi Dhamotharan, Eraj, Samee, Athanasios, Albert, “SeDaSC: Secure Data Sharing in Clouds”, 1932-8184, 2015 IEEE Systems Journal.

[31] Tania Gaur, Nisha Kharb, “Security of Data Storage in Cloud Computing. International Journal of Computer Applications (0975-8887), Volume 110 – No.10, January 2015.

[32] Rizwana Shaikh, Dr. M. Sasikumar, “Data Classification for Achieving Security in Cloud Computing”, Elsevier, 1877-0509, 2015.

[33] Florian Pfarr, Thomas Buckel, Anxel Winkelmann, “Cloud Computing Data Protection – A Literature Review and Analysis”, 2014 47th Hawaii International Conference on System Science.

[34] Harshit Srivastava, Sathish Alampalayam Kumar, “Control Framework for Secure Cloud Computing”, Journal of Information Security, 2015, 6, 12-23.

[35] Osama Harfoushi, Bader Alfawwaz, Nazeeh, Ruba, Mua’ad, Hossam, “Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review”, Communications and Network, 2014, 6, 15-21.

[36] R.V. Gandhi, M Seshaiah, A. Srinivas, C. ReddiNeelima, “Data Back-up and Recovery Techniques for Cloud Server Using Seed Block Algorithm. International Journal of Engineering Research and Applications”, ISSN: 2248-9622, Vol.5, Issue 2(Part 3), February 2015, pp.89-93.

[37] Valentina Casola, Alessandra, Massimiliano Rak, “On the Adoption of Security SLAs in the Cloud”, Springer International Publishing Switzerland 2015, M.Felici and C.Fernandez-Gago (Eds.): A4Cloud 2014, LNCS8937, pp. 45-62, 2015.

[38] Keiko Hashizume, David G Rosado, Eduardo, Eduardo B, “An Analysis for Security Issues for Cloud Computing”, Springer Open Journal, Journal of Internet Services and Applications 2013, 4:5.

[39] Cloud Standards Customer Council, “Cloud Security Standards: What to Expect and What to Negotiate”, October 2013.

[40] Dale Johnstone, “ISO/IEC 27018 Introduction ISO/IEC 27017 Update”, 26 January 2015.

[41] Cloud Special Interest Group, PCI Security Standards Council, “Information Supplement: PCI DSS Cloud Computing Guidelines”, 2013 Cloud Standards Customer Council, February 2013.