Master Thesis
Electrical Engineerig
October 2012

Cloud Computing as a Tool to Secure and Manage Information Flow in Swedish Armed Forces Networks

Muhammad Usman Ali and Rizwan Ayub

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirement for the degree of Master of Science in Electrical Engineering. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):
Muhammad Usman Ali
Blekinge Institute of Technology, Sweden
Email : malikusmanali@hotmail.com

Rizwan Ayub
Luleå University of Technology, Sweden
Email: rizayu-0@student.ltu.se

External advisor(s):
Ross Tsagalidis, MSc
Project Manager
FMKE, SWAF
+46-733666982
wross@tele2.se

Jens Kvarnberg
Major
FMKE, SWAF
+46-171-158128
jens.kvarnberg@mil.se

University advisor(s):
Professor Adrian Popescu
Dept. of Telecommunication Systems
Blekinge Institute of Technology, Sweden
Email: adrian.popescu@bth.se

School of Computing
Blekinge Institute of Technology
371 79 Karlskrona
Sweden

Internet: www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

In the last few years cloud computing has created much hype in the IT world. It has provided new strategies to cut down costs and provide better utilization of resources. Apart from all drawbacks, the cloud infrastructure has been long discussed for its vulnerabilities and security issues. There is a long list of service providers and clients, who have implemented different service structures using cloud infrastructure. Despite of all these efforts many organizations especially with higher security concerns have doubts about the data privacy or theft protection in cloud. This thesis aims to encourage Swedish Armed Forces (SWAF) networks to move to cloud infrastructures as this is the technology that will make a huge difference and revolutionize the service delivery models in the IT world. Organizations avoiding it would lag behind but at the same time organizations should consider to adapt a cloud strategy most reliable and compatible with their requirements. This document provides an insight on different technologies and tools implemented specifically for monitoring and security in cloud. Much emphasize is given on virtualization technology because cloud computing highly relies on it. Amazon EC2 cloud is analyzed from security point of view. An intensive survey has also been conducted to understand the market trends and people's perception about cloud implementation, security threats, cost savings and reliability of different services provided.

Keywords: Cloud Computing, Virtualization, SWAF, Amazon EC2.

ACKNOWLEDGEMENTS

First of all thanks to our most beloved ALLAH almighty, for giving me guidance and strength to complete this work.

I would like to thank our supervisor at Swedish Armed Forces, Ross Tsagalidis and Jens Kvarnberg for their guidance and support. I am gratefull to Swedish Armed Forces who gave me this wonderful opportunity. Special thanks to my supervisor at BTH Professor Adrian Popescu for his support and interest. I also would like to thank survey participants, who contributed to the survey part. Finally we would like to thank our families and friends for their support.

I would also like to mention special thanks to my thesis partner Rizwan Ayub from LTH for his support and commitment. We both have done this thesis together at SWAF and share the major tasks in this work. Literature review and survey questionnaire is a joint effort whereas the conclusion, discussion and analysis are done separately. This report is for BTH which is showing mostly my work. To make it convenient for readers to understand the conclusion, we have shared our work. These are the sections which have been taken from Rizwan Ayub's work 1.1, 2.3, 3.2.1, 3.5, 3.6.1 .

Muhammad Usman Ali

TABLE OF CONTENTS

LIST OF FIGURES

LIST TABLES

LIST OF ABBREVIATIONS

ARP	Address Resolution Protocol
AWS	Amazon Web Services
CRM	Customer Resource Management
DMTF	Distributed Management Task Force
EC2	Elastic Compute Cloud
GENI	Global Environment for Network Innovation
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol Secure
HVM	Hardware Virtualized Machine
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention System
IPC	Inter Process Communication
MAC	Mandatory Access Control
NAT	Network address translation
NIST	National Institute of Standards and Technology
NX	Non-Executable
OASIS	Organization for the Advancement of Structured Information Standards
OVF	Open Virtualization Format
PaaS	Platform as a Service
PV	Paravirtualization
QEMU-DM	Quick Emulator-Debian module
RDBMS	Relational Database Management System
RDM	Raw Device Mode
S3	Simple Storage Service
SAML	Security Assertion Markup Language
SaaS	Software as a Service
SLA	Service Level Agreement
SNIA	Storage Networking Industry Association

SOX	Sarbanes-Oxley Act
SQS	Simple Queue Service
SSL	Secure Socket Layer
SWAF	Swedish Armed Forces
TCG	Trusted Computing Group
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	Virtual Machine File System
VMM	Virtual Machine Monitor
VPC	Virtual Private Cloud
VPN	Virtual Private Network

Chapter 1
INTRODUCTION

1.1 Overview

The idea of using cloud computing as a utility is attracting new organizations to adopt this environment to cope with a vigorously altering business environment. IT managers see cloud computing as a source to maintain scalable IT infrastructures that allow business agility.

Cloud Computing started as a mean for interpersonal computing but now it is widely used for accessing software online, online storage [1] without worrying about infrastructure cost and processing power [2]. Organizations can offload their IT infrastructure in the cloud and gain from fast scalability. These organizations, not only include small businesses but also some parts of American government IT infrastructure is moved to cloud [3] as well.

It is important to understand the risks and threats in a cloud environment, so that an efficient security policy can be prepared for defense purposes. Preparation begins with understanding where awareness comes in. To adopt cloud computing it is important that organizations have an acceptable level of trust in it. Information security enhancement or success does not mean tossing technical solution to all the problems but it can also be accomplished with awareness like training and education.

The need to address some security issues related to cloud [4] and virtualization as well as people's perceptions to analyze, the level of awareness is needed. There has been a lot of research work that covers the technical side of these technologies but a lot of work has to be done on people's perception of cloud computing and its security issues.

In IT sector the most discussed and revolutionary topic is cloud computing. Immense research is being conducted in the academia and industry on cloud computing [5]. This study shows that cloud computing is comprised of different core technologies [6] and cloud can be used as a tool in SWAF, which will help them in monitoring and managing their networks.

1.2 Aim of Study

A survey conducted by IDC [7] shows that 87.5% of the respondents think that the biggest challenge to cloud/on-demand model is security. Even though there are security issues in the cloud, people's perception towards cloud and their knowledge/awareness about security issues is known very little.

This study brings facts about some security issues related to cloud computing and virtualization usage in cloud and it also intends to bring up the amount/level of awareness among people in SWAF, which influence the trust level on cloud computing. This study helps in changing the perception of cloud computing and encourages SWAF to take further practical step toward cloud computing in future.

1.3 Delimitations

As cloud computing and virtualization consists of many security issues this work is not focused on all possible security issues related to them. Due to sensitivity of survey questions it is not possible to disclose organizations name and/or respondent's identity.

1.4 Thesis Structure

The structure of this thesis is organized as follows. The first chapter presents general background, research aims and delimitations related to our study. The second chapter is an intensive literature review of the theoretical framework, which describes the types, services and deployment methods of cloud infrastructures. Further we have shed some light on the present cloud vendors, existing technologies being implemented by these vendors. Third chapter provides an in depth and detailed explanation about virtualization, being the core of cloud computing technology and the security issues, which might be faced by different organizations and military. The Fourth chapter comprises of our research methodology explaining research purpose, approach, strategy and data collection method and analysis plan. Fifth chapter presents our empirical findings and data analysis derived from studies. The last chapter focuses on conclusion and related future work.

Chapter 2
LITERATURE REVIEW

2.1 Cloud Computing

2.1.1 Definition

The US National Institute of Standards and Technology (NIST) defines cloud computing as

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models and four deployment models." [8]

2.1.2 Service Models

Cloud computing has been categorized into three models depending on the services provided by the cloud. Following is the brief description of each service model. The table 1 shows benefits of cloud services provided by different cloud vendors in the present market.

- **Software as a Service (SaaS)**

The consumer is provided with the capability to use provider's application running on a cloud infrastructure. The consumer does not have to manage cloud infrastructure like servers, operating system, storage and network. The services are accessed typically with a web browser. [9]

- **Platform as a Service (PaaS)**

The consumer is provided with the capability to create applications on their own or through the tools provided by the provider on cloud infrastructure. The consumer has the control over their deployed applications but have not to manage server, storage, network or operating system. [9]

- **Infrastructure as a Service (IaaS)**

The consumer is provided with the capability to processing, storage, networks and any software which they want to run and the operating system which they choose on the cloud infrastructure. The consumer does not control the cloud infrastructure but networking components like host firewall, storage, operating systems and deployed applications are controlled by the consumer. [9]

Service	Offering	Benefits	Vendors
Software-as-a-service (SaaS)	Provider's software accessible over a thin-client interface, on-demand, by employing multitenant architecture and complex caching mechanisms (deals with the end-user directly)	Low initiating costs, painless upgrades, seamless integration, easy customization, and managed service-level agreements (SLAs)	• Salesforce.com CRM • 3Tera • IBM Lotus Live
Platform-as-a-service (PaaS)	Computing platform including add-on development facilities, stand-alone development environments, an application only delivery-only environment, and a runtime environment for compiled application code	Cost reduction, especially in ensuring security, scalability, and failover services; geographical distributed development teams	• Google App Engine • Sun Microsystems • GoGrid
Infrastructure-as-a-service (IaaS)	Processors, memory, bandwidth, network (such as firewalls and load balancers), and storage on demand using virtualization technologies	Lower IT infrastructure, administrative, and maintenance costs	• Microsoft SQL Azure • The Rackspace Cloud • Oracle • EnterpriseDB

Table 1: Different types of cloud services [10]

2.1.3 Deployment Models

There are four deployment models with reference to the services and users. [11]

- **Private cloud**

The cloud is maintained and operated for a specific organization. Private cloud can be in-house or with a third party on the premises. The figure 1 below is a simple architecture of an Onsite private cloud (In-house) showing clients within the security premises can access the cloud services whereas the unauthorized clients are blocked. Whereas the figure 2 shows an Out sourced private cloud where the cloud is located on a third party premises hosting the server side and is accessible only by the authorized clients.

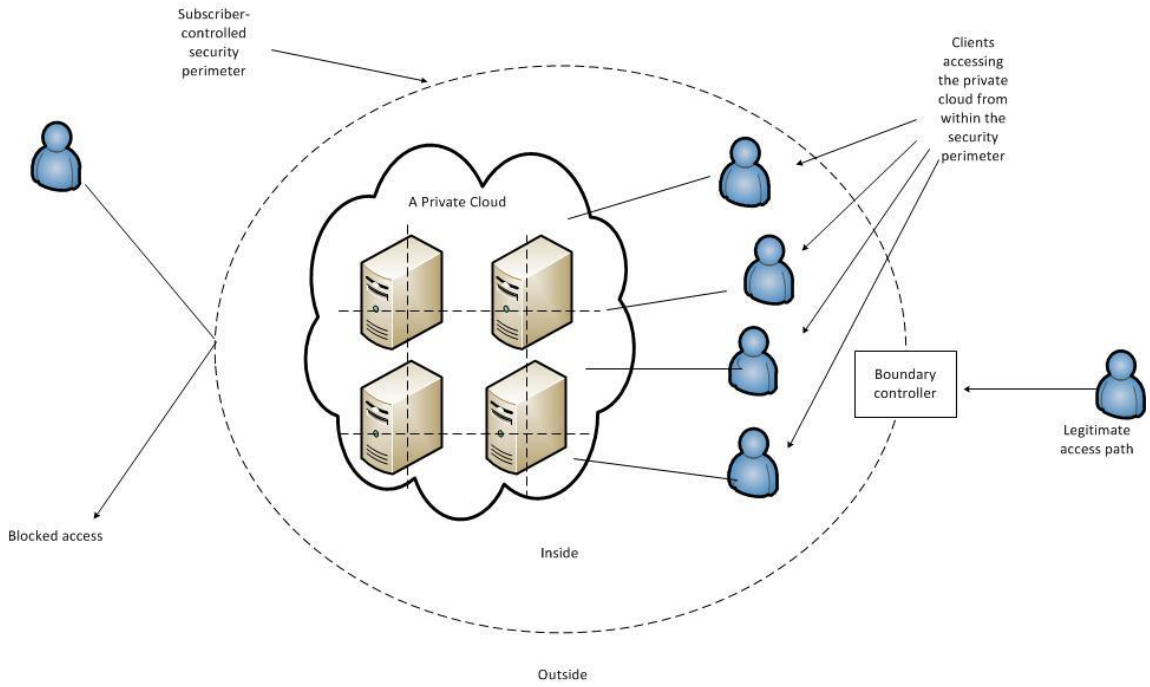


Figure 1: Onsite private cloud [12]

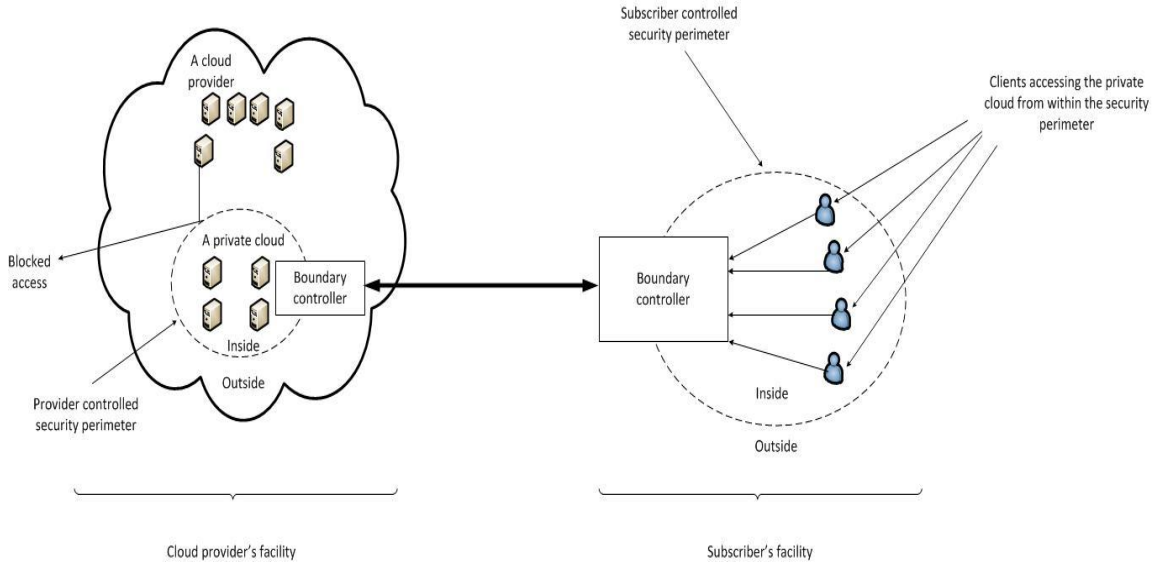


Figure 2: Outsourced private cloud [12]

- **Community cloud**

The cloud infrastructure is shared among a number of organizations with similar requirements and interests. It can be in-house (Onsite community cloud) or with a third party (Outsourced community cloud) on the premises as shown in figure 3 and 4.

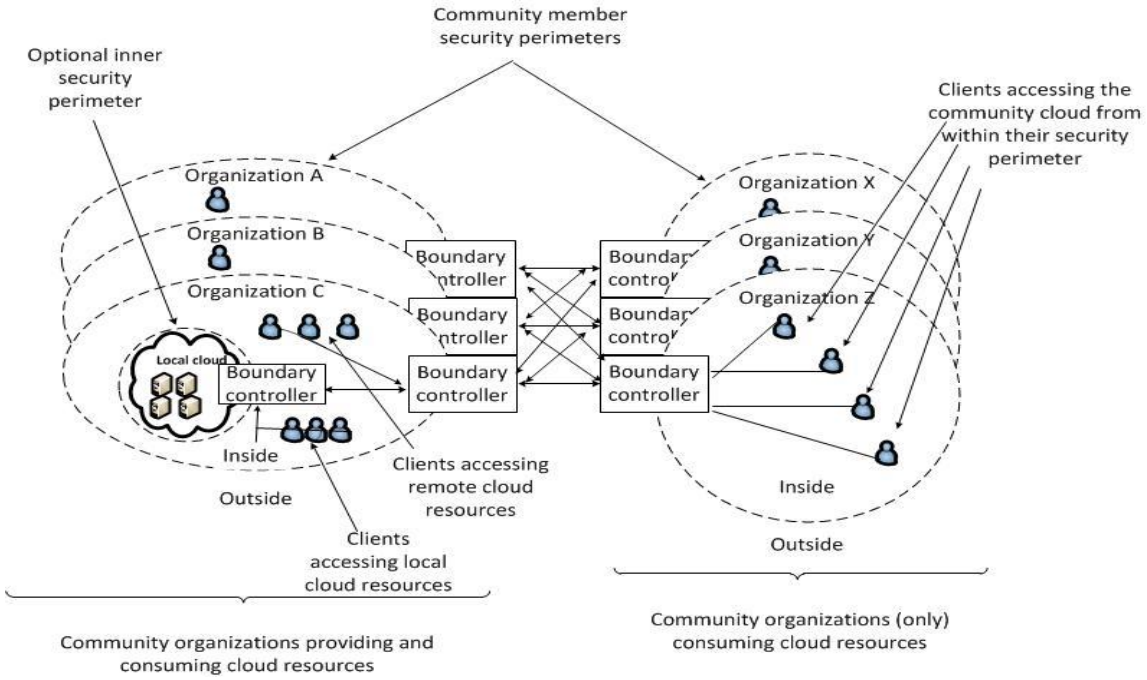


Figure 3: Onsite community cloud [12]

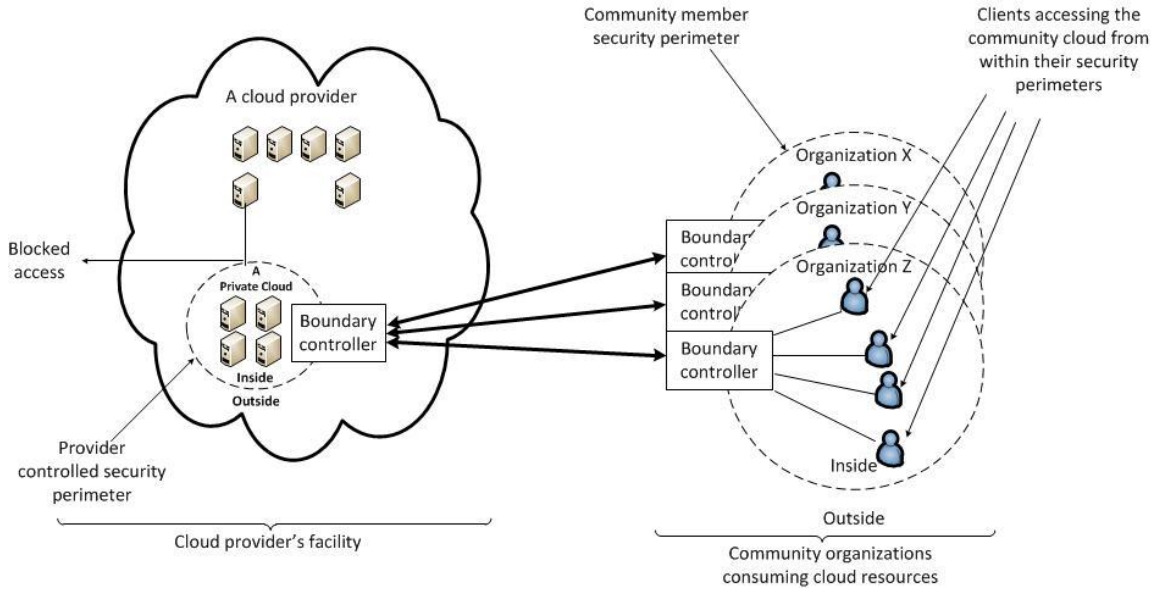


Figure 4: Outsourced community cloud [12]

- **Public cloud**

The cloud is available to the public on commercial basis by a cloud service provider. As shown in figure 5 the public cloud has a large variety of organizational and general public clients making it easier to adapt but more vulnerable to security risks.

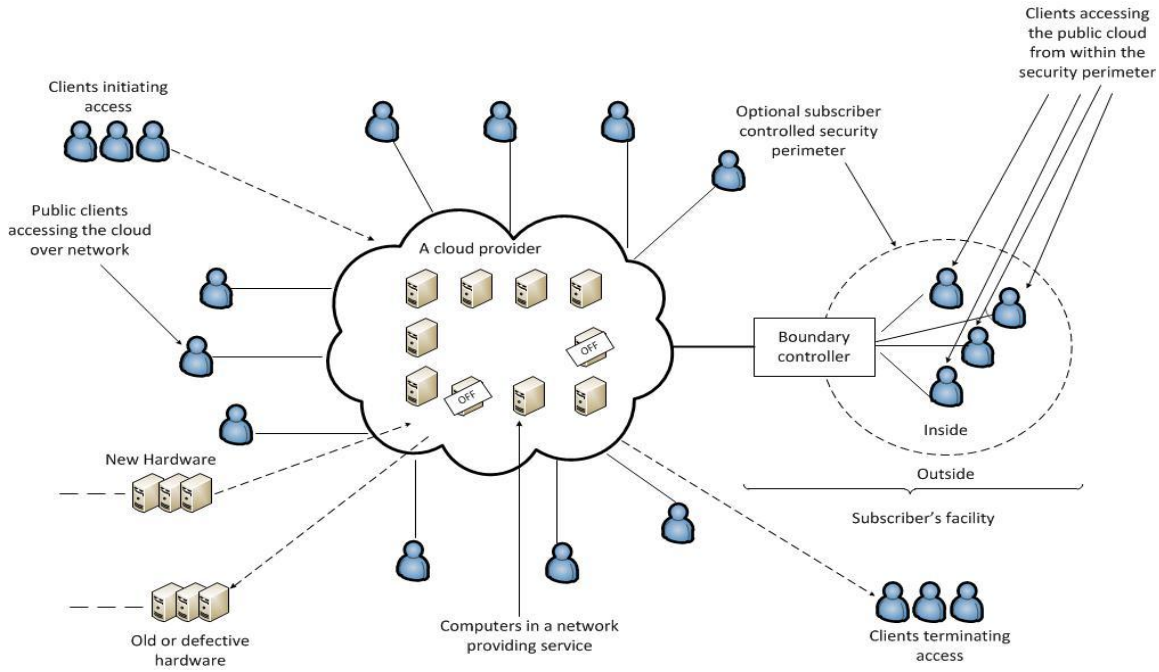


Figure 5: Public cloud [12]

- **Hybrid cloud**

This is the combination of different types of clouds (public, community or private clouds) as shown in figure 6 below. The hybrid cloud has clear limitations for data/application access but as they are part of a single standardized or proprietary technology, which allows the data and application to be moved if required from one cloud to another.

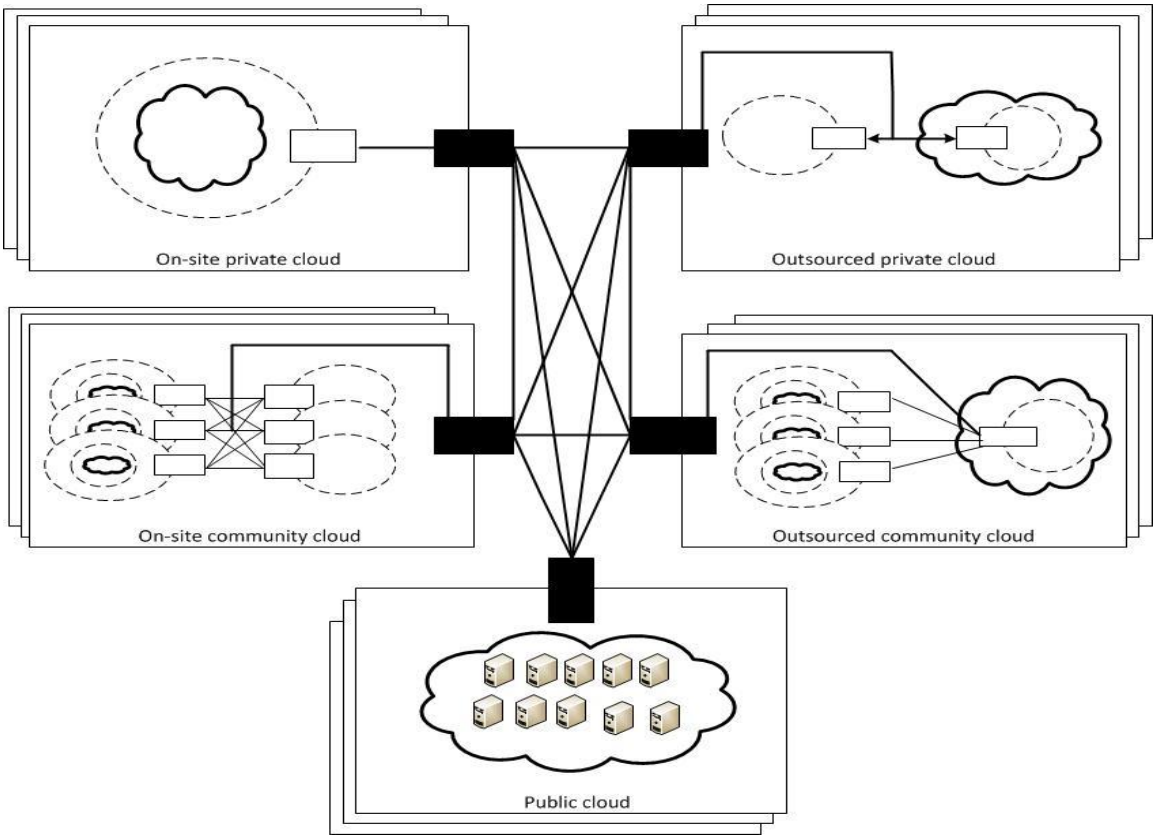


Figure 6: Hybrid Cloud [12]

2.2 Public Vs Private Cloud

A private cloud means using own resources in own datacenters making organization in control but additional responsibility of management comes upon organization. While in public cloud, organization will be relieved from management tasks but the organization will have less control [13].

The location is also a differentiating factor as in public cloud the hosting will be done in the provider's data center and the services will be provided through web browser. While

in private cloud the deployment will be done within the firewall and managed by the organization's own employees. [14]

The public cloud will be charged on monthly basis. The cost includes the usage per Gigabit with bandwidth transfer fees. The storage can be scaled on the demand of user and they don't have to buy the storage hardware. The company manages the resources and users don't have to worry about maintenance. In private cloud the equipment is solely owned by the company and they have to manage the cloud. The company can easily scale their storage by adding new servers to the existing ones. All the data is intended for the company itself and there is no sharing outside the company. The scalability is the great advantage in private cloud and it leaves the company with greater performance and capacity. [14]

- **Elementary expense**

It is falsely believed that private cloud is very expensive. Whereas it is simply easy to build a private cloud at an affordable budget and the deployment is also pretty easy. Public cloud hosting is offered at reasonable prices keeping in mind that companies don't have to buy hardware or software.

- **Volume of data**

Private cloud can be started from a few terabytes of data and can be scaled by simply adding the new node or disk as the need arises. Similarly in public cloud company can start from just the backup of their laptop. And it can be increased according to the situation with increase in cost also.

- **Duration of data storage**

In public cloud if company wants their data to store for a longer period then there will be increase in costs. Public cloud is most suitable for an organization if its data keeps on changing over time. While in private cloud the duration won't add to organization's cost and it is suitable if they have large archives of data.

- **Performance expectations**

In private cloud the resources can be accessed at Ethernet Local Area Network inside the firewall. The read access speed is pretty high usually at 100 MB/s. While in public cloud the services are provided on the internet so there could be some problems of speed. This can be overcome if appropriate bandwidth is chosen while selecting the public cloud.

- **Access patterns and locations**

In public cloud if organizations have users all over the world, they can replicate data to different geo-locations but it will also increase costs. When the data is stored in different places, data stolen risk is very high. To overcome this problem the encryption approach is needed. Transport Layer Security (TLS) and Secure Socket Layer (SSL) are cryptographic protocols that can used to ensure safe data transfer [15].

It is most suitable in content distribution networks. While private cloud is in a single location accessed through Local Area Network. The remote users will connect through Wide Area Network, maybe through internet. A private cloud at different locations making it a distribution approach may cost more initially. Access control mechanisms are very important to ensure the data security in cloud storage [15].

- **Security and data isolation**

In public cloud different cloud vendors have their security policies but the main concern is how much they have control-ability of their data. The isolation is only as strong as the virtualization technology used and the provider's firewall. While in private cloud isolation of data depends on company's requirements and security is based on internal processes.

- **Confidentiality and destruction of data**

In public cloud different vendors have their own terms and conditions so they must carefully go through them before selecting them. While in private there is no such problem of data deletion as they themselves manage it.

- **Service Level Agreements SLA's**

In private cloud individual server malfunction will not affect other services. Hence company's data is not lost and SLA's are fulfilled. Company must keep in mind the architecture and its capabilities before deploying their private cloud. While in public cloud the vendors publish their SLA's and it is their responsibility to keep up to that. In case of data loss, vendor will retrieve the data from last backup files and it might the company.

- **In-house technical crew**

In public cloud company don't have to hire technical crew as they don't buy hardware and software to be looked after. It is the responsibility of the vendors to manage their

applications and data. While in private cloud the companies have to hire the technical crew as the deployment is inside the firewall. Those persons will manage the cloud.

- **Availability of services**

If the organization can't afford disruption in service then the best solution is private cloud. Multi cloud can be good approach for eliminating the availability problem. A recent downtime in 2011 of Amazon web services has affected a large number of enterprises which further raises doubts about the availability of services provided by public cloud vendors [16].

2.3 Characteristics of Cloud Computing

To differentiate cloud computing from traditional computing a research done by Cloud Security Alliance [22] has defined five distinct characteristics of this model.

- **Resource pooling**

Generally resource pooling in a cloud environment is achieved through multi-tenant architecture. Multiple customers in a multi-tenant environment access provider pooled resources.

- **Rapid elasticity**

Computing resources such as CPU, memory and storage is available for provisioning and can be acquired in any quantity at any instant. These resources can be allocated to a user rapidly.

- **Broad network access**

Cloud based services can be accessed over network with the help of variety of client platforms.

- **Measured service**

Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.

- **On demand self service**

Resource allocation such as storage, processing and server time is done automatically and no human interface is essential.

2.4 Benefits of Cloud Computing

Cloud computing can help to counter an organization's IT needs. Let's look at the key benefits in cloud computing. [17]

- **Scalability**

If company came to know that there is an increase in demand of resources, then cloud computing can help. Rather than buy new equipment, install and configure them, instead company can buy additional CPU cycles or storage from a third party. This will lower their cost of new equipment. Once they have met their needs for additional equipment, they can stop using cloud provider's services and they don't have to deal with unneeded equipment.

- **Simplicity**

By not buying new equipment and configuring them allows IT staff to get to the business directly. The cloud makes it possible to start applications immediately and the cost is very less if the company would have to find an onsite solution.

- **More internal resources**

By shifting non-critical data needs to cloud, company is allowing their IT department to focus on business more. And they don't have to hire or manage more.

- **Security**

Vendors have strict policies for ensuring security. They have proven cryptographic methods to authenticate users. Additionally, they can always encrypt their data before storing on the cloud. By these measures their data is more secure on cloud than in-house.

2.5 Cloud Security Issues

The responsibility of secured infrastructure in cloud computing depends upon service provider and customer, keeping in view the service model [18]. The security controls in cloud computing are same as in any other IT environment. Different deployment models and technologies are used to provide cloud computing services to organizations which may pose different risks [9].

We can take some examples to show that responsibility of security falls on both provider and consumer. In Amazon's EC2, which is a IaaS offering, the providers responsibility is

up to the hypervisor that means they provide physical security, environmental security and virtualization security. While the consumer's responsibility of security, is of operating system, application and data. But in the example of Salesforce.com's Customer Resource Management (CRM), which is a SaaS offering. The entire responsibility lies on the provider that means it will take care of physical, environmental, application and data security controls. This will relieve the customer. The difference in two examples is due to different service models.

The cloud service providers have to deliver diverse services to many users. They also have to manage the security and when they take steps to improve security, the services become more rigid. This rigidity is what we said earlier that, it may pose some different risks to the organization. These risks arise mostly at the network layer of security controls.

- **Data Integrity**

The consumer wants that [19]

1. They should access cloud resources with security protocols like HTTPS or Secure Sockets Layer (SSL) as well as security auditing and compliance checking.
2. Fine-grained access control to protect data integrity and protection from intruders or hackers. And single sign-on or sign-off.
3. Shared datasets that are protected from malicious alteration, deletion or copyright violation.

- **Data Theft**

1. One possible solution is to encrypt the data. [20]
2. Personal firewalls and shared datasets protected from Java, JavaScript and ActiveX Applets as well as established VPN channels between resource sites and cloud clients. [19]

- **Privacy Issues**

The client and service provider should have same privacy policy if not better than the other. The provider should assign to every user an access control mechanism defining when and who is going to access the data. The clients are also worried that their data might be looked at by the vendors. Clients also need to look at all the access log of their employees and also of vendor employees. [10]

- **Infected Application**

The vendor should have access to the servers so that they can check if any malicious user has uploaded any infected application. In that case they can take the necessary actions to avoid any inconvenience to the customer.

- **Governance**

IT infrastructure manages complex set of hardware and software environments and these services are provided to a customer with a guaranteed service level. Governance means to have proper control over policies, measures and principles for IT service achievement [22]. If governance is compromised then the policies and measures for security can be ignored.

- **Compliance**

Compliance refers to the responsibility of an organization to work under a specific agreement with established laws, standards and regulations. Compliance become complex issue for cloud service provider because of varying security and privacy laws administrated in different countries [22].

***Law and Regulations*:** Even though cloud service providers are becoming aware of different laws and regulations, and may store data in specific control and apply required protection for security and privacy. Laws such as SOX and HIPAA etc. require the customer to be responsible for the security and privacy of data hosted in cloud.

***Data Location*:** Data location is one of the most important compliance issues faced by organizations nowadays [21]. In case of data center housed within organization premises the data location as well as the security controls in place to protect the data is transparent. In a typical cloud computing environment the data is stored in numerous physical locations and data location is unknown to the service customer.

- **Trust**

In a cloud environment an organization hands over control over many aspects of security by putting its trust on the cloud service provider [22] [23]. Data that is being stored outside the physical boundaries of an organization bring with intrinsic level of risk. [22].

The Insider access issue or threat as we know is an issue that is equally true in cloud environment. Insider threats include fraud, information theft and information resources sabotage. Apart from causing an incident intentionally it is possible that it happens unintentionally.

Moving organizational data into the cloud do not only broaden the domain of threat from organizational staff but also from other cloud customers utilizing cloud services and sharing resources like virtual machine instances in cloud for computational requirements. Such an attack has been conducted in the past against an IaaS cloud as described in [22].

- **Data Ownership**

It is important that an organization hold possession over all its data. Cloud service provider should not be given any rights to alter or use the data for its own purpose or gain.

- **Identity and Access management**

One of main areas of concern for organization to move toward adopting cloud is privacy and data sensitivity issues. Illegal access prevention has also become one of the considerations for cloud service providers. SAML standard is being used by number of cloud service providers nowadays to manage users in cloud.

- **Data Protection**

Data is stored in a shared environment in cloud i.e. in a shared environment data is located with other customer's data. Data types that are stored in cloud can vary and to keep data away from unauthorized users access control as well encryption are the only choices. As access control mechanism is typically identity based, encryption remains the only way to protect the data.

2.6 Cloud Vendors

There are many vendors who offer cloud services with different pricing models. We will take a peek in few of the leading vendors like Amazon, Google and Microsoft. [17]

2.6.1 Amazon

Offers a number of cloud services, which are;

- **Elastic Compute Cloud (EC2)**

EC2 offers virtual machines and extra CPU cycles for an organization. EC2 is rented in units called instances. Where each instance, is a virtual server. There are five different types of instances to rent from, each with varying CPU power, memory, hard disk space and IO performance. [24]

- **Simple Storage Service (S3)**

S3 was launched in 2006. S3 allows company to store items up to 5GB in size in Amazon's virtual storage service. [24][17]

- **Simple Queue Service (SQS)**

With message passing API the machine can talk between distributed software components. This service is used with EC2 to coordinate between different instances.

- **SimpleDB**

This service works with S3 and EC2 and collectively providing the ability to store, process and query data sets in the cloud. It is a relational data storage service like RDBMS. SimpleDB is accessible independent of EC2 instances and SQL-like query language is used.

These services are command line because Amazon's virtual machines are Linux based.

2.6.2 Google

Google offers Google's App Engine, which enable developers to build their own applications like Google's own applications. It is the example of PaaS offering. Google removed the feature to write file out of security reasons. To store, company must use Google's database. App Engine is not as uptake as Amazon because it is newer and is only out for test basis. [24] [17]

2.6.3 Microsoft

Microsoft offers operating system Windows Azure to run Windows applications and store files and data using their datacenters. Key features of Azure platform are;

- **Windows Azure**

Windows Azure provides service hosting and management of storage and networking. Users have to choose Web or Worker roles for application instances. Web role is suitable for application interacting with outside world using the network while the worker role is for applications just needed for simple processing. The Azure platform provides storage in three forms that are Blobs, Tables and Queues. Blob storage is similar to Amazon's S3. Table storage is similar to Amazon's SimpleDB. Queue storage is similar to Amazon's SQS.

- **Microsoft SQL Services**

Microsoft SQL service provides database services and reporting. The software is similar to RDBMS SQL server with a slight modification to the interface. This service is similar to Amazon's SimpleDB.

- **Microsoft .NET Services**

Provides service based implementation of .NET framework. .Net services has three components which are

1) Access control service. 2) Service Bus and. 3) Workflow Service.

Live Services: used to share, store and synchronize documents, photos and files.

2.6.4 EMC

EMC's Symmetric V-Max is a management system that supports high end virtual datacenters. It provides storage facilities and different datacenters can be managed from one place.

2.6.5 NetApp

NetApp and Cisco have joined together to provide dynamic data centers and storage service and server virtualization.

2.6.6 IBM

IBM offers Smartcloud. It provides both public and private cloud solutions. Customer can choose from the available servers, operating system and applications. It provides PaaS, IaaS and SaaS services. [25]

2.6.7 OpenStack

OpenStack is open source cloud computing platform for public and private clouds. It is founded by RackSpace hosting and NASA. [26]

2.6.8 Eucalyptus

Eucalyptus provides the platform for private cloud computing. It has an API which can be integrated with Amazon cloud. It uses current infrastructure to create an AWS compatible cloud resources for storage, network and computing. [27]

2.7 Performance and Cost Factors

The study[28] shows there are many influential factors in adopting cloud computing like Reliability, Security, Performance, Scalability, Compliance and Physical Location, Integration with other Services, Environmental issues, Cost, Innovation, IT Department's Stand and Changes, Cloud Model, Time to Market and Ease of Use. Here only two important factors, cost and performance are taken into account.

2.7.1 Performance

Any organization who wants to adopt cloud environment should think about the Performance issues. Performance factors depend upon cloud deployment model, different technologies and techniques an organization uses. The connection between the cloud server and user can be a major factor which can affect the performance [29]. Different latency concerns like Network latency, processing latency and client side latency can affect the performance. For improved performance the latency should be guaranteed end-to-end and edge devices should be configured according to cloud configurations. [30]

2.7.2 Cost

Reduction in cost is also a primary factor for inclination towards cloud computing. An organization has to spend a lot of cost on setting up IT infrastructure and still the resources cannot be fully utilized which is a waste of money. But by using Cloud an organization have to pay for the resources they will use. Capacity planning can become easy because of cloud computing. Users only have to pay for the resources they used,

according to their demands. Reduction in cost depends upon the cloud deployment model. Data transfer will be a costing issue in public clouds. In [31] different costing issues have been analyzed in AWS.

A recent research project [32] carried out for the connectivity of GENI resources to the resources allocated on Amazon EC2 shows a very clear explanation of cost implications. Amazon EC2 cloud has different regions with multiple availability zones to avoid complete failure during server instances. Amazon has provided the access to EC2 resources purely on IP and only layer-3 solutions.

Only the traffic in the same availability zone is free where as the traffic between different regions and different availability zone even in same regions are all charged. Amazon has a charging of $0.10per GB for data transfer in the EC2 cloud while the data transfer out has different rates as high as $0.17per GB for 10TB per month to as low as $0.10per GB for over 150TB of data per month. Moreover the data transfer between instances in the availability zone in same regions charges $0.01 per GB in/out. Static IP addresses are also offered and charged by Amazon on customer demand. Assigning a static IP address to an instance can cost $0.01, while the unused static IP addresses is charged $0.01 per hour.

The above costs also imply for VLAN connectivity using any software e.g. VPN if customer requires within the allocated resources. Another option is to create layer-3 VLAN using Amazon VPC. This helps to bridge or expand VLAN capacity using the EC2 cloud. A basic price of $0.05 per VPN connection per hour is charged but it should be noted that there are further restrictions such as number of subnets per VPC, number of VPC per AWS, VPN gateway per AWS account and more. Hence these implementations give a much clearer picture of cost expenses for a customer moving to cloud services

2.8 Cloud Computing Standardization Issues

Lack of Standardization arises issues like data privacy, encryption and interoperability [33], which is affecting its adoption. To overcome the standardization issues different well known organizations are playing their roles. DMTF's OVF is helpful for Hypervisor by providing a way to transport VM between different platforms [34]. IEEE is working on standards to support interoperability among different cloud computing platforms.

OASIS is working to solve security issues like identity management and vulnerability mitigation. It is also working to improve the quality of service (QoS). SNIA provide standards for clients to interact with cloud based storage, interaction between two cloud storage and data management in cloud.

When using public cloud enterprises have to face vendor lock-in issue. In order to reduce vendor lock-in, open standards are needed. For avoiding the issue of vendor lock-in the enterprises are looking for inter-cloud concept, so that back up of their application data can be stored in another cloud. [35]

These efforts are not enough but timing and user input are very important factors. Standardization process will refine in coming years. Cloud computing is still in infancy stage and trust level is weak, once the big organization and government agencies start adopting cloud environment this will speed up the standardization process.

2.9 Military Security Issues

We had a special task to find through intensive literature studies and a survey targeting the professionals in IT to find out whether it's safe for the armed forces to shift to cloud infrastructure or not. As we know that the data in military is highly sensitive, so a security policy is essential. In military the security policy dictates that every information should be tagged as who can access which information. There should be proper authorization of the users. In commercial environment the disclosure of information is not so important but it must be applied in military. There should be no disclosure of information to any unauthorized person. There should be a proper check as to which person can read which data items. To do this there should be a check on who can write the data. There should also be a proper security measure while copying a data item. Because when an item is copied, it should be ensured that all the security constraints are also applied to the copied document. If there is no security constraints applied to the copied data item, then it can easily become declassified and problems may arise. In 1983, the U.S Department of Defense produced the Orange Book. In this book all the mechanisms to apply the security policy are written for computer based data. For example all the stress in that is on data labels and user access control. [36]

Chapter 3
VIRTUALIZATION

There are many different existing technologies and practices used by cloud providers such as the usage of Internet Protocols for communication, Virtual Private Cloud (VPC) Provisioning, Identity and Access Management (IAM), Load Balancing and Scalability, High Performance Computing Technologies and Virtualization. In this chapter we will focus on virtualization being the core technology used in market and describe in detail the types, functionality, security benefits and how it is used as a tool for monitoring and securing the network. Further we will also highlight on some security attacks which might be possible using this technology.

3.1 Virtualization

One of the important factors behind cloud computing is scalability and it can be achieved using virtualization technology [37]. Virtualization can be defined as a technology such that there is a software abstraction layer between the hardware and operating system and applications running on top of it. This software abstraction layer is called Virtual Machine Monitor (VMM) or Hypervisor. The VMM hides the physical resources from the operating system because hardware resources are controlled by the VMM. This is the reason that user can have two or more operating systems running on the same machine in parallel. Therefore hardware can be partitioned into two or more logical units called virtual machine (VM). VMs share the physical resources like memory, disk and network devices. Programs running in one VM cannot be seen by other VM's programs, that is, they are isolated. [38]

3.1.1 Definition

Virtualization defined by SNIA,

"The act of abstracting, hiding, or isolating the internal functions of a storage (sub)system or service from applications, host computers, or general network resources, for the purpose of enabling application and network-independent management of storage or data"[37].

3.2 Benefits of Virtualization

Different core technologies can be used to build cloud computing depending upon the organization needs [39]. One of the most important and heavily relied technology in cloud computing is Virtualization [40]. The reason for using virtualization is reduced cost and better monitoring. Some of the main benefits of virtualization are described below.

- **Easier manageability**

Whole network can be monitored and managed form a single point. Administrators manage and monitor the whole group of computers in a network from a single physical computer [37].

- **Availability**

One can keep the virtualized instances running even if the node needs to be shut down for maintenance purposes. This can be done by migrating the virtualized instances to other machines and later migrating them back to the computer without closing the instance. So there is no downtime in the services [38].

- **Scalability**

Administrator can easily add a new node with basic installation to contribute with the existing virtual machines to provide the services. So as the company expands the cluster will also expand [38].

- **Increased security**

The information and applications can be put in different virtual machines on a single physical machine. Thereby increasing the security as virtual machines are separate entities. If a virus comes in it will not affect the whole computer because it will reside only in the one VM and other VMs will not be affected thus delivering the services [37].

- **Reduced costs**

Costs are reduced in the sense that less hardware, less space and less staffing requirements. Network costs are also lowered as less switches, hubs and wiring closets are required [37].

3.2.1 Security Benefits of Virtualization [41]

As we know that security is one of the main worries for organizations to adapt cloud computing so we must peek into the security benefits and their implementations using virtualization.

- **External monitoring**

Virtual machines share resources from a single physical machine so it is possible to observe resource usage of a VM and detect a malicious software activity through an external VM. VM monitoring can be done by hypervisor or a dedicated external VM. It is prudent to dedicate a separate VM for this purpose as hypervisor should remain as secure as possible.

- **Transience**

VMs one of the most exciting feature is to start it remotely, which means that it can be used when needed. Since an offline server cannot be accessed, reducing the time it is online can be helpful to save it from attackers. When the servers are online they should be used all the time which ensures that the system is being directly observed helping to monitor any interference.

- **Isolation**

One of the most popular and important feature is *"isolation"*. A single physical machine resource is partitioned into segments so that each Guest VM can run separately. This isolation makes sure that a single VM failure would not affect other VMs or if a VM is compromised then other VMs sharing resources on the same physical machine are not affected. Isolation at VM level brings additional security along with multi-user OS file access security (read, write or execute).

- **Abstraction**

Hypervisor typically serve as a layer of abstraction between VMs and hardware. Each VM is allowed to access its share of allocated resources. A guest OS running on a VM has no idea about hardware nor it has any idea about virtualized environment (Full virtualization). This abstraction also enhance the security as an attacker wouldn't know about host environment and compromising it, will be to a great extent difficult.

3.3 Types of Virtualization

There are two types of virtualization which are process virtualization and system virtualization. It is also noteworthy to mention paravirtualization and previrtualization which are the two types of approaches for system and processes virtualization. Let us throw some light on all of them one by one.

- **Process Virtualization**

In process virtualization the operating system virtualizes the memory address space, CPU registers and other system resources for each running process [42]. Each process is unaware of the activities of other processes. The operating system assigns CPU time to each process based on scheduling algorithm. So that every process gets the fair share of CPU time and thus creating the illusion that each process has got the sole CPU time [43]. Through virtual memory each process has the illusion as if it has its own address space. In which it has the access to its code and data and also to the system and application libraries. The virtualization of memory is achieved through page tables. The virtual memory page addresses are mapped from process virtual address space to actual physical memory.

- **System Virtualization**

In system virtualization the entire system is virtualized, the memory, CPU, devices and processes creating a virtual environment known as Virtual Machine (VM). This is achieved through a hypervisor or Virtual Machine Monitor (VMM). The hypervisor manages the resources and provides them to the VMs safely [43, 42].

- **Paravirtualization**

In paravirtualization the actual guest code is modified to use a different interface. This modified interface will access the hardware directly or the virtual resources controlled by the VMM [44]. Systems like Xen use paravirtualization.

- **Previrtualization**

Previrtualization is a technique for combining the performance of traditional virtualization with paravirtualization [45]. Previrtualization is achieved through an intermediary interface between guest code and VMM. This interface should be agreed on by VMM and guest OS developers or there should be a special compiler to do this.

3.4 Hypervisors or Virtual Machine Monitor (VMM)

Hypervisor or virtual machine monitor (VMM) is the heart of virtualization technology. As briefly described above in 3.1 hypervisor is a software which sits between virtual machines (VM) and hardware to allow multiple operating systems to run on top of single physical machine. Hypervisor controls each VM access to I/O, memory or/and storage which gives a benefit of isolation. Hypervisor makes sure that VM's operations are isolated from each other like crash of one VM should not affect working of other VM's and one VM should not access memory block already belong to other VM. Hypervisor should have a very high level of security because whole of the system is dependent on the stability of the hypervisor. Mechanisms should be used which guarantee, secure communication and strong isolation [46]. Following are some of the types of hypervisors being used at present.

- **Traditional hypervisors**

These types of hypervisor can support more than one virtual machines, and runs on bare metal. Traditional hypervisor such as Xen and VMWare ESX supports its virtual machine completely regarding device drivers and other necessary services [47, 48].

- **Hosted hypervisors**

These types of hypervisor can support more than one virtual machine and runs on standard OS. Hosted hypervisors can take advantage of existing device drivers in the host OS and other service. Desktop users with the help of hosted hypervisors take advantages of virtualization. Examples are VirtualBox or VMWare Workstation [49, 50, 51].

- **Microkernels**

Microkernels mostly used in embedded system and implement low level mechanism and can be used to isolate operating system servers in user mode. Communication paradigm between operating system's servers is inter-process communication (IPC). Microkernel only knows about threads, tasks, memory context of tasks and OS processes. Microkernels don't offer any service or device drivers like other hypervisors [52].

- **Thin hypervisors**

Thin hypervisor like traditional hypervisors run on bare metal. These are very small in size to give less functionality. They are suitable for embedded system because of low cost and low resources. Examples are SecVisor and BitVisor [53, 54].

3.4.1 Hypervisor Based Security Architecture

3.4.1.1 Isolation based services

There are many isolation based services as part of the hypervisor based security architecture which is also an advantage, so a brief description is given below.

- ***Protecting against a malicious OS***

The hypervisor does not safeguard the application's own vulnerabilities and a malicious operating system from posing a threat [55].

- ***I/O Security***

BitVisor is an example of hypervisor which provide I/O security. Most I/O instructions pass through the driver to the hardware but the control and data instructions are handled by the hypervisor [54].

- ***Mandatory Access Control***

With Mandatory Access Control (MAC) policies, better security can be brought to critical applications. The hypervisor based MAC can be used to secure virtual domains.

3.4.1.2 Monitoring based services

Another part of hypervisor based security architecture is monitoring based services. Following are the main aspects which can be achieved through monitoring based services.

- ***Attestation***

Hypervisors can be used to attest the guest code integrity and state. This is done with the architecture of Trusted Computing Group (TCG). An early VMM used for attestation was Terra [56]. It supports open and closed box domains with sealed storage and remote code attestation for domains. Closed box domains cannot be even examined by the owners. Examples are game consoles, ATM's and mobile phones. Terra was implemented using

VMware GSX Server along with management VM, which allocate resources and interaction between VM's.

- ***Malware analysis***

There are many examples of virtualization based systems for malware analysis. We will take the example of Patagonix system [57]. It tracks code execution supported by hardware mechanisms and remain consistent of any OS differences. This is done by setting up a non-executable (NX) bit on all pages. Any code execution can be trapped by the hypervisor where upon it can be inspected.

- ***Intrusion detection***

Intrusion detection in a system Introvirt [58], bridges the semantic gap between predicates and guest software, the system can execute the guest code in guest address space. And if there is any change in the guest state because of executing the guest code, the system has the roll back functionality.

3.5 VMware ESXi and XEN Hypervisors

VMware ESXi, KVM, Xen and Hyper-V are some of the popular hypervisors. Recent studies [59] [60] show that VMware and Xen are the two most used hypervisors but Xen is slightly ahead and gaining popularity rapidly. Hence description of VMware (proprietary) in brief and Xen (open source) in detail is provided in the following sections.

3.5.1 VMware ESXi

In virtualization products Vmware is the leader and ESXi is their product. VMware ESXi server is a hypervisor technology by VMware. Its functionally is similar to VMware ESX server but with small modifications. Full virtualization approach is used by VMware. Full virtualization in simple words means that the OS is unmodified and it doesn't need to know that other VM's are running or sharing the physical machine resources and is achieved with binary translation. In [61] VMware architecture is discussed in detail, hypervisor in VMware architecture is called "VMkernel". VMkernel provides a way for running all processes on the system which includes virtual machines. It has control of all the devices.

- **Networking**

In VMware ESXi server a VM is configured with an emulated network card which runs in the Guest Operating System. The real NIC hardware device driver runs inside VMkernel. VMware vSwitch runs inside VMkernel and it switch the packets back and forth between the guest buffers and queues and the hardware device driver's buffers and queues.

- **Storage**

ESX emulates an SCSI device in the VM which runs in the Guest OS. The real storage drive runs inside VMkernel. It supports two types of Logical units:

1) VMFS (virtual machine file system)
2) RDM (raw device mode)

- **VMotion**

ESX has the ability to move a VM from one physical server to another without noticeable downtime. This ability is called as VMotion. In order for VM migration to happen without any downtime it is necessary that storage and network are configured correctly.

3.5.2 XEN

Xen is an open source hypervisor used widely for virtualization of CPU architectures like x86 [60]. It also supports broad reach of operating systems to be used as guest OS like Linux, Windows, UNIX and Solaris. The following section will explain XEN architecture which will help us to understand how a hypervisor works and what components does it comprise. The reason to discuss XEN VMM architecture is solely related to its Open Source nature. This section will introduce us with a high level architecture as well as some general low level OS terminologies. [62] Shows the basic components of XEN based environment which are as follows:

- **XEN Hypervisor**

Hypervisor as described previously is like a software to be used as an abstraction layer which hides all the low level details from the user i.e. arranges the low-level interaction between VM and physical hardware. The main duty of a hypervisor is to control the execution of virtual machines as well as provide functions like access to physical I/O, physical memory, network etc. No VM has a direct I/O path except Dom0.

- **Domain 0**

Domain 0 is also a VM. Domain 0 has special rights to access I/O resources and it can access other VMs. It is required that Domain 0 must be loaded and run first in the system before loading any other VM. Most of the management work is done by Domain 0 and none of the guest OS has rights to access the I/O resources directly so it also communicates with the hypervisor on behalf of guest OS or Domain U PV (Paravirtualization) guest or HVM (Hardware Virtualized Machine) guest. Two drivers namely Network Backend Driver and Block Backend Driver have been incorporated in Domain 0 which take care of request from Domain U PV and HVM guests regarding network and disk requests.

- **Domain U**

Domain U unlike Domain 0 has no direct access for the resources on the physical hardware. It has to request Domain 0. Guests on Domain U are divided into two types depending on types of virtualization in general i.e. Paravirtualized virtual machine called Domain U PV guest and hardware virtual machines called Domain U HVM guest. The difference between both is, paravirtualized virtual machine run modified OS like Linux or UNIX and for hardware virtual machine unmodified OS like windows is used. There are certain limitations associated with both of them. Paravirtualized VM as stated above run modified OS and unlike hardware VM i.e. imitating each component of a typical system like memory, I/O and BIOS to the VM, it just presents the VM with an abstraction of the hardware [63].

Domain U PV guest is aware of other VM running and sharing of resources whereas Domain U HVM is not, that is why Domain U HVM machines don't have PV drivers within the virtual machine. A daemon called as Qemu-dm is started for each HVM machine on Domain 0 which handles networking and disk access requests.

3.5.2.1 Domain U and Domain 0 communication [62]

As stated before that Domain U guests can not request for memory or disk access directly but it has to communicate Domain 0 for this. In order to write something on the local disk Domain U PV guest writes the data on local memory which is shared with Domain 0. The following figure explains this interaction at a fairly high level to understand this concept.

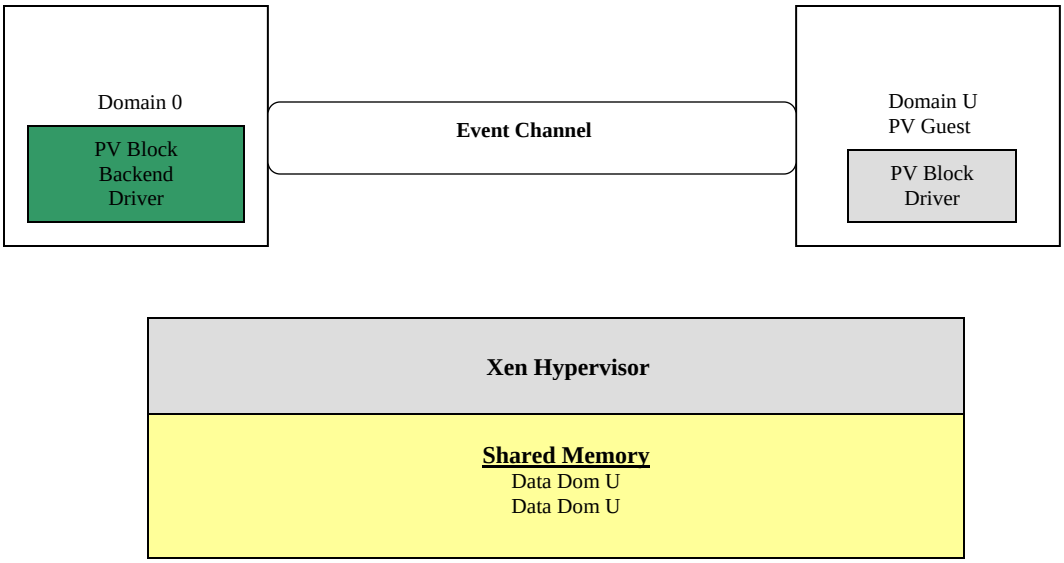


Figure 7: Domain 0 and Domain U interaction [62]

Let's suppose Domain U gets a request to write some data on the disk. Domain U will write it to local shared memory first. As shown in the figure, there is an event channel opened between both domains which help in communicating via interrupts in the XEN hypervisor.

When Domain 0 gets an interrupt from XEN hypervisor, PV Block Backend Driver will access and read the local shared memory and data is written to a specified location on the local disk space. Please note that event channel have certain interrupts which are registered in Xenstored.

3.5.2.2 XEN network configurations

Depending on the network card they can be configured to operate in different modes. Below is the explanation of these modes.

- ***Network bridge configuration mode***

Bridge default behavior is to relay frames based on MAC identifier. It is used for advanced networking purpose. It skips the network stack and connects to the network

card and transfers data directly. In this configuration mode, IP address is obtained on local ethernet and accesses the network directly. From security point of view MAC filtering is applicable in this mode through ebtables [64].

- ***Network route configuration mode***

In this mode traffic is based on IP address. Unlike bridge mode it is dependent on driver domain for routing on Ethernet, getting IP address or accessing the network. To make this mode secure we can use iptables.

Domain U guests don't have direct access and they rely on backend drivers on Domain 0, which acts as an interface between guests and the required service/hardware [64].

- ***Network NAT configuration mode:***

NAT stands for Network Address Translation. XEN NAT configuration need driver domain for working. All the guests get internal IP address from software NAT router and are inaccessible from outside (behind NAT router). Security can be implemented by using iptables.

An additional NAT layer is between guests and network card. Domain 0 driver domain is used for NAT. The guests receive internal IP address. This mode is secure obviously as not even different VM's can access each other by default. The VM's are not accessible from Internet that is why this mode is not suited to run servers on unless port forwarding is enabled in the NAT router [64].

- ***Network Host only configuration mode:***

It is a hybrid mode which creates a virtual software interface to which guests can connect. For the purpose of understanding, it can be considered as a loop back interface which is created on Domain 0 (Independent of physical network interface) [65].

3.6 Cross VM Attacks

3.6.1 Introduction

A shift towards cloud-based computing is gaining popularity among organizations irrespective of their size or role. Cloud solution for computing is bringing many benefits to organizations in terms of cost and scalability. With the growing popularity of cloud computing more and more organizations are inclining towards this change to benefit from all the promises it has made including low operational as well as capital cost.

Cloud based services like Amazon EC2 or Microsoft Azure allow user to utilize on-demand access to computing capacity and leveraging benefits for an organization in terms of economies of scale, dynamic provisioning, and low capital expenditures [66].

Third party cloud providers increase their infrastructure by usage of multi-tenancy by having multiple customer virtual machines to exist together on a single physical host. Although it is an efficient way to maximize the utilization of capital cost of cloud service provider, it introduces number of vulnerabilities.

VM in such environment share resources like CPU, memory, network, I/O etc. of the physical machine. It is possible to plan the internal cloud infrastructure, recognize where a particular target VM is likely to exist in, and then start new VMs until one is placed co-resident with the target [66].

In a traditional network, hosts are secured by placing in-depth security controls at appropriate levels which are not transparent and controlled by a customer in a public cloud infrastructure. Even though virtualization and multi-tenancy in public cloud brings a lot of benefits for users it introduces new risks, which raise some trust issues among service provider and customer.

In a typical cross VM attack an attacker use a VM to compromise other VMs on the same physical machine via side-channels between VMs to violate user's confidentiality [66]. According to [66], the attack is possible by carrying out two steps: Placement and Extraction. As the name is self explanatory Placement refers to placing a VM on same physical machine as victim and Extraction means to extract confidential information from VMs by conducting cross VM attack.

- **Amazon EC2**

One of the most popular third party cloud is Amazon EC2, which enables users to acquire computational resources. It provides user to run Linux, Windows and Solaris as guest OS in a XEN based virtualized environment. XEN hypervisor or VMM is used as an abstraction layer which controls access to hardware resources for each VM.

Amazon EC2 service can be obtained by registering for it and can create one or more virtual machine images called an *"instance"* [66].

Amazon generally provides three regions, two of them located in U.S and one in Europe. Each of these regions contains multiple *"availability zone"*. Availability zone refers to

failure mode like power and network connectivity [66]. Amazon give flexibility for users to choose between different *"instance type"* depending on their computational requirements. Different instances in Amazon cloud share same physical machine resources and each instance is provided with independent external IPv4 domain name and internal IPv4 domain name.

3.6.2 Cloud Cartography

First step in cross VM attack is to locate the target VM in the cloud. This process needs to map EC2 cloud to determine the location of different or required target VM for co-residence. In Amazon EC2 cloud, VMs can only be co-resident if they have similar creation parameters like region and instance type [66].

- **Enumerating public web servers**

The first step is to enumerate EC2 public web servers through external probes and translating all the responsive public IPs to internal IPs [66]. External probes are originated from a system outside EC2 infrastructure and the destination is an EC2 instance [66]. To achieve network probing tools like nmap, hping and wget are used. The researchers in [66] utilized WHOIS queries to identify different public IP subnets assigned to Amazon EC2 and later with the help of external network probes estimated the responsive IP addresses in all of those subnets.

- **Launching multiple EC2 instances**

Another part of this method is to launch a number of EC2 instances so that all the assigned IP addresses are analyzed in order to make an assumption.

3.6.3 How Instances are placed in EC2

In [66] different tests on EC2 derived that the instance parameters are not assigned separately from the primary infrastructure. Internal IP addressing is tightly coupled with the availability zone and instance type. In Amazon EC2 cloud, all the instances are assigned IP addresses from disjoint portion of internal IP subnet.

3.6.4 Determining Co-Residence

Before launching an attack on a VM it is important to be co-resident with the target VM. In above sections we saw how mapping can help placement of an instance on the same physical machine. The question is how to check or determine co-residence with another VM? There are few checks which can tell us how to determine that instances are co-resident with each other.

- **Matching Dom0 IP**

As discussed in the previous sections, XEN hypervisor runs a VM, which handles the management duties called Dom0. In a networked environment, DomU traffic will traverse through Dom0, which means that it has an IP address. In reality Dom0 serves as the instance first hop. One can determine its Dom0 IP address by a simple trace route. An unrestrained instance Dom0 IP address can be figured out by launching a TCP SYN trace route to it.

- **Small packet RTT**

Instances seem to be co-resident, if they have small RTT for packets. IN [66] it is analyzed that the first packet RTT in probes was slower than following probes.

- **Close IP addresses**

Internal IP addresses assigned to instances sharing same Dom0 are contiguous, it means that they are numerically closer to each other.

3.6.5 Placement of Exploit in EC2

Before the attacker achieves placement of VM on same physical machine as that of victim, [66] describes a hypothesis about how to use map and co-residence check. In [66] it is described that a single account even if running multiple instances in Amazon EC2 cannot be co-resident. So even if an attacker is running *n* instances from a single account they will be placed in *n* different machines.

In EC2 there is a strong *placement locality* [66]. It means if two instances are run sequentially, it will be co-resident and it's true for instances running in parallel.

As seen in previous sections, how a mapping is done and a check for testing co-residence in this section, we will see how we can place a VM with target VM in the same physical machine. [66] describes two methods to achieve this:

- **Brute force placement**

It is evident from its name that multiple instances run for a longer period of time and continuous effort is done, where attacker enumerates a group of possible targets. The attacker then decides with the help of a map that, which of these victims belong to a particular availability zone and particular instance type. The attacker continually runs probe instances. Probe instance checks its co-residency with the targets. If an attacker instance is not co-resident with the victim's instance, it will be ended quickly.

- **Abusing placement locality**

As explained in previous sections, parallel placement locality exists when instances run at approximately the same time. This approach can be useful in initializing new VMs on same physical machines by running instances roughly at the same time when a target VM is launched. One might think that is it a reasonable situation? Yes! The core promise of third party cloud infrastructure is to provide pay-per use capability, which gives the flexibility to a user to run the servers when needed.

3.6.6 Information Leakage

A side channel is referred to cross VM information leakage due to the sharing of physical resources like CPU, memory etc. [66]. After placing himself on the same physical machine as victim, the attacker can use side channels to get information from the target instance.

Side-channel attacks are long studied and are used to extract cryptographic keys with the help of cache based side-channels. Attacks such as exploitation of shared cache can be carried out to extract cryptographic keys from co-residents which can be damaging in the third party cloud environment [66]. An example of how cache based side-channel attack is carried out is described in following section.

- **Cache attack**

Main memory consists of CPU which is comprised of small fast memory cache shared by all applications [66]. If only an attacker accesses the cache it is being served from the fast cache, but when it is shared by the victim the cache fills up and attacker can notice slow down. The memory access pattern can be analyzed by an attacker by this slow down. For

example if a victim is decrypting an AES or RSA, access pattern is determined by shared key [66].

- **Measure of cache usage**

Measurement of cache usage can be done by an attacker to find out the current utilization of CPU cache on the physical machine. Logically speaking it is clear that a high load reflects activity on co-resident virtual machines. Cache usage can be measured by adopting PRIME+PROBE technique [67].

In [67] PRIME+PROBE mechanism is described in detail, which is used by attacker to measure the cache usage. In simple terms the attacker reads a memory location from its allocated memory space and read until fills it. The attacker waits for a random or specified amount of time until a victim uses the cache. When the attacker again reads the memory and if the usage by a victim was high, then attacker's data on the cache will be deleted which will result in high timing measurement in a time-shared virtual environment [67].

- **Cache based covert channels**

Utilizing this technique an attacker can create a covert channel. Cache based covert channels are useful in situations where network based cross VM communication is not possible. The main idea is to divide the cache in to odd and even sets i.e. read 0 for even and 1 for odd.

- **Traffic rate estimates**

This technique provides a way for knowing the number of visits to a web server residing on co-resident VM or even how many times a page is visited. If a competitor accesses theses statistics then it can be harmful.

- **Timing attacks using key stroke**

By utilizing load measurement techniques an attacker can measure the time between each key stroke by a target when typing sensitive information (password). The information obtained by the attacker can then be used to retrieve sensitive information. In a controlled lab environment this method has detected keystroke with 95% success rate [66].

3.7 VM Migration Attack

3.7.1 Introduction

Third party cloud sees live migration of VMs as a solution simplifying problems related to management and work load balancing [68]. The basic concept behind Live VM migration is to transfer a VM from one physical machine to another with minimum downtime.

The benefits available from VM migration are high ease of use, improved mobility and dynamic load sharing. Live VM migration ensures the minimized service downtime as well as the period of migration. There are three types of migration strategies namely:

- Stop and copy
- Demand migration
- Iterative pre-copy

In stop and copy techniques the source VM is stopped first and then all the pages are copied over the network. Once the files are copied, destination VM is started. The benefit for adopting stop and copy technique is less migration time, whereas down time is increased proportionally.

Demand migration technique has shortest down time of all but the migration time is increased. All the OS structures are copied and the destination VM is started while the network files are copied once a page fault is triggered.

In iterative pre-copy, as the name implies files are copied over network iteratively and the number of copied pages is kept until threshold [68]. Once threshold is met the remaining files are copied, the source VM is stopped and destination VM is started. It balances the down time and migration time. This technique is used by VMware as well as XEN for VM migration.

While an exciting technology, where a live VM is migrated from one VM to another without any stoppage of guest OS, opens door for new security challenges. If a VMM which incorporates a vulnerable migration module, can expose the guest as well as the host to attacks [68].

Researchers introduce three classes of threats to the VM migration process [68] which are as follows:

3.7.2 Control Plane

The VMM uses some sort of communication means to begin and handle live authentication of VM migrations [68]. It is possible that a malicious user can influence the control plane of a VMM and take control of the guest operating system.

It is also important that the protocols used in control plane must be protected. An attacker can intercept incoming migrations and influence the migration to its machine likewise it can influence outgoing migration and carry out a DoS attack by overloading VMM with bulk of VMs.

3.7.3 Data Plane

Data plane through which VM migrations traverse must be protected against attacks like snooping and unauthorized change so that state of a VM can be protected. Using attacks like route hijacking and/or ARP poisoning, an attacker can carry out a man-in-the-middle attack [68]. By conducting passive attacks an attacker can take out sensitive information where as a severe type of attack like manipulating memory of a VM can result in compromising a Guest OS.

3.7.4 Migration Module

Migration module provides an interface over which a VM is transferred. It is important that migration modules are resilient to attacks [68]. Simple vulnerabilities such as stack, heap and overflow in software can be exploited by an attacker to undermine a VMM. A VMM's main function is to control all guest operating systems and safeguard them, the attacker can compromise the VMM through any guest OS running within it.

Chapter 4
RESEARCH METHODOLOGY

Research Methodology is a science of conducting research or solving research problems systematically. In order to achieve the desired research goal, different relevant methods or techniques can be used [69].

For addressing the research questions and objectives of this study, the approach used is exploratory approach. An exploratory study is an important way of having the new insight of the problems and it also helps in clarifying the problems [70]. Literature review and survey are used as a research strategy in this thesis. First literature review is conducted to understand the basic concept of cloud computing and how SWAF can use cloud as a tool to secure and manage their information flow. On the basis of literature review an online survey is conducted from selected persons from different organizations and different locations to know their understanding on cloud computing and current problems faced by them in current system.

4.1 Literature Review

Literature review is very vital and significant step in any research. Good plane is needed in order to join literature review with other research steps. After literature review of publicly available material like books, article or anything related to research area, it will become easy to determine and evaluate the problem. Literature review can give reader an idea about what work have been done in the related field and how this work is different [71].

The reason for conducting literature review was to understand what exactly cloud computing is, different core technologies behind cloud computing, understanding cloud from different perspectives and to know what are the current trends of using cloud as a tool. We also focused on how we can encourage SWAF to adopt cloud environment by discussing big players in cloud computing and different organizations who are migrating to cloud environment.

Database of IEEE, Blekinge Institute of Technology and ACM digital library were used for searching relevant materials. But we were not limited to these databases only, many other sources like journals, white papers and online sources were used. After collecting literature it was critically reviewed and was narrowed down to provide a clear conclusion. The literature related to our scope was selected after going through full text.

4.2 Survey

We had planned to include some interviews with SWAF IT-staff but due to security concerns it was impossible to have some interviews or even conduct any survey at the organization. Because of security issues, our supervisors at SWAF suggested it is better to conduct survey with different IT professionals outside SWAF.

For data collection we used survey, which is easy, less time consumption and common strategy. We made the questionnaire on the basis of our extensive literature review.

After an intensive literature review and informal discussion with our colleagues who were interested in our topic, we targeted IT personnels for this survey. We made the questionnaire keeping in mind our main objectives and collected as much data as we can from the survey.

4.2.1 Sources Used for Data Collection

For our survey an online source for data collection is used, which is a web-based survey tool [72], called “Esurveyspro”. It is very cheap, easy to use and a powerful tool for the researchers and students. There is no limit for number of questions. To analyze our results we used bar charts. Results are included in Appendix A.

4.2.2 Designing Questionnaire

Designing questionnaire was an important task. We prepared questionnaire on the basis of findings form literature review in order to achieve our objectives. We prepared questionnaire in such a manner to conclude our research questions in a precise manner. Before finalizing our questionnaire we discussed many times with our colleagues and our supervisors.

4.2.3 Targeted Population

After literature review and discussion with our colleagues, we targeted IT personnels, network administrators, system assistants, network consultants, software developers, students, penetration testers, network security analysts, network and system officers etc. for this survey. Since cloud computing is in its premature stage and it's not very common among various organizations, so it was very difficult to find right people who are experts in cloud computing.

4.3 Research Questions

R1. Whether public or private cloud will be suitable for SWAF?

R2. What are the current trends in using cloud computing as a tool to secure and manage networks?

R3. What are the security issues related to cloud computing and virtualization?

R4. What are cost and performance factors in adopting cloud environment in SWAF?

Literature review and survey were used as research strategies for answering above research questions. With the help of literature review we came to know, what is cloud computing and how it can be deployed according to any organization needs, current trends and techniques of implementing cloud computing and major security issues.

Our research question 1 on whether public or private cloud will be suitable for SWAF is addressed in literature review and also in survey. Research question 2 of current trends is addressed through literature review in chapter 2 and chapter 3 when we explored for deployment models and service models. Beside core technologies and their implementation by leading vendors were also discussed. Research question 3 of security risks is targeted in detail through our literature review. In survey, we also asked 7 questions related to security and came to know the concerns of the respondent's organizations. Research question 4 was partially addressed in literature review and partially in survey.

Chapter 5
EMPIRICAL STUDY

This part of the report focuses on the empirical study that was carried out and the findings from it. To target the goal the best choice was to include individuals from enterprises already using cloud computing or are willing to migrate in the near future. This part also presents a discussion on the major findings of the various components of the literature study and survey.

5.1 Survey Results

The survey was conducted from 18 respondents, who are working professionals in small-to-medium enterprises as well as large multinational organizations. The main purpose is to have an insight on people's awareness and the perception, that has been built around cloud and virtualization due to lack of awareness. Our survey was focused particularly on organizations, to get an insight about their networks and the reason why they think migration towards cloud is needed as well as the gap between their knowledge on cloud and security issues in traditional IP networks and cloud environment in general.

Professionals who participated in this survey hold key positions but due to severity of information names are kept undisclosed. The main focus of this survey was to have an insight in to organization and respondent's view on scalability, complexity, security concerns, cost savings, data types and access control mechanisms. All of these will be discussed in the next section. This survey will give an understanding on how organization needs are aligned in terms of cloud advantages (i.e. services) and how professionals perceive some of the issues and their solutions. For convenience questionnaire is added at the end of this report. Following are the outcomes of our survey.

5.1.1 Scalability

We got mixed response about the size of the organizations of the respondents. About 38% were less than 500 employees and 27% more than 4000. Questions 2 to 5 in the survey, were related to scalability. These questions were asked to get an idea about their

future expansion. To our amazement majority of the respondents need to scale their organization. According to the survey, network resource provisioning is the reason for the delaying of network's expansion. About 72% replied that scalability is needed in the current networks and 88% replied that scalability is the reason which is driving them to go for cloud computing. In the literature review, we have learned that through virtualization we can achieve scalability.

5.1.2 Complexity

Questions 6 to 8 in the survey, were related to complexity. The complexity of current system is rated 61%, which means that current system is slightly hard to maintain. Those respondents with less population of organization replied that it is fairly simple to maintain the system. But the results show that as the organization grows the complexity also increases. So in this case the best solution can be cloud computing. When asked whether deployment, maintenance or both are complex 50% replied that maintenance is more complex. While 44% replied that both maintenance and deployment are complex. We assume from the results that maintenance is more complex. So with virtualization, company can have less number of employees to maintain the system i.e. servers storage and networks. By selecting a suitable hypervisor, the system can be maintained from one place, and it becomes fairly simple.

Although secure sharing of classified information via email should not raise any security concerns but respondents claim that, it raises security complexity. This can be addressed as sharing the classified information through established VPN channels and presence of personal firewalls.

5.1.3 Platform

In the survey, questions from 9 to 16 were related to platform. More than 50% replied that they use Linux as operating system for servers. In order to move to the cloud, a suitable hypervisor is needed. As most of the respondents choice of hypervisor is VMware. Half of the respondents replied that they use dedicated physical servers and half virtualized servers. Those with virtualized servers have already taken the step towards cloud computing and remaining can also move toward cloud. Most respondents liked that

they have their own virtualized servers running on dedicated hardware in their own datacenters. So they are very concerned about the security and do not want to opt for a hosted data center or public cloud. It is because they think that service level agreements from cloud providers can affect service availability for their organization. Also they think that private cloud in their own data centers can protect it from becoming hacker's target. The solution can be a private cloud on-premise.

5.1.4 Problems

In survey, questions related to different problems faced in network were from 17 to 20. The problem is that, companies think that cloud computing is less reliable. They even do not trust the secured VPN deployment for remote access of private data through cloud service. But a ray of hope is seen, when they are convinced that a disaster recovery infrastructure along with primary infrastructure can improve availability.

5.1.5 Security Concerns

To get to know about security concerns, questions from 21 to 27 were asked in the survey. The responsibility of ensuring security falls both on cloud provider and user. 72% respondents agreed with this. In the current environment some efforts are put into the security and control related activities by dedicating some resource percentage. In few organizations, this activity is seen less but in other the percentage is high. We have to make aware the organizations that are moving to cloud is more secure than their current environment as they don't have to dedicate extra resources for this activity.

Most of the respondents were concerned about the data loss and data theft than data integrity, identity theft, privacy, denial of service attacks, downtime and website vulnerabilities. We have to ensure the organization that their data will be safe once they move towards the cloud. And this can be achieved by cloud provider by taking every step like security protocols, encrypting the data and personal firewalls. Besides this, the single sign-on and single sign-off should be enforced to enhance security and user friendliness.

Most of the respondents agreed that their data should be encrypted both in storage and transit. When asked how much they are confident on the current network resources are secured without cloud computing. 11% replied that they are very confident, 61% replied

that they are only confident and 27% replied that they are not confident. It can be seen that more percentage of respondents are confident with their current security of network resources. 66% agreed that moving public data to cloud will be safe and by not moving the classified data to the cloud will improve the security. They do not want their sensitive data to be moved to cloud. These concerns are valid but choosing an appropriate deployment model and service model will remove their concern.

Keeping the records for logs on the same system is unsafe and the practice of respondents shows that they have taken the right measure. But some of them keep the log on same system. The main concern we have come to know is data security. General perception is that cloud is extremely unsecure. A lot of effort is needed to change the perception that cloud can be secure through proper deployment and core technologies, which build the cloud.

5.1.6 Existing Cost

In survey, questions from 28 to 30 helped us in finding issues related cost. Approximately 11 to 20 percent of respondents organization's IT budget was allocated for cloud initiatives. When asked that which is the main reason that better suits an organization's shift towards cloud computing. 16% replied that it is because of reduced cost. 5% replied that shift is because of increased security. 22% thought it is due to increased efficiency. 33% think that it is because of increased flexibility. 22% replied that all of the above four reasons were determining factors in organization's shift towards cloud computing. Respondents also say that, maintaining disaster recovery costs high keeping in view the current structure of applications, platforms and network. As moving to cloud does not require much cost, so it is better to go for cloud computing.

5.1.7 Predictable Savings

From question 31 to 33 in the survey, we have find out about the predictable savings which can be achieved by adopting cloud environment. More than 50% of respondents think that deploying virtual machines can help cut the cost. Storage, networks, servers, application licensing and IT staff were the multiple choices for the question that which cost more to maintain and scale. The high percentage of respondents, think that

application licensing cost more. Cloud computing addresses all of these domains and cost is reduced. Also moving redundancy to cloud reduces cost and most of respondents agreed with this.

5.1.8 Data types

In the survey, questions related to data types were from 34 to 38. Most respondents replied that they have more web traffic in their networks. Confidential data is relevant to which type of organization it is. As far as confidentiality is concerned, it depends on the organization whether they want to move sensitive data to cloud or not. Most respondents think that financial application is too risky to be moved to cloud. From our literature and survey we come to know that issues like data flow, confidentially of data and risky applications can be targeted through deployment model and technologies used in a cloud.

5.1.9 Access Control Management

In the survey, questions related to access control management were from 39 to 41. Access control lists are used in most organizations as access control management. Most companies do not want to disclose whether an inside breach by an authorized user had ever happened. Organization is more concerned about the security model being deployed by the cloud provider.

5.1.10 Potential Threat

In the end of the survey, questions from 42 to 47 were related to potential threats. Viruses are the main security threat experienced by the network administrators. Biggest challenges to adopt cloud computing are integration with the existing systems and network security. The roadmap to cloud computing is to separate the public and private data from the network. Penetration testing by customer can help building the trust on cloud service provider security plan.

5.2 Discussion

This thesis has presented a detailed study on the implementation of cloud environment for a secure organization such as SWAF. We have categorized our study in a manner so

that, we can first find out why we should use cloud infrastructure and later we have studied virtualization in detail, as a technique to secure and manage the information flow. We planned to provide SWAF with enough proof to make them aware of cloud based services in their network.

We had to gather enough arguments and concrete evidence to do that. We started our research by our literature review in which we read in detail and understood the basics of cloud computing. Our literature review provided us with a flood of knowledge related to cloud computing which we had to filter that to our needs. From the initial studies we came to know that cloud has different deployment models, of which private cloud is perceived as more secure.

Further we linked our literature studies with different service models provided by vendors to different organizations. We discussed about different common characteristics, benefits and security concerns in cloud infrastructure. Survey questions in section 5.1.1 also showed that scalability is the major reason for organizations to adapt cloud infrastructure. Hence we further studied on a list of different vendors, their services, their clients and the tools being used to provide these services for different organizations. This led to much encouragement to adapt cloud infrastructure.

To find out how these infrastructures are implemented specially related to monitoring and securing of data, so we can suggest one for SWAF. Initial studies related to the present market competitors and their implementation strategies showed us that virtualization as the most used technology. We thoroughly discussed general benefits, security benefits, different types and most used tools for virtualization. This led us to specified tools like hypervisors being used to implement this technology. In our survey we found out the most of the industry is using VMware or Xen as hypervisors.

We then focused on VMware (proprietary) and Xen (open source) as a tool to monitor and secure a network. Most of the details were related to Xen architecture and its network configurations as we should also keep in mind the standardization issues which might cause a vendor lock in, if proprietary tools are used. We further discussed implementation of cloud services provided by one of the largest vendor from where, we pointed different security threats involved in that network. In the survey we observed that most of the

professionals were much concerned about the data loss and data theft, which can be avoided by disaster recovery tools also.

Cost is one of the major role players in the migration of organizations to cloud network. We have taken into account the cost of public clouds and their policies related to costs. In the survey we came to know that organizations are willing to spend more resources on cloud based environments if they are assured of better reliability and data security. More professionals think that virtualization is the only technique which can help cut costs in their networks, as expenses on maintenance are already high. More data capacity is required for expansion of network, which becomes even more costly. Hence virtualization is the only cheap solution for such hindrances.

Chapter 6
CONCLUSIONS

6.1 Conclusion

This chapter focuses on the results found in our research to derive a conclusion in order to answer our research questions. This study is about having a deep look on cloud computing for finding out, whether cloud computing is mature enough so that it can be adopted by SWAF as a tool to secure and manage their information flow. Survey has been conducted to conclude, which technology fulfils our goals and to understand the general perception of IT professionals to migrate to cloud technology.

This research provides the research required to build confidence of different organizations towards cloud. The literature review is comprised of detailed study on cloud computing in general and some of the security issues or vulnerabilities. It also focuses on the security awareness in general and then focuses on virtualization details as well as some of practical security issues like cross VM attacks and VM migration attacks. The survey consists of cloud and security related questions which provided us with insights from respondent's views about their present networks and how they foresee an "ideal" cloud infrastructure. All this work has helped us to provide a better landscape for SWAF. From our study certain results are gathered which persuaded us to conclude.

- The data security, reliability and privacy issues for an organization such as SWAF with high level of security we would suggest a private cloud approach will be much safer. People perceive that cloud computing is not secure, but the reality is cloud environments can be extremely secure and security can range to fit a particular business's needs. Using on-premise hosting, dedicated servers, strict network policies, IDPS, firewall, strong encryption, AAA etc can make a private cloud network reliable.
- Virtualization is a widely used technique for scalability and from our research we have come to know that, it is matured and highly reliable also. Further tools like Xen should be implemented as it is an open source tool which avoids vendor lock in. It has proved to be a reliable tool for monitoring and securing a cloud network.

- Different security threats in cloud computing such as data integrity, data theft, privacy issues, infected applications, data ownership, and identity access management are described in literature review and questioned in survey. At the same time their prevention techniques are also described which should be implemented by cloud vendors and customers. Further a detailed study of cross VM attacks and VM migration attacks show the security risks related to virtualization technique, these threats give rise to problems, such as information leakage and data theft. On the basis of these attacks, it can be concluded that public cloud is more vulnerable to external attacks. Access control management is an essential part of military security policy which avoids these attacks, while using private cloud.
- Cost is considered to be the most effective element in implementation of cloud infrastructure in an organization. Virtualized environments provide better allocation of resources and easy maintenance of network elements. It should be noted that, cloud computing is based on automated systems which reduces human resources. Even if the redundant resources are moved to virtualized environments it could save a lot of money. Moreover latency concerns like network latency, processing latency and client side latency are the performance factors which can be improved using better bandwidth and right configurations on edge devices.

6.2 Future Work

This thesis provides the basic research work needed for the deployment of cloud infrastructure in new organizations. We have provided the present trends in market as well as the technologies that can be cost effective and secure if implemented. Future research work can be comprised of looking more and more closely in to virtualization technique and its implementation. More work is also required on migration of a small part of network with public data on a cloud for experimental bases which could even give further exploration on practical basis. This research work can also be used in future to supplement the decision for building a framework or a model.

REFERENCES

[1] C. Cachin, I. Keidar, and A. Shraer, "Trusting the Cloud," SIGACT News, pp.81-86, 2009.

[2] D. N. Chorafas, "Cloud Computing Strategies," CRC press, 2010.

[3] U.S. Air Force Selects IBM to Design and Demonstrate Mission-Oriented Cloud Architecture for Cyber Security. [Online]. Available: http://www-03.ibm.com/press/us/en/pressrelease/29326.wss, accessed on March 2012.

[4] I. Frank, A. Oludele, and O. Shade, "Cloud Computing Security Issues and Challenges," *International Journal of Computer Networks (IJCN)*, p. 247, 2011.

[5] H. Xu, M. Song, J. Peng, and Q. Yu, "Research on Telecom Service Deployment in Cloud Environments," *5th IEEE International Conference on Pervasive Computing and Applications*, pp.189-194, 2010.

[6] L. Yousef, M. Butrico, and D. Da Silva, "Towards a Unified Ontology of Cloud Computing," *Grid Computing Environments Workshop,* pp.1-10, 2008.

[7] New IDC IT Cloud Services Survey: Top Benefits and Challenges. [Online]. Available: http://blogs.idc.com/ie/?p=730, accessed on February 2012.

[8] H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security and Privacy*, vol. 8, pp.24-31, 2010.

[9] Security Guidance for Critical Aread of Focus in Cloud Computing V2.1. [Online]. Available: https://cloudsecurityalliance.org/csaguide.pdf, accessed on February 2012.

[10] R. Chakraborty, S. Ramireddy, T.S. Raghu and H. R. Rao, "The Information Assurance Practices of Cloud Computing Vendors," vol.12, pp.29-37, 2010.

[11] Introduction to Cloud Computing. [Online]. Available: http://www.dialogic.com/Solutions/CloudCommunications/Build/~/media/products/docs/whitepapers/12023-cloud-computing-wp.pdf , accessed on February 2012.

[12] Cloud Deployment Models – Private, Community, Public, Hybrid with Examples. [Online]. Available: http://www.techno- pulse.com/2011/10/cloud-deployment-private-public-example.html, accessed on February 2012.

[13] Cloud: Public or private? [Online]. Available: http://www.networkworld.com/community/tech-debate-private-public-cloud, accessed on February 2012.

[14] What is the difference between public clouds and a private cloud.[Online]. Available:http://blog.eukhost.com/webhosting/what-is-the-difference-between-public-clouds-and-a-private-cloud/, accessed on February 2012

[15] X. Zhang, H. Du, J. Chen, Y. Lin, and L. Zeng, "Ensure Data Security in Cloud Storage," *IEEE International Conference on Network Computing and Information Security*, pp.284-287, 2011.

[16] News Briefs, "Amazon's Massive Cloud Hosting Site Crashes," *IEEE Computer Magazine*, vol. 44, pp.18-20, 2011.

[17] A. T. Velte, T. J. Velte and R. C. Elsenpeter, "Cloud Computing, A practical approach," USA: McGraw-Hills, 2009.

[18] Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business. [Online]. Available:http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/CloudComputingLumley.pdf, accessed on February 2012.

[19] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing*, vol.14, pp.14-22, 2010.

[20] V. D. Cunsolo, S. Distefano, A. Puliafito and M. Scarpa, "Achieving Information Security in Network Computing Systems,", *8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp.71-77, 2009.

[21] How to Negotiate a Better Cloud Computing Contract. [Online]. Available: http://www.cio.com/article/591629/How_to_Negotiate_a_Better_Cloud_Computing_Contract, accessed on March 2012.

[22] W. Jansen and T.Grance, "Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology Special Publication 800-144*, 2011.

[23] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *44th Hawaii International Conference on System Sciences (HICSS)*, pp.1-10, 2011.

[24] D. Hilley, "Cloud computing: A taxonomy of platform and infrastructure-level offerings," *Georgia Institute of Technology*, 2009.

[25] IBM Unveils Next Generation Smart Cloud Platform for Business. [Online]. Available:http://www-03.ibm.com/press/us/en/pressrelease/34197.wss, accessed on March 2012.

[26] Openstack cloud software. [Online]. Available: http://www.openstack.org/, accessed on February 2012.

[27] Eucalyptus Systems, Inc. [Online]. Available: http://www.eucalyptus.com/, accessed on February 2012.

[28] M. Jlelaty and Y. Monzer, "Factors in Cloud Computing Adoption," *M.S. Thesis, Department of Informatics, Lund University*, May 2012.

[29] W. Kim, S. D. Kim, E. Lee and S. Lee, "Adoption Issues for Cloud Computing," *7th International Conference on Mobile Computing and Multimedia*, 2009.

[30] D. Verchere, "Cloud computing over telecom network," *IEEE conference on Optical Fiber Communications Conference and Exposition, and National Fiber Optic Engineers Conference*, 2011.

[31] S. Wee, "Debunking Real-Time Pricing in Cloud Computing," *11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp.585-590, 2011.

[32] M. Zink, P. Shenoy, D. Irwin, and E. Cecchet, "Options and Cost implications for GENI network connectivity with Amazon EC2 cloud resources," *DiCloud Deliverables S2.b, University of Massachusetts, Amherst*, 2009.

[33] S. Ortiz, "The Problem with Cloud-Computing Standardization," *IEEE Journal on Computer*, vol. 44, pp.13-16, 2011.

[34] Open Virtualization Format White Paper. [Online]. Available: http://www.dmtf.org/sites/default/files/standards/documents/DSP2017_1.0.0.pdf, accessed on March 2012.

[35] Cloud Computing Use Cases WhitePaper. [Online]. Available: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf, accessed on July 2011.

[36] D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *IEEE Symposium on Security and Privacy*, 1987.

[37] I. Menken and G. Blokdijk, "Cloud Computing Virtualization Specialist Complete Certification Kit - Study Guide Book and Online Course," Emereo Pty Ltd, 2009.

[38] J. Sahoo, S. Mohapatra, and R. Lath, “Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues,” pp.222-226, 2010.

[39] B. Grobauer, T. Walloschek, E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security and Privacy,* vol.9, pp.50-57, 2011.

[40] Q. Liu, C. Weng, M. Li and Y. Luo, "An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds," *IEEE Security and Privacy,* vol.8, pp.56-62, 2010.

[41] D. Hyde, “A Survey on the Security of Virtual Machines,” *Dept. of Comp. Science, Washington Univ. in St. Louis, Tech. Rep.*, 2009.

[42] J. E. Smith and R. Nair, “Virtual Machines: Versatile Platforms for Systems and Processes,” Morgan Kaufman, 2005.

[43] J. E. Smith and R. Nair, “The Architecture of Virtual Machines,” *IEEE Computer Society,* pp.32-38, 2005.

[44] S. J. Vaughan-Nichols, “New Approach to Virtualization is Lightweight,” *IEEE Computer Society,* pp.12-14. 2006.

[45] L4Ka Project: Pre-virtualization. [Online]. Available:http://www.l4ka.org/79.php, accessed on February 2012.

[46] H. Takabi, J. B. D. Joshi and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security and Privacy*, vol.8, pp.24-31, 2010.

[47] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt and A. Warfield, “Xen and the Art of Virtualization,” *19th ACM symposium on Operating systems principles*, pp.164-177, 2003.

[48] VMWare ESX and ESXi product page. [Online]. Available: http://www.vmware.com/products/esx/index.html, accessed on March 2012.

[49] J. Sugerman, G. Venkitachalam and B.H. Lim, “Virtualizing I/O Devices on VMware Workstation’s Hosted Virtual Machine Monitor,” *USENIX Annual Technical Conference,* pp.1-14, 2001.

[50] VMWare Workstation product page. [Online]. Available. http://www.vmware.com/products/workstation/index.html, accessed on March 2012.

[51] J. Watson, “VirtualBox: Bits and Bytes Masquerading as Machines,” *Linux Journal*, 2008.

[52] F. Armand and M. Gien, "A Practical Look at Micro-Kernels and Virtual Machine Monitors," *IEEE Consumer Communications and Networking Conference*, pp.1-7, 2009.

[53] A. Seshadri, M. Luk, N. Qu and A. Perrig, "SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes," *21st Symposium on Operating System Principles(SOSP)*, pp.335-350, 2007.

[54] T. Shinagawa and others, "BitVisor: A Thin Hypervisor for Enforcing I/O Device Security," *International conference on Virtual Execution Environments (VEE)*, pp.121-130, 2009.

[55] D. R. K. Ports and T. Garfinkel, "Towards Application Security on Untrusted Operating Systems," *USENIX Workshop on Hot Topics in Security (HOTSEC)*, 2008.

[56] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum and D. Boneh, "Terra: A Virtual Machine-Based Platform for Trusted Computing," *19th Symposium on Operating System Principles(SOSP)*, pp.193-206, 2003.

[57] L. Litty, H. Andrés Lagar-Cavilla and D. Lie, "Hypervisor Support for Identifying Covertly Executing Binaries," *17th USENIX Security Symposium*, pp.243-258, 2008.

[58] T. Garfinkel and M. Rosenblum, "A Virtual Machine IntrospectionBased Architecture for Intrusion Detection," *Proc. Network and Distributed Systems Security Symposium*, 2003.

[59] P. Muditha Perera and C.Keppitiyagama, "A Performance Comparison of Hypervisors," *International Conference on Advances in ICT for Emerging Regions (ICTer)*, 2011.

[60] J. Che, Q. He, Q. Gao, D. Huang, "Performance Measuring and Comparing of Virtual Machine Monitors," *International Conference on Embedded and Ubiquitous Computing*, vol.2, pp.381-386, 2008.

[61] Understanding Full Virtualization, Paravirtualization, and Hardware Assist. [Online]. Available: http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf, accessed on March 2012.

[62] How Does Xen Work? [Online]. Available: http://www.xen.org/files/Marketing/HowDoesXenWork.pdf, accessed on March 2012.

[63] An Overview of XEN Virtualization. [Online]. Available: http://www.dell.com/downloads/global/power/ps3q05-20050191-Abels.pdf, accessed on March 2012.

[64] Introduction to the Open Source Xen Hypervisor. [Online]. Available: http://support.bull.com/ols/product/system/linux/redhat/doc/docf/g/DC000040/xen_training_sessions_2009.pdf, accessed on April 2012.

[65] Xen 'host-only" networking. [Online]. Available: http://blog.rabidgeek.com/?p=128, accessed on April 2012.

[66] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," *16th ACM Conference on Computer and Communications Security*, pp.199-212, 2009.

[67] D. Page, "Defending Against Cache-Based Side-Channel Attacks," *Information Security Technial Report*, vol. 8, pp.30-44, 2003.

[68] J. Oberheide, E. Cooke, F. Jahanian, "Empirical Exploitation of Live Virtual Machine Migration," *Black Hat Security Conference*, 2008.

[69] C.R. Kothari, "Research Methodology: Methods and Techniques," India: New Age International Publishers, 2004.

[70] M. Saunders, P.Lewis, and A. Thornhill,"Research Methods for business students," England: Pearson Education Limited, 2007.

[71] L.E. Reed, "Performing a Literature Review," *28th IEEE Annual Frontiers in Education Conference*, pp.380-383, 1998.

[72] Esurveyspro. [Online]. Available: http://www.esurveyspro.com/, accessed on February 2012.

APPENDIX A

SURVEY QUESTIONNAIRE & RESULTS

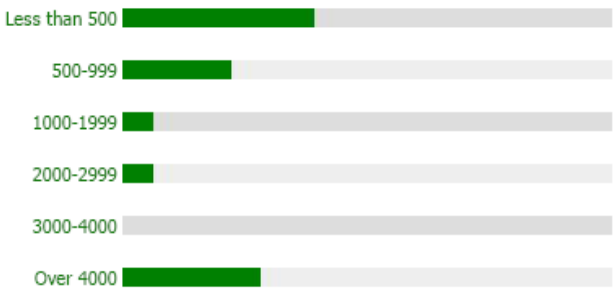
1. Personal Background

Full Name	17
Organization	17
Department	15
Designation	17
Number of Respondents	17
Number of respondents who skipped this question	1

Scalability

2.

What is the size of your organization?



Number of respondents	***18***
Number of respondents who skipped this question	***0***

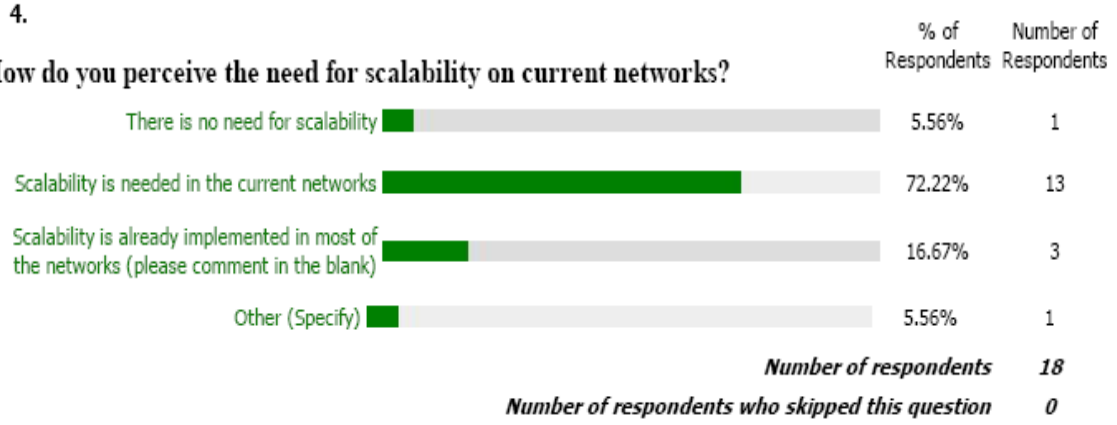
3.

Do you think that network resource provisioning is an important factor in delaying the network expansion in current networks?

Number of respondents	***18***
Number of respondents who skipped this question	***0***

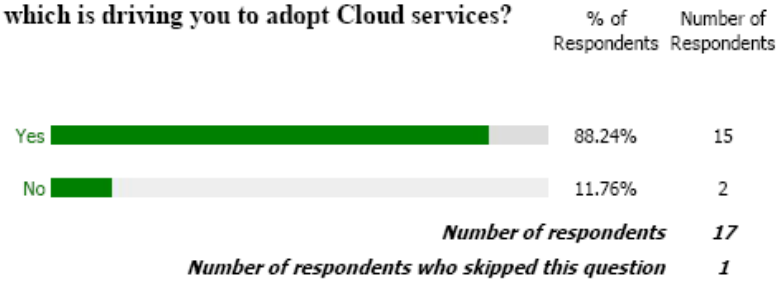
4.

How do you perceive the need for scalability on current networks?



5.

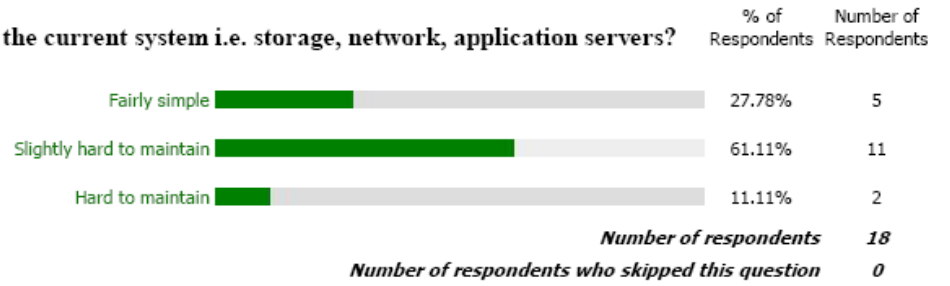
Is Scalability one of the factors which is driving you to adopt Cloud services?



Complexity

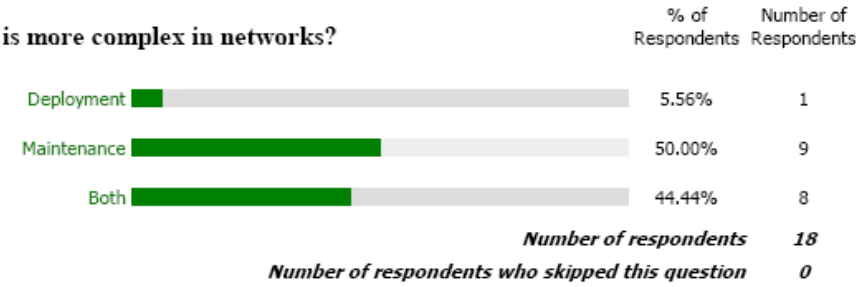
6.

How complex is the current system i.e. storage, network, application servers?

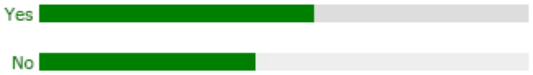


7.

Which type of servicing is more complex in networks?



8. Do you think sharing of classified information via secure mail to group of people brings security complexity?

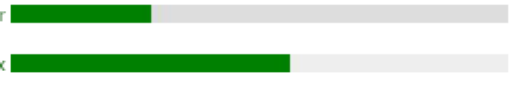


	% of Respondents	Number of Respondents
Yes	55.56%	10
No	44.44%	8
Number of respondents		***18***
Number of respondents who skipped this question		***0***

Platform

9.

Which operating system do you use for servers?



	% of Respondents	Number of Respondents
MS Windows server	27.78%	5
Linux	55.56%	10
Solaris	0.00%	0
Unix	11.11%	2
Other	5.56%	1
Number of respondents		***18***
Number of respondents who skipped this question		***0***

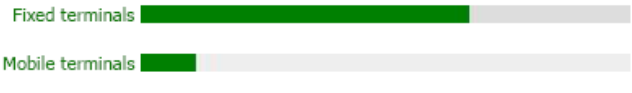
10.

Which operating system do you use for client?

	% of Respondents	Number of Respondents
MS Windows	72.22%	13
Linux	22.22%	4
Solaris	0.00%	0
Unix	5.56%	1
Other	0.00%	0
Number of respondents		***18***
Number of respondents who skipped this question		***0***

11.

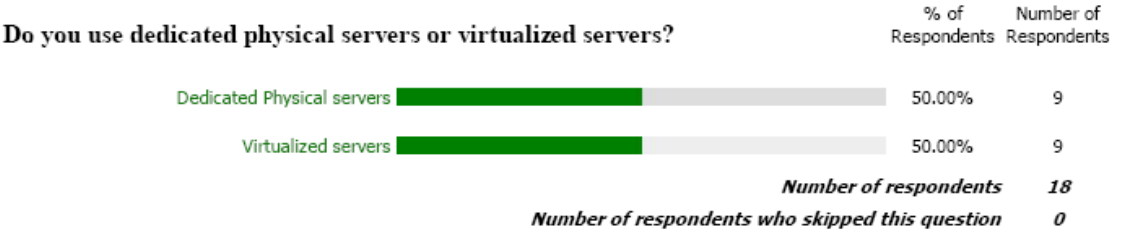
What type of terminals/nodes you use most often?



	% of Respondents	Number of Respondents
Fixed terminals	66.67%	12
Mobile terminals	11.11%	2
Not sure	22.22%	4
Number of respondents		***18***
Number of respondents who skipped this question		***0***

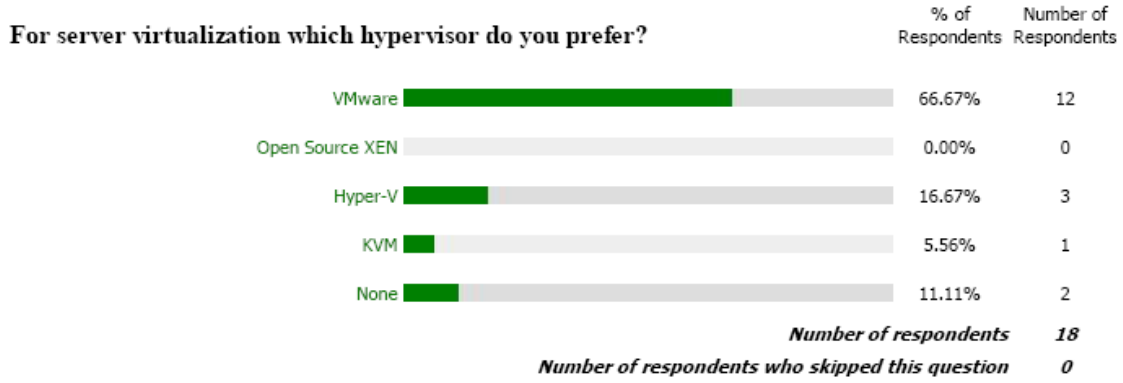
12.

Do you use dedicated physical servers or virtualized servers?



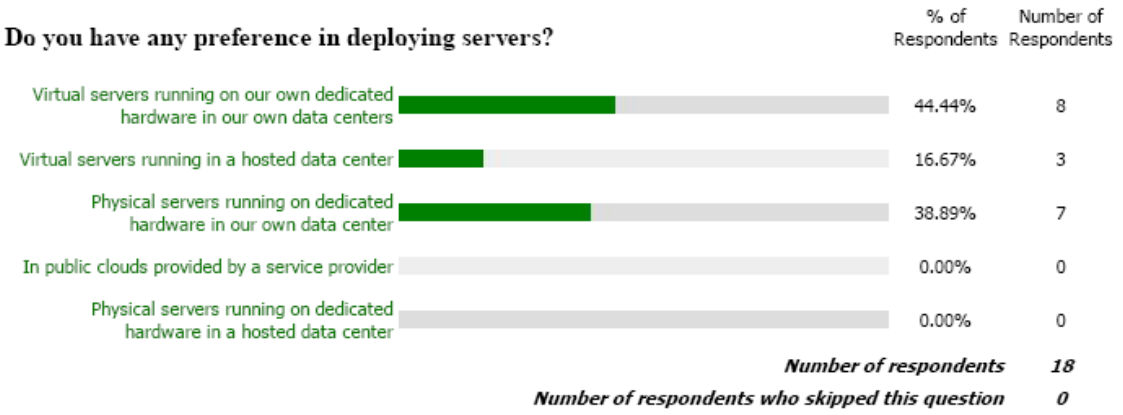
13.

For server virtualization which hypervisor do you prefer?



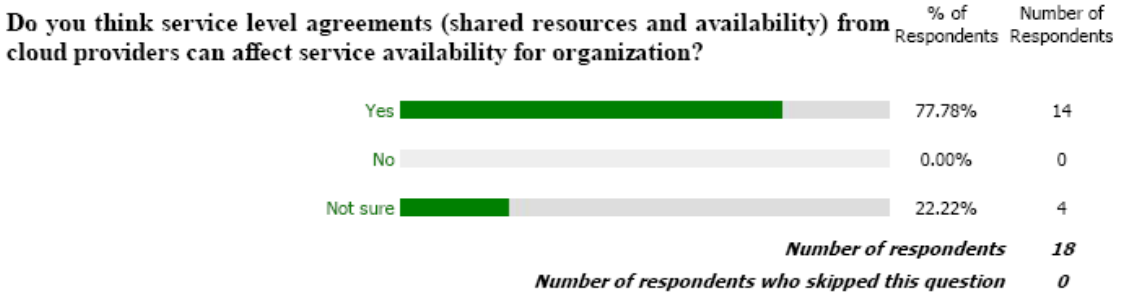
14.

Do you have any preference in deploying servers?



15.

Do you think service level agreements (shared resources and availability) from cloud providers can affect service availability for organization?



16.

Do you think running cloud based solutions for government agencies on their intranets on their servers; in their data center can protect it becoming Hackers target?

	% of Respondents	Number of Respondents
Yes	50.00%	9
No	50.00%	9
Number of respondents		***18***
Number of respondents who skipped this question		***0***

Problems

17.

Which of these factors you think can affect the trust of companies from cloud computing if compromised?

	% of Respondents	Number of Respondents
Less Scalability	0.00%	0
Less Reliable	35.29%	6
High Cost	23.53%	4
Less platform transparency	17.65%	3
All of the above	23.53%	4
Number of respondents		***17***
Number of respondents who skipped this question		***1***

18.

How do you classify the structure of the application in your organization?

	% of Respondents	Number of Respondents
Very Structured	17.65%	3
Structured	76.47%	13
Not so Structured	5.88%	1
Number of respondents		***17***
Number of respondents who skipped this question		***1***

19.

Do you think remote access of private data through cloud service can be a problem even after deploying secured VPN?

	% of Respondents	Number of Respondents
Yes	50.00%	9
No	22.22%	4
Unsure	27.78%	5
Number of respondents		***18***
Number of respondents who skipped this question		***0***

20.

Do you think having a disaster recovery infrastructure along with primary infrastructure can improve availability?

	% of Respondents	Number of Respondents
Yes	100.00%	18
No	0.00%	0
Number of respondents		*18*
Number of respondents who skipped this question		*0*

Security Concerns

21.

Who does you thinks is responsible for ensuring security in the cloud?

	% of Respondents	Number of Respondents
Cloud service provider	27.78%	5
Cloud service user	0.00%	0
Shared responsibility of provider and user	72.22%	13
Number of respondents		*18*
Number of respondents who skipped this question		*0*

22.

How much effort and resource percentage is dedicated to security and control related activities?

	% of Respondents	Number of Respondents
Between 0-10%	38.89%	7
Between 11-20%	16.67%	3
Between 21-50%	33.33%	6
more than 50%	11.11%	2
Number of respondents		*18*
Number of respondents who skipped this question		*0*

23.

What do you consider is the most important security threat for your organization?

	% of Respondents	Number of Respondents
Data loss/Theft	27.78%	5
Data Integrity	16.67%	3
Identity theft	0.00%	0
Privacy	11.11%	2
Denial of Service Attacks	0.00%	0
Downtime	22.22%	4
Website vulnerabilities	22.22%	4
Number of respondents		*18*
Number of respondents who skipped this question		*0*

24.

Do you prefer your data to be encrypted both in storage and in transit?

	% of Respondents	Number of Respondents
Yes	83.33%	15
No	16.67%	3
Number of respondents		***18***
Number of respondents who skipped this question		***0***

25.

How much are you confident that the current network resources are secured without cloud computing?

	% of Respondents	Number of Respondents
Very confident	11.11%	2
Confident	61.11%	11
Not confident	27.78%	5
Number of respondents		***18***
Number of respondents who skipped this question		***0***

26.

Most of the government agencies hold their public and private data in same network. Do you think moving public data to cloud can improve security for classified data?

	% of Respondents	Number of Respondents
Yes	66.67%	12
No	33.33%	6
Number of respondents		***18***
Number of respondents who skipped this question		***0***

27.

Are the record for logs is kept on the same system which is being logged?

	% of Respondents	Number of Respondents
Yes	50.00%	9
No	50.00%	9
Number of respondents		***18***
Number of respondents who skipped this question		***0***

Existing Cost

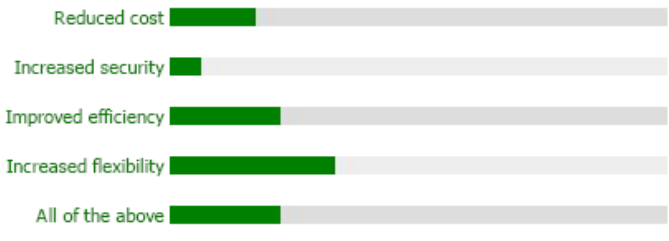
28.

Approximately, what percent of your organizations IT budget will be allocated to cloud computing initiatives?

	% of Respondents	Number of Respondents
Between 0-10%	44.44%	8
Between 11-20%	44.44%	8
Between 21-50%	11.11%	2
More than 50%	0.00%	0
Number of respondents		***18***
Number of respondents who skipped this question		***0***

29.

Which is the main reason that better suit an organization's shift towards cloud computing?

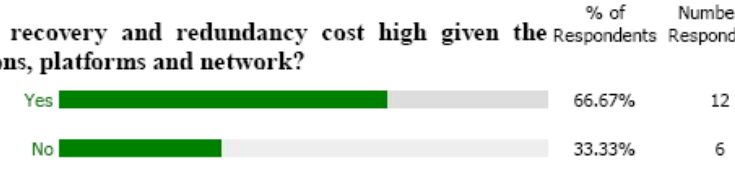


Number of respondents ***18***

Number of respondents who skipped this question ***0***

30.

Does maintaining a Disaster recovery and redundancy cost high given the current structure of applications, platforms and network?



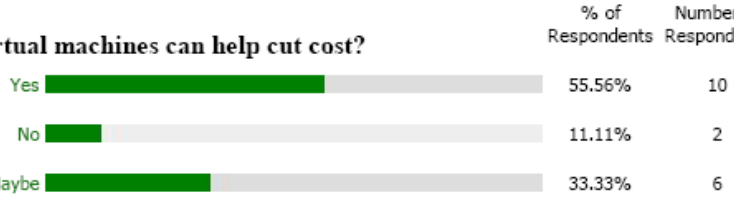
Number of respondents ***18***

Number of respondents who skipped this question ***0***

Predictable Savings

31.

Do you think that deploying Virtual machines can help cut cost?

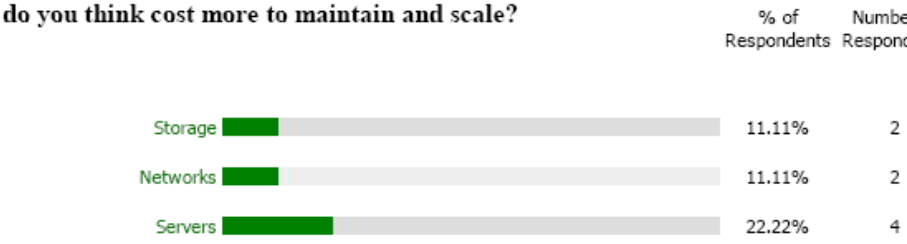


Number of respondents ***18***

Number of respondents who skipped this question ***0***

32.

Which domains do you think cost more to maintain and scale?

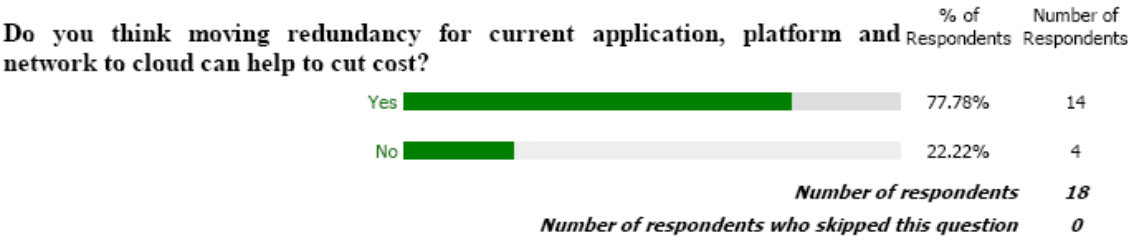


Number of respondents ***18***

Number of respondents who skipped this question ***0***

33.

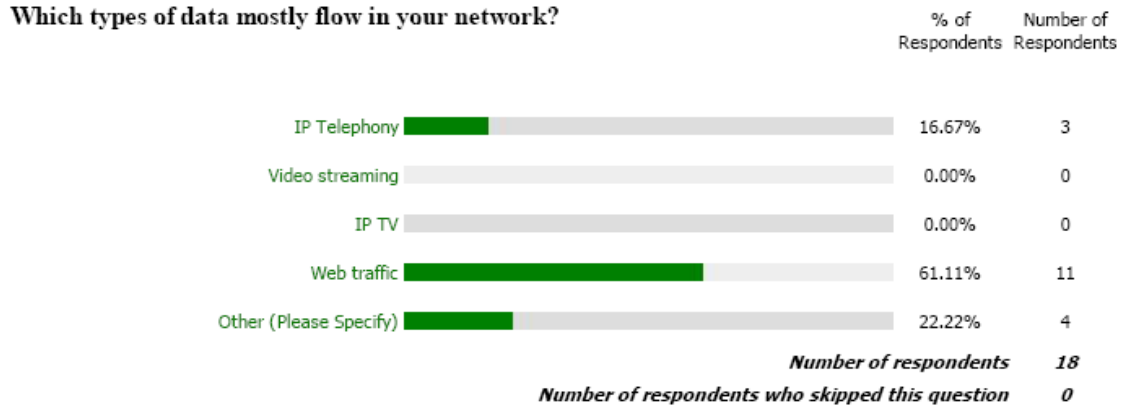
Do you think moving redundancy for current application, platform and network to cloud can help to cut cost?



Data Types

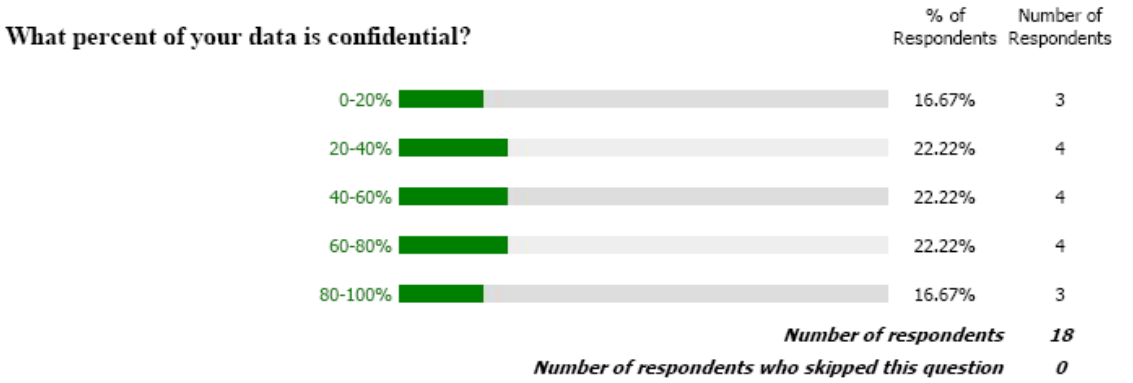
34.

Which types of data mostly flow in your network?



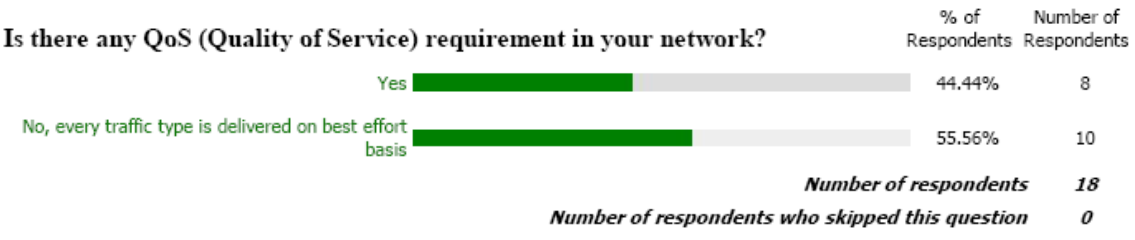
35.

What percent of your data is confidential?



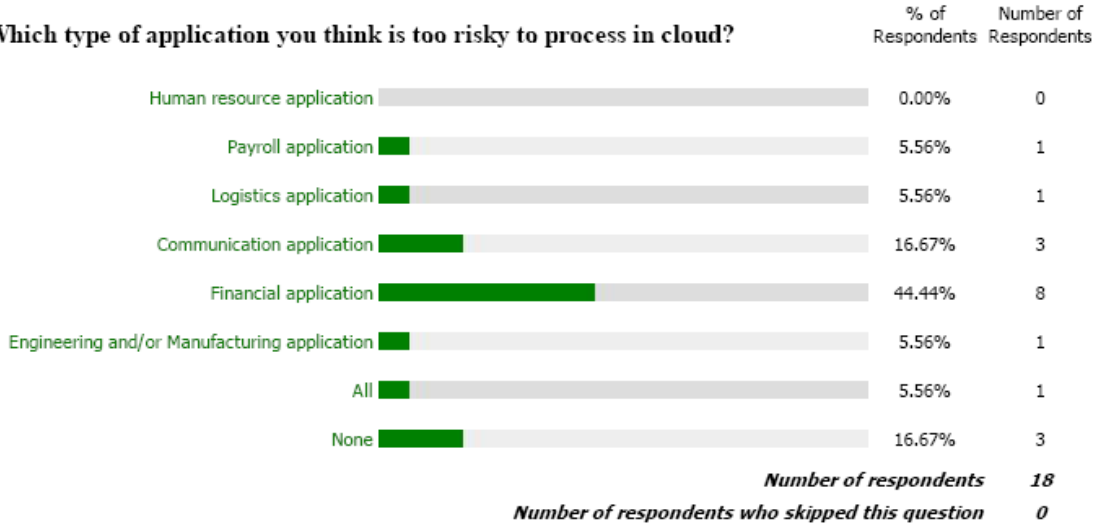
36.

Is there any QoS (Quality of Service) requirement in your network?



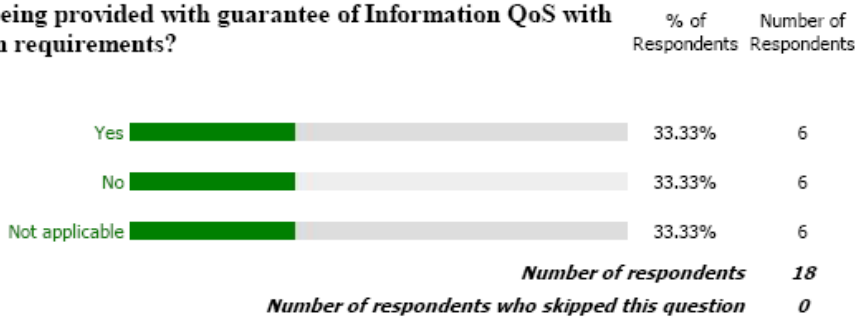
37.

Which type of application you think is too risky to process in cloud?



38.

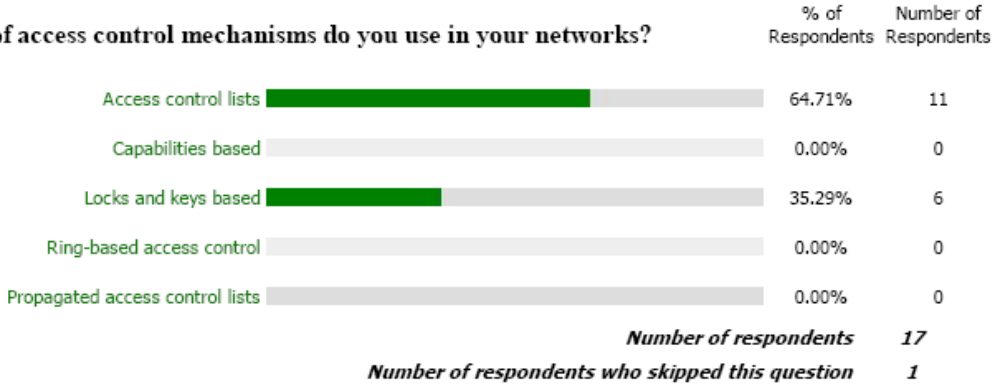
Are the network users being provided with guarantee of Information QoS with time critical information requirements?



Access Control Management

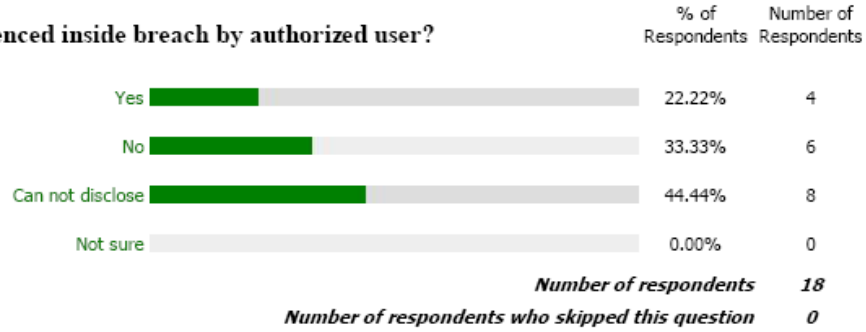
39.

What type of access control mechanisms do you use in your networks?



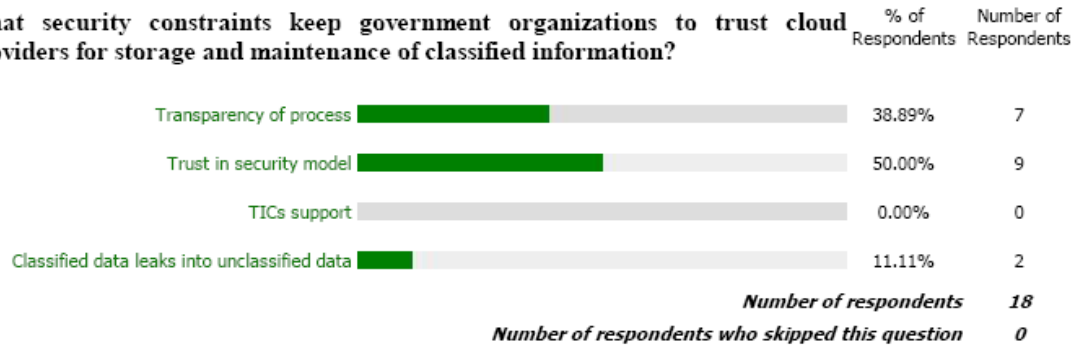
40.

Have you ever experienced inside breach by authorized user?



41.

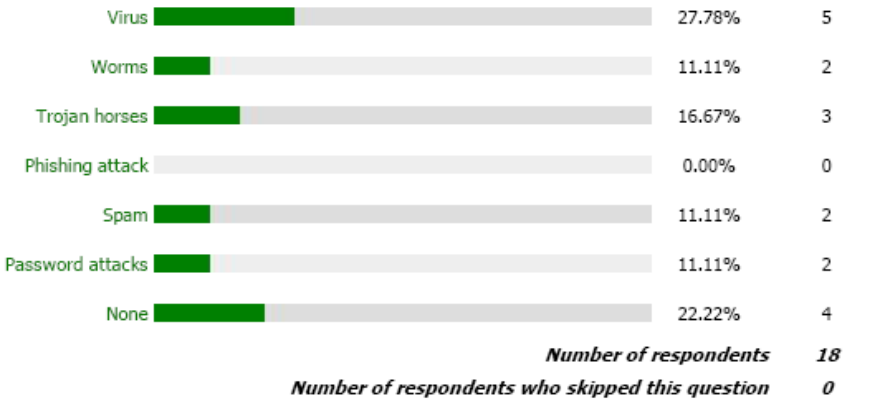
What security constraints keep government organizations to trust cloud providers for storage and maintenance of classified information?



Potential Threats

42.

Which of the following network security threats have been experienced by network administrators?



43.

Are you satisfied with the disaster recovery and business continuity plans for the current network?

	% of Respondents	Number of Respondents
Yes satisfied	27.78%	5
Partially satisfied	55.56%	10
Not satisfied	16.67%	3
Number of respondents		***18***
Number of respondents who skipped this question		***0***

44.

What are biggest challenges according to you for adopting Cloud environment?

	% of Respondents	Number of Respondents
IT governance issues	5.56%	1
Integration with the existing systems	33.33%	6
System and Network security	38.89%	7
Control over the applications	11.11%	2
Application security	5.56%	1
Physical security	5.56%	1
Number of respondents		***18***
Number of respondents who skipped this question		***0***

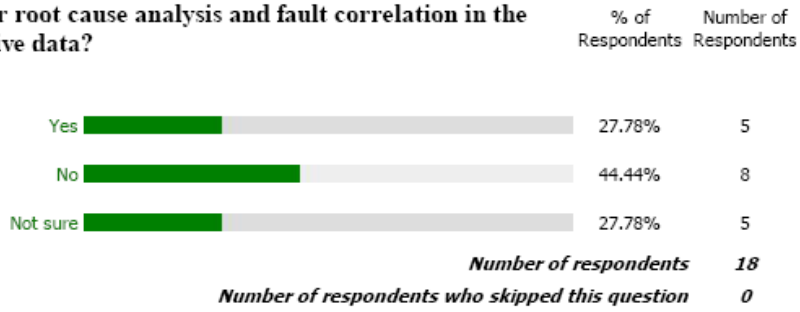
45.

What should be the roadmap to adopt Cloud Environment for classified information?

	% of Respondents	Number of Respondents
Migration to public cloud	16.67%	3
Migration to private cloud	11.11%	2
Migration to hybrid solution	0.00%	0
Separation of public and private data from network	50.00%	9
Usage of government existing data center's servers and storage	11.11%	2
Not sure	11.11%	2
Number of respondents		***18***
Number of respondents who skipped this question		***0***

46.

Is there a model to follow for root cause analysis and fault correlation in the wireless networks for sensitive data?



47.

Penetration testing on a regular basis can help to maintain a check on server and network security but do you think penetration testing via 3rd party or even a customer can help building trust on cloud service provider security plan?