

**Research Based Project On  
“Effective Approach of Analyzing Security Attacks and Implementing the  
Solutions in Cloud Computing”**

**BY**

Abir Hossain

ID : 161-15-6923

Akib Mahmud Tonmoy

ID : 161-15-7422

Abdul Aziz Opu

ID : 161-15-6825

Md. Faysal Hossain

ID : 161-15-7416

This Report Presented in Partial Fulfillment of the Requirements for the Degree  
of Bachelor of Science in Computer Science and Engineering

**Supervised By**

Md. Rakib Hasan

Lecturer

Department of CSE

Daffodil International University

Co-Supervised By

Daffodil International University



**DAFFODIL INTERNATIONAL UNIVERSITY**

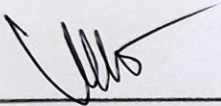
**DHAKA, BANGLADESH**

**December 2019**

## APPROVAL

This Project/internship titled “**Effective Approach of Analyzing Security Attacks and Implementing the Solutions in Cloud Computing**”, submitted by Abir Hossain, Akib Mahmud Tonmoy, Abdul Aziz Opu, Md. Faysal Hossain, ID No: 161-15-6923, 161-15-7422, 161-15-6825, 161-15-7416 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 06-12-2019.

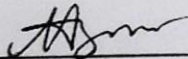
## BOARD OF EXAMINERS



---

**Dr. Syed Akhter Hossain**  
**Professor and Head**  
Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

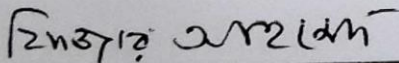
**Chairman**



---

**Nazmun Nessa Moon**  
**Assistant Professor**  
Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

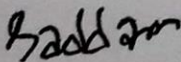
**Internal Examiner**



---

**Dr. Fizar Ahmed**  
**Assistant Professor**  
Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



---

**Dr. Md. Saddam Hossain**  
**Assistant Professor**  
Department of Computer Science and Engineering  
United International University

**External Examiner**

## DECLARATION

We hereby declare that this project has been done by us under the supervision of MD. RAKIB HASAN, Lecturer, Department of CSE, and Daffodil International University in Partial of the requirements for the Degree of Bachelor of Computer Science. We also declare that neither this project report nor any part of this project report has been submitted elsewhere of any Degree or Diploma. We also declare that we collect information from our project work experience and Internet.

### Supervised by:



---

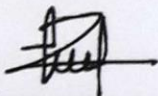
**MD. Rakib Hasan**

Lecturer

Department of CSE

Daffodil International University

### Co-Supervised by:



---

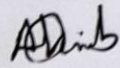
**Md. Jeual Mia**

Lecturer

Department of CSE

Daffodil International University

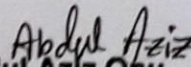
### Submitted by:

**Akib Mahmud Tonmoy** 

ID: 161-15-7422

Department of CSE

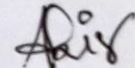
Daffodil International University

  
**Abdul Aziz Opu**

ID: 161-15-6825

Department of CSE

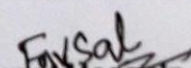
Daffodil International University

**Abir Hossain** 

ID: 161-15-6923

Department of CSE

Daffodil International University

  
**Md. Faysal Hossain**

ID: 161-15-7416

Department of CSE

Daffodil International University

## ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for his divine blessing makes us possible to complete the final year project successfully. We have been taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them.

We really grateful and wish our profound our indebtedness to **Md. Rakib Hasan**, Lecturer, Department of CSE, Daffodil International University, Dhaka. Deep Knowledge & keen interest in our supervisor field in the “**Security Attacks and Solutions in Clouds**” to carry out this project. His endless patience, continual encouragement scholarly guidance, constant and energetics supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain** Head, Department of CSE, for his kind help to finish our project and we would also like to admit with much appreciation the crucial role of the staff of Daffodil International University (DIU), who gave me the permission to access all kind of library materials and equipment to gain knowledge and to clear out our understandings. We have to appreciate the guidance given by the other supervisors and lecturers who has helped us to clear our understanding and created a concern and importance of completing the project report carefully with maintain good knowledge and quality.

Finally, we would like to express our gratitude towards our parents & our supervisor **Md. Rakib Hasan** for their kind co-operation and encouragement which helped us in the completion of this project.

# Abstract

Cloud Computing is a unique technology that provides us flexible, scalable & reliable framework and services for almost every organization. Cloud data are stored at remote servers and that can be accessed by the help of cloud service providers. Some renowned name of cloud service providers are Amazon Web Service, Google's Application, IBM, Microsoft Azure cloud etc. which provides us the excellent facility for user to store their data and resources on cloud environment and allow us to access them from any remote location. The main thing for which the organizations grab the services of cloud computing is reduced cost and reliable security through optimized and efficient computing. Apart from all these facilities the most frequent thread for cloud computing is its security. There are various obligations and threads in cloud computing that affect its security. In our thesis, we mainly tried to focus and analyze the structural concept and the security threats on cloud computing, that is still an emerging and progressing technology for the information of users over the internet via different platforms. Cloud Computing provides us the virtualized and portable resources with efficient network-based services built up with millions of distributed computers instead of local computers or storages. Meanwhile, the implementation and applications of cloud computing increased prominently, which has caught the focus of new IT industries in expanding the utilization of computing technologies.

## TABLE OF CONTENTS

**CONTENTS**

**PAGE**

Board of examiners	II
Declaration	III
Acknowledgements	IV
Abstract	V

## CHAPTER

### CHAPTER 1: INTRODUCTION

1.1 Introduction .....	1
1.2 Motivation .....	1-2
1.3 Project objectives.....	3
1.4 Report layout.....	4

### CHAPTER 2: BACKGROUND

2.1 Introduction.....	5
2.2 Communication.....	6

### CHAPTER 3: STRUCTURE AND DEPLOYMENT OF CLOUD COMPUTING

3.1 Brief review.....	7
3.2 History and evolutions.....	8-9
3.3 Features.....	9-10
3.4 Main types of cloud.....	10
3.4.1 Private cloud.....	10-11
3.4.2 Public cloud.....	12
3.4.3 Community cloud .....	12
3.4.4 Hybrid cloud .....	12-13
3.6.1 Infrastructure as a service (IaaS) .....	14
3.6.2 Platform as a service (PaaS) .....	14
3.6.3 Software as a service (SaaS) .....	15

### CHAPTER 4: SECURITY ATTACKS ON CLOUD

4.1 Denial of Service (DoS) attacks.....	16-19
4.2 Cloud Malware Injection Attack.....	16
4.3 Side Channel Attacks.....	17
4.4 Authentication Attacks.....	16-19
4.5 Man-In-The-Middle Cryptographic Attacks.....	22-23

### CHAPTER 5: MAIN SECURITY ISSUES IN CLOUD COMPUTING

5.1 Privacy management .....	24
------------------------------	----

5.2 Data security and confidentiality .....	25
5.3 Data audit .....	26
5.4 Authentication and access control policy .....	26
5.5 Virtual machine security and automated management .....	26

**CHAPTER 6: CLOUD SECURITY FRAMEWORK**

6.1 Introduction.....	28
6.2 Proposed Cloud Security Model .....	28
6.3 Physical Security.....	29
6.4 Network and perimeter security.....	29
6.5 Virtual OS/IMAGE Security.....	29-30
6.6 IAM.....	
6.7 Data and Storage Security.....	30
6.8 Client Level Security.....	31

**CHAPTER 7: NETWORK SIMULATION**

6.1 Introduction.....	32
6.2 Vlan.....	32
6.3 Hardware.....	33
6.4 Software.....	34
6.5 Use Case.....	35-40

**CHAPTER 8: CONCLUSION ..... 41-42**

**REFERENCES..... 43-47**

**LIST OF FIGURES**

**Figures**

**Page No.**

- Fig: 3.1.1- Distributed Computing and Parallel Computing
- Fig: 3.1.2- NAS and SAN
- Fig: 3.4- Cloud Deployment
- Fig: 3.4.2- Public cloud v/s Private cloud
- Fig: 3.6- Cloud service delivery models
- Fig: 3.6.3- Cloud Services types and examples
- Fig: 4.1- Cloud Security and Privacy
- Fig: 5.1- Public key encryption
- Fig: 5.4- Proxy re-encryption
- Fig: 6.2- proposed model for cloud security
- Fig: 7.2- Difference Between Traditional Lan Segmentation and Vlan Segmentation
- Fig 7.5.1: Proposed Secured Network Design
- Fig 7.5.2: Simulation of Proposed Network design
- Fig 7.5.3: VLAN communication
- Fig 7.5.6: Head Office PC to Web Server



## **LIST OF ABBREVIATION (OR) SYMBOLS**

NIST	National Institute of Standards and Technology (U.S.)
NAS	Network Attached Storage
SAN	Storage Area Network
FC	Fiber Channel
Amazon EC2	Amazon Elastic Compute Cloud
CPU	Central Processing Unit
CEO	Chief Executive Officer
NASA	National Aeronautics and Space Administration (U.S.)
PDA	Personal Digital Assistant
SLA	Service Level Agreement
VAS	Value Added Service
HTML	Hypertext Markup Language
CSS	Cascading Style Sheets
RIA	Rich Internet Applications
REST	Representational State Transfer
ESX	Elastic Sky X
SQL	Structured Query Language
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
EC	Electronic Commerce
TB	Tera Byte
GPU	Graphics Processing Unit
ESB	Enterprise Service Bus
BPM	Business Process Management
AM	Active Messenger

API	Application Programming Interface
ASP	Application Service Provider
RFID	Radio Frequency Identification Devices
GPS	Global Positioning System
SOAP	Simple Object Access Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
I/O	Input/ Output
GFS	Google File System
GB	Giga Byte
RSS	Really Simple Syndication
CLR	Common Language Runtime
WAN	Wide Area Network
SCSI	Small Computer System Interface
iSCSI	Internet Small Computer System Interface
SAS	Serial Attached SCSI
DAS	Direct Attached Storage
IPTV	Internet Protocol Television
VOD	Video on Demand
STB	Set Top Box
FPS	Frames per Second

CDN	Content Distribution Network
MS-SQL	Microsoft Structured Query Language
TPM	Trusted Platform Module
PEKS	Public key Encryption with Keyword Search
XML	Extensible Markup Language
DoS	Denial of Service
RSA	One of the first practical public-key cryptosystems created by Ron Rivest, Adi Shamir, and Leonard Adleman
SSLAP	Secure Sockets Layer Authentication Protocol
IBE	Identity-Based Encryption
IBS	Identity-Based Signature
ABE	Attribute-Based Encryption
PRE	Proxy Re-Encryption
LRE	Lazy Re-Encryption
VMC	Virtual Machine Contract
OVF	Open Virtualization Format
CSA	Cloud Security Alliance

# CHAPTER-1

## INTRODUCTION

### 1.1 Introduction:

These days, it's become widespread to listen to concerning Cloud information, Cloud Security, and Cloud scheme. Be that as it may, 'CLOUD' is still particularly confounding for non-geeks out there. The "Cloud" here doesn't demonstrate a specific condition. The essential meaning of "Cloud computing," which is as yet another developing and amassed figuring innovation that is steadily reaching from a small segment of the examination zone to tremendous scale advancing and using. Furthermore, the Cloud Service will be the framework of Web. World for the coming age and propelling the new illustration of Online administrations.

In this manner, to get the progression of extending "Cloud," that is essential to clear the fundamental ideas of Distributed Computing. In any case, the impression of Cloud Computing is still very befuddling and hazy for a non-IT go-between specialist. So, what decisively the Distributed and Cloud Computing innovation is? Which techniques to construct a promising Cloud? What are the focal points and utility of our work and life? What are the threat issues that lie in it, and how might we manage them? Bit by bit, the intricacy of Cloud System Measurement will be unshrouded in the proposed work and introduced in a trained design.

### 1.2 Motivation:

We are following our Bachelors in Computer Science Engineering at Daffodil International University. In this study period, mainly student gains theoretical knowledge, but now a day, practical experience is much more essential for any student. Practical knowledge helps a student to gain a larger prospect of the subjects. Practical knowledge gradually helps to complement textbook knowledge.

The most continuous inquiry that emerges about Cloud Computing is if a Cloud is sufficiently secure? Since there are numerous sorts of conceivable malignant assaults, for example,

Browser Attack, Malware-Injection Attack, Phishing Attack, Wrapping Attack, Flooding Attack.

Our motive is trying to find the answer to this question.

### **1.3 Objective:**

The objective to work with this project is to carry out the advantages and drawbacks considering the value of cost, data security, and data possibility of any organization, and try to classify the possible security attacks and threats on clouds including Flooding attacks, Browser attacks, Wrapping attacks, Malware-Injection attacks and so on.

We will try to scale down the proportion of data from the cloud and try to increase the competence of fully homomorphism type encryption to process encrypted data. The goals of the project are:

- Learn about computer networking.
- Learn about the different networking protocols.
- Learn about the cloud computing.
- Learn about the non-server computing applications.
- Learn about the threats of clouds.
- Learn about the data security.
- Learn about the database security system.
- Learn about software and tools that are made for cloud computing.
- Learn about the clouds algorithm.
- Ensure the sustainability in clouds.
- Try to find the solutions of the threats.
- Try to prevent data from stealing.
- Try to enhance security system.
- Try to be secure data from cyber-attacks.

## 1.4 Expected Result:

Today most of our work is done online, and the Web is working as an inevitable medium. For this reason, the network security issue is enhancing very challenging and critical task to maintain. Cloud computing technology is dynamic and demanding services nowadays, that's why network security becomes very problematic to handle. The main objective to build a cloud network is to trim the maintenance requirement of using such belongings as storages, processing power, etc. This kind of resources benefits organizations can target on their business prominently. The development of Cloud Computing included with different advancements, for example, virtualization, network registering, autonomic figuring, and some different methods. Doesn't make a difference how much innovation is utilized under it, New difficulties emerge at whatever point another innovation comes.

When all is said in done, Cloud computing security recognizes the following primary objectives:

- **Accessibility:** The objective of accessibility for Cloud Computing frameworks is to guarantee that information and administrations are constantly accessible for its clients whenever at wherever.
- **Confidentiality:** The privacy objective of privacy is to keep the client's information mystery in the distributed frameworks by developing that accessible just to qualified elements, and no unapproved approach to information may be acquired.
- **Integrity:** The objective of Data integrity in the Cloud framework is to guarantee that information has not been changed at all while it is put away or while its vehicle over the system.
- **Validation:** The objective of validation is to guarantee the character of the substance engaged with the correspondence.

- **Responsibility:** The objective of responsibility is to guarantee that no substance can deny its investment in an information move between them.

## 1.5 Report Layout:

For completing this report, we have added this layout.

This layout is the operation of adding something in a short time or in a tabular form to define the whole process in time. We work according to plans because we want them to show all of my work in a concise way so that the viewer can understand it clearly.

**Chapter 1** is describing the introduction, objective, motivation, expected result of this project.

**Chapter 2** is about the project background and the project overview. This chapter gives the information about related work, scope of the problem and project challenges.

**Chapter 3** is describing the structure and deployment of cloud computing.

**Chapter 4 & 5** is discussing about all kind of cloud security issues briefly and how can you solve out these problems.

**Chapter 6** is about a safe and secure network system and how the secure cloud can be implemented on this.

**Chapter 7** is about utilization of cloud.

**Chapter 8** is about the conclusion.

## **CHAPTER- 2**

### **BACKGROUND**

#### **2.1 Introduction:**

In our proposal, we mainly attempted to focus and analyze the auxiliary idea and the security dangers on distributed computing, which is as yet a developing and advancing innovation for the data of clients over the web through distinct stages. Cloud computing gives us the virtualized and convenient assets with a proficient system based administrations developed with a massive number of appropriated PCs rather than nearby PCs or stockpiles. Then, the execution and uses of distributed computing expanded unmistakably, which has gotten the focal point of new IT ventures in growing the usage of processing advances.

In addition, this theory likewise incorporates the handy applications and genuine business estimation of distributed computing. As distributed cloud computing is generally reliant on the Internet and Web, this innovation is getting more focused on assaulting with various specialized vulnerabilities, infection, malware, and careless practices. In addition, this proposal works with the essential security and hostile to string issues of distributed computing. At long last, this theory paper centers and proposes some conceivable less costing arrangements that can help improve the specialized perspectives and mirrors the best approach to work with a processing framework for further advancement later on.

#### **2.2 Communication:**

Communication is very important part of our life. Communication makes our life so easy. Using computer networking we can communicate with each other in sitting at home. Using computer networking we can easily maintain our office, business etc. The time of communication is decreasing by using computer networking.



## 2.3 Networking (computer):

Computer Networking is the process of multiple interconnecting devices for transporting and exchanging the data between hosts over a shared medium. Network composes not only the structure, framework but also the management and application of the network infrastructure, software, and policies.

### **Everybody knows about the "Cloud". But what does it refer to?**

How about we make it Easy. "Cloud" essentially alludes to the web and "Cloud computing" is a specialized word that portrays and benefits that works through the Internet and Web as opposed to on private servers and hard drives.

Cloud computing is one of the quickest developing fragment in Information Technology. During the previous two decades, when virtualization and circulated figuring has advanced alongside superfast arrange associations, Cloud processing has accomplished extraordinary development and presented endless conceivable outcomes.

“The worldwide Cloud computing market grew by 28% to \$110B in revenues in 2015. Synergy Research Group found that public IaaS/PaaS services attained the highest growth rate of 51%, followed by private & hybrid cloud infrastructure services at 45%.”

According to the official NIST definition,

"Cloud computing is a model for enabling ubiquitous, 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 inter-action."

## CHAPTER-3

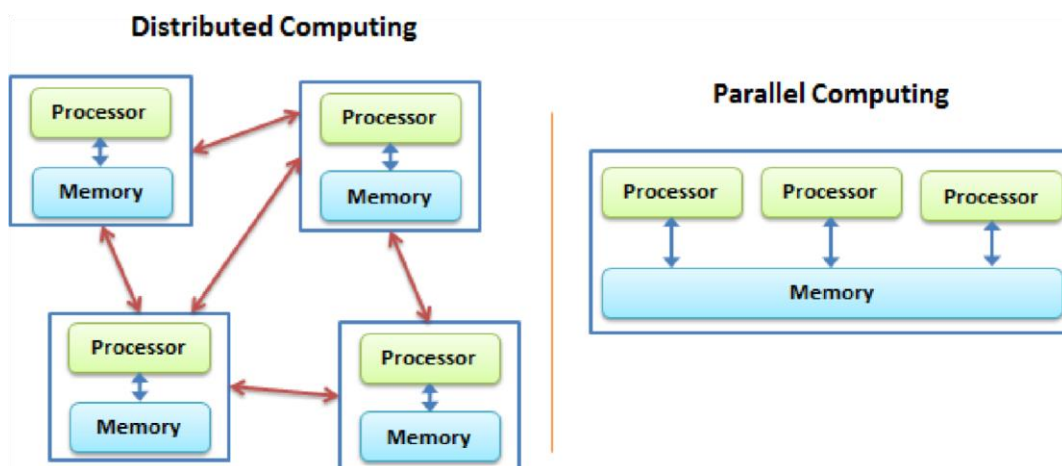
### STRUCTURE AND DEPLOYMENT OF CLOUD COMPUTING

#### 3.1 Brief Review

"Cloud" innovation is enormously compelling a direct result of its mutual assets by a huge of quantities of clients and for its powerfully got to rely upon the requests.

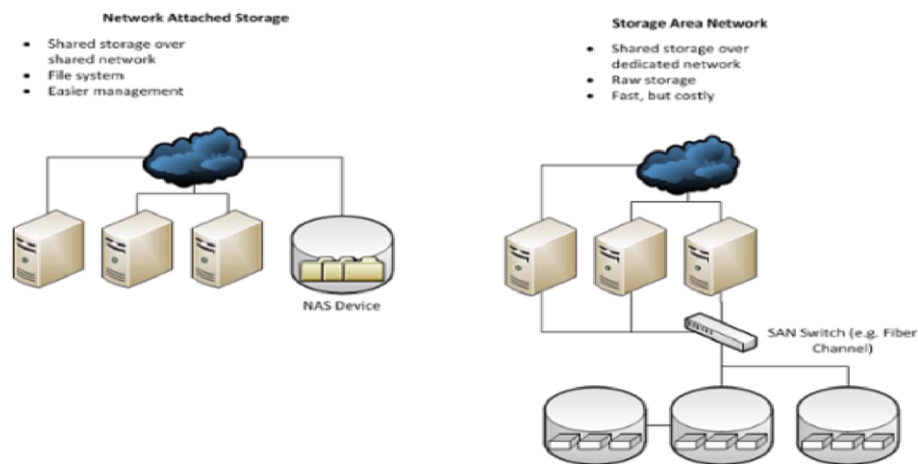
The name "Cloud" comes because of the forceful difference in scale and perplexing area like a genuine Cloud in the sky, besides it happening in real life. Cloud isn't made out of sets of equipment or programming. It is fundamentally the blend and unions of enormous data innovations. In addition, the territory of Cloud is continuously expanding step by step since new building up innovation, likewise participating around there.

Dispersed Computing strategy focuses on a monstrous calculation into discrete sections, and it doles out various PCs to figure, at that point in the wake of ascertaining the entirety of the outcomes gather together. Additionally, parallel computing joins a significant number of computational resources to work a particular undertaking, which is an extraordinary accomplished reply for identical problems. The image shows an examination between Parallel Computing and Distributed Computing.



**Fig 3.1.1: Framework of Distribute and Parallel Computing**

For the most part, Network Attached Storage (NAS) innovation works associating memory appliances connecting with massive number of computers utilizing system topology. Network Attached Storage is prepared continuously for giving enough extra room and expeditiously expanding stockpiling volumes for the associated hubs. Then again, Storage Area Network which applies Fiber Channel to interface with a massive number of computers without topology, as a rule utilizing large volume memory storages condition. The picture shows the diverse topology of NAS and SAN.



**Fig 3.1.2: Framework of NAS and SAN**

## 3.2 History and Evolutions

To get a better clarification of Cloud Computing, we have to take a more in-depth look into its history and evolutions.

In back 1950s, Computer Engineers were giving priority to a mainframe computer in the computation area, and it was declared as the revolution of computing as it was growing and taking place as quite fashionable in academia and corporations.

Be that as it may, it lacked in inner preparing limits. At that point, customer PCs proposed to enable numerous clients to contribute logical access to computers time from different nodes. This method was known as time-sharing at that time. Hence the foundation of "Cloud" was developed.

First, Sun Microsystems came with the concept that "the network was the computer" in 1983, this concept was different from the traditional system defined in the computer who grabbed the attention to the users and developers.

At that point. In March 2006, Amazon presented Elastic Computer Cloud administration, giving reusable and adaptable limit in the cloud, which prepares for progressively available for the web-scale distributed computing. That year, on the ninth of August, Eric Schmidt, the CEO of Google, started the idea of "Distributed computing" which was chiefly founded on the Project "Google 101" by engineer Christophe Bisciglia. The task was meaning to decrease the expense of conveyed figuring in scholarly field examine additionally it offered help in equipment, programming, and procedure. In 2008, the first of February, IBM announced the building up the primary distributed computing Center in Wuxi, China. Around the same time, On the twenty-ninth of July, In 2008, Intel, Yahoo, HP, and reported a connection to investigate program in Singapore, Germany, and U.S.A focusing on developing six datacenters for inquiring about the stage.

In 2008, Microsoft built up its first Cloud Computing stage and framework named Microsoft Azure, which is an offering application and administration foundation, execution, and the executives through Microsoft datacenter. In July 2010, Rackspace, NASA proclaimed an open-source enterprise "OpenStack," that controls colossal quantities of computers. Later On, IBM and Oracle announced their distributed administrations "IBM Smart Cloud" and "Prophet Cloud" in the recent year of 2013 and 2014. The history and development referenced above give us a visible sign that distributed computing innovation gained seriously quickened ground after 2000 and is getting further develop and open all through the world.

### **3.3 Attributes**

It is vital to unearth the significance of the achievement of Distributed Computing. Why it is getting well known and broadly agreed by numerous software firms and users, what is the provocativeness of Cloud Computing?

In the recent time, Google has developed approximately 1 million data servers; Microsoft, Yahoo, Amazon etc.has a massive amount of servers, guaranteeing the eccentric computation capacity for users among the world. Clients can get the connection from anyplace through it.

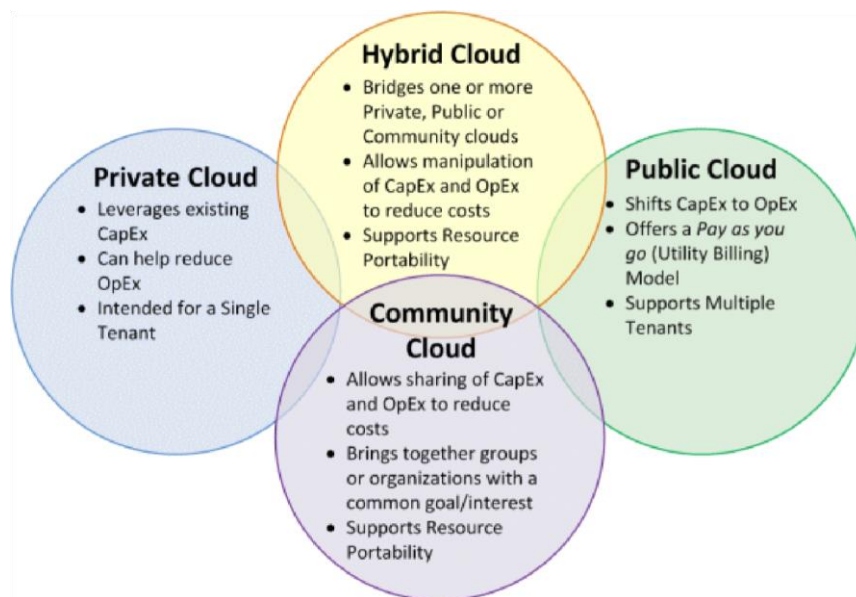
Rather than originating from substantial elements, all the mentioned assets originate from the "Cloud." However, there is no condition for users getting the exact access; the software is running someplace inside the "Cloud." Thus, the "Cloud" is viewed as an excellent asset.

Moreover, to gratify the requirements of large number of software's and clients, the aspect of the "Cloud" is extensible. The utilization of "Cloud" is more trustworthy than nearby computers. With the help of the "Cloud," cases would be darkened. The equivalent "Cloud" can continue original running softwares simultaneously.

### 3.4 Main Types of Cloud

There are mainly four kinds of clouds architecture that are implemented in cloud server and these are:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud



**Fig 3.4: Cloud Architecture Models**

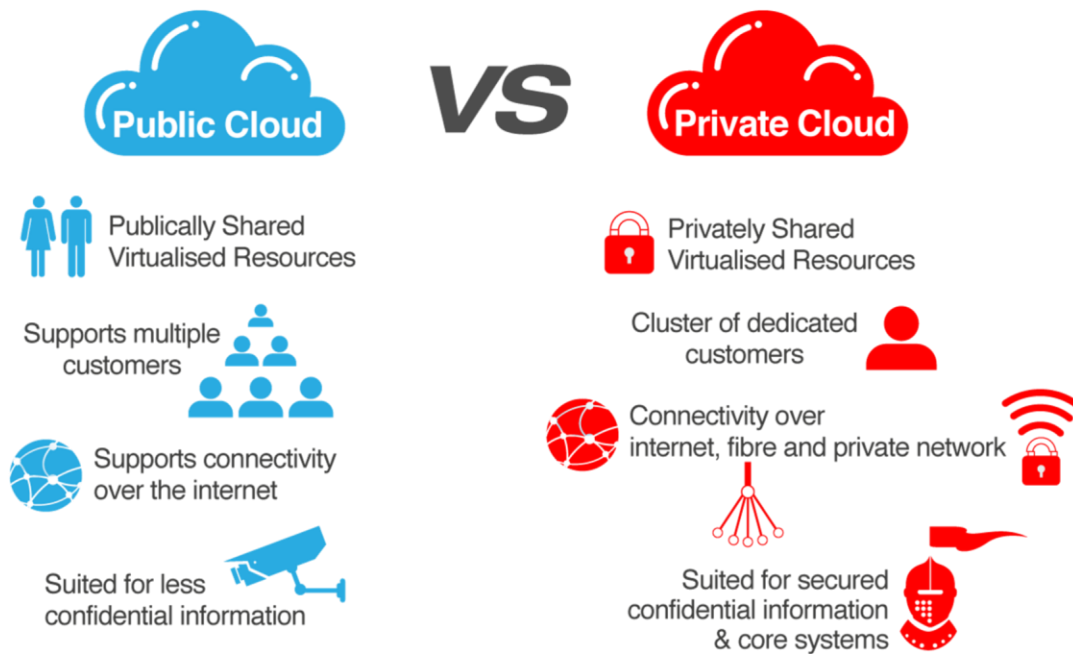
### **3.4.1 Private Cloud**

A private cloud is manufactured and fundamentally utilized by an individual client or organizations. The associations builds up its model design and manages the development of implementations through it. The goal and focal evaluation of a private cloud are its resources. A private cloud is nearly simple to construct and can be built up by an associations or a cloud technologists co-op. In view of facilitating the board specialists, cloud specialist organizations like Amazon and IBM should design, introduce and deal with the framework to hold the private cloud keeping up the business server acknowledged by a particular or individual organization. The usage of cloud resources is solidly constrained by the associations. Finally, the expert information on creating and running this condition can be picked up proficiently.

### **3.4.2 Public Cloud**

Open cloud portrays the cloud allowed by outside cloud server authority associations got by getting to the Internet. This cloud system is outstanding by virtue of it's decently ease. A cloud association gives its help of outside customers access to their structure direct, and external customers can get to the organization by online without having disseminated figuring resources. There is also some significance to individuals in the public cloud.

It offers an ensured and secure data storing center appear differently in relation to some other accumulating methods. Prior to progressions, people calculated the information must be taken care of in their computers, and this is only a safe system; this isn't substantial. There is a generous likelihood that the close by computers may be physically hurt, attacked by software engineers or contamination, some even suspicious movement from an external customer who can get to the access to the computers.



**Fig 3.4.2: Public cloud v/s Private cloud**

### 3.4.3 Community Cloud

A Community cloud is a thing that empowers various free terms to get cash sparing preferences in a common closed cloud. The section is reached out in the local cloud on a particular extent of the area and formed like a system. In perspective on indistinct managerial, consistence, or legal control, this model has an enormous augmentation for associations or affiliations. System fogs are gathered in places where customers have related importance's; offering united organizations. For instance, the customers are teachers, undergraduate, and staff from a wide scope of schools, ask about workplaces, and organization associations in school towns. The organizations of this system cloud consolidate cloud has, cloud servers, dispersed stockpiling, and a cloud data server.

### 3.4.4 Hybrid Cloud

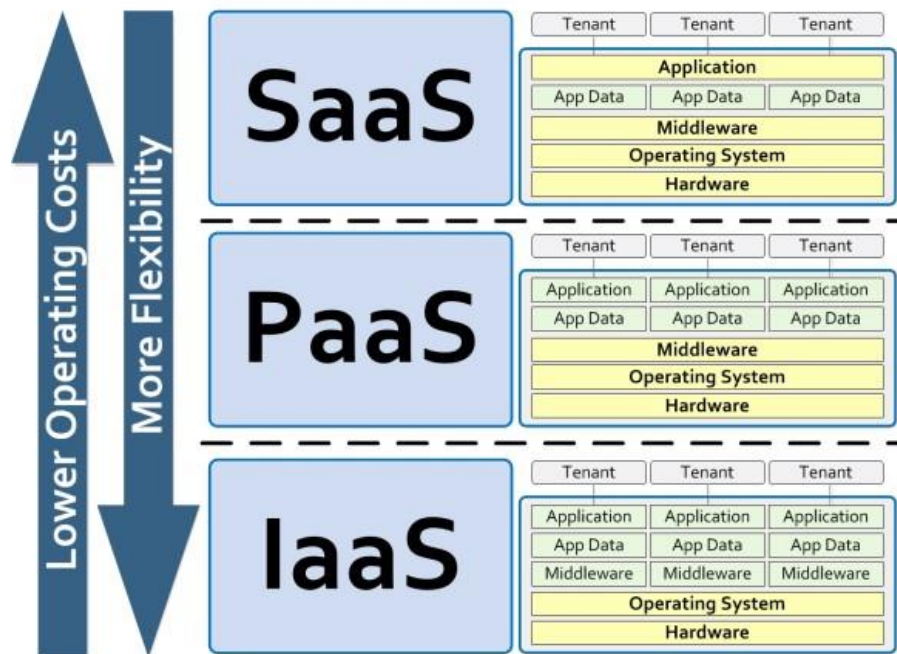
A hybrid cloud is a setup of different mists that stay diverse assigns yet in addition bound together. The advantages of this cloud originate from numerous organization models. From past research, we as a whole have come to realize that a private cloud is more secure than an

open cloud, however an open cloud gets countless open assets. Consequently, an ideal answer for this conflicting circumstance is given by a perfect answer for this unfriendly circumstance: half and half cloud. The security highlights of the private cloud contain applicable interior information in the neighborhood server farm. They can likewise use registering assets from the general population cloud to finish work proficiently and successfully. A half and half cloud takes the proficiencies of general society cloud to increase higher calculation limit, and it breaks the equipment constraint of a private cloud. As it can switch between open cloud and private cloud dependent on the clients' prerequisite, the expense would be lower, which alludes to application and information on the most suitable stage.

### 3.6 Service Models

There are primarily three models by which they offer their administrations. They are:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS),



**Fig 3.6: Cloud service Delivery Models**



### **3.6.1 Infrastructure as a service (IaaS)**

IaaS gives the organization subject to the use of all enlisting structure, including memory, storing, CPU, orchestrate, and other focal handling resources that can be applied and executed by customers, for instance, working system and applications. Purchasers can control the decision of the working structure, additional room, and passed on the application similarly as increase the benefit of control of kept framework sections like a switch, firewall, and weight balance controller. In like manner, they supervise or control any disseminated processing systems.

Establishment as an assistance gives Consumers perfect organizations through the PC system. The Internet-based help is a bit of IaaS, for instance, amassing and database.

Amazon EC2 handles open server pools in the establishment. Private organizations will use a great deal of free or restricted server pools in an organization's database. Individuals by and large, private, and a creamer cloud are out and out available just if the datacenter state of the association is used to make programming improvement.

### **3.6.2 Platform as a service (PaaS)**

Here, we are discussing what cloud organization offers. Cloud master associations offer a figuring stage which contains a working system, a programming language execution condition, a web server, and a database. Later on, the server stage will be used as a game plan that passes on organizations. Theoretically, PaaS is one of the arrangements of SaaS applications. PaaS is the application establishment organization in the disseminated figuring condition, which is called middleware as help. PaaS is masterminded into two sorts; one spotlights on application sending and running PaaS. Another is called IPaaS. In a general sense, PaaS permits to PaaS, like Force and Google App Engine.

PaaS fuses a wide scope of current business as an application server; business limit gets to, business engine, and open business arrange. IaaS gives API, which downwardly figures establishment limit as showed by business need called hardware resources. Upwardly, it passes on business dispatch organization, which screens each kind of benefits ceaselessly and passing those advantages for SaaS end customers by methods for Application Program Interface.

### 3.6.3 Software as a service (SaaS)

In the 21st century, there is a rising of the new programming application model, with the progress of Internet advancement and the improvement of applied programming. The organization charges rely upon the quantity of organizations and the hour of utilization. Customers can tie down electronic programming through providers by lease to regulate association assignments without close by programming upkeep that will be totally managed and compelled by providers, and they don't need to purchase programming any more. SaaS is the perfect way to deal with apply for high advances since it executes the limit of obtainment, establishment, and system upkeep for associations for some little associations.

The cost of SaaS writing computer programs is, generally, in a full group, which joins standard programming grant charge, upkeep charge similarly as specific assistance charge that has been solidified as a month to month rental charges. In any case, the extent of SaaS is exceptionally far reaching since it covers from close to nothing or focus associations to tremendous organizations. The charging procedure is versatile also. From one point of view, associations can incorporate or empty the record as per their needs. Of course, the cost from the genuine report and time helps with reducing help costs, and it gets more affordable than the traditional charging methodology.

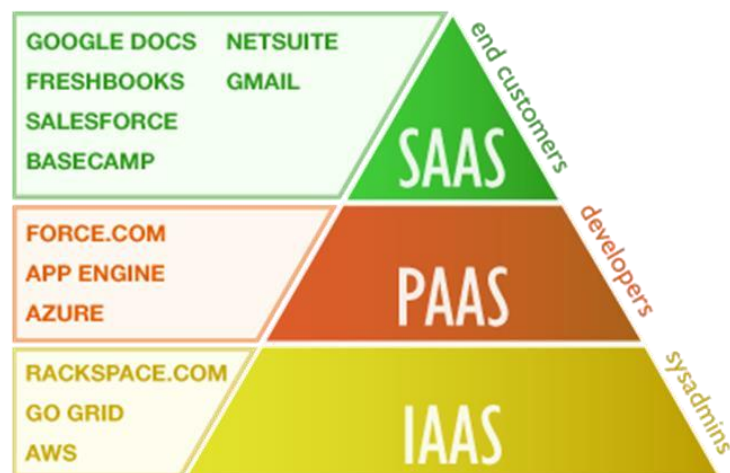


Fig 3.6.3: Cloud services types and examples

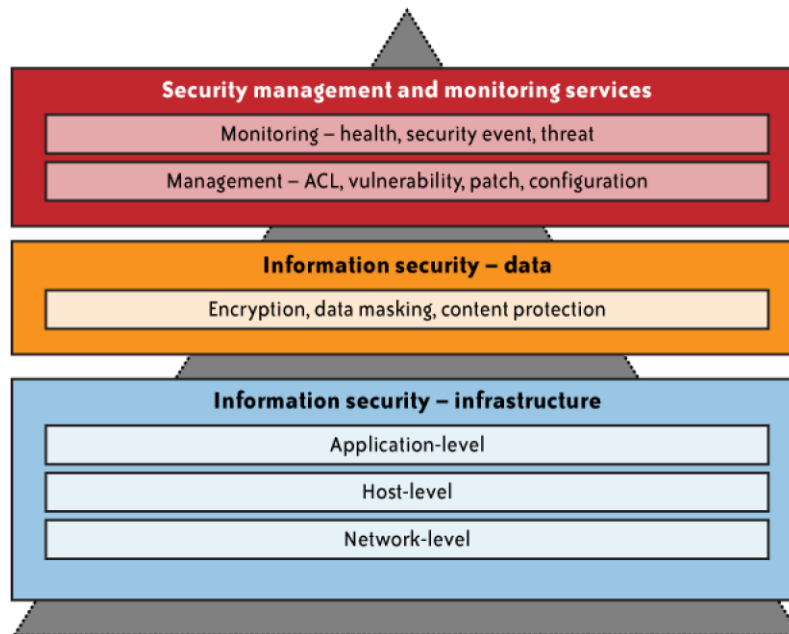
## **CHAPTER-4**

### **SECURITY ATTACKS ON CLOUD**

Internet, Technology, Social media, all of them have become already a part of life for business and current users. Every information is now available for us to get connected with this modern world. But all of these technologies were not possible couple of decade of ago. Nowadays Information technology has risen a lot of possibilities for public users and also authoritative people to get speedy internet access for the deployment of mobile functionalities o get access from almost everywhere.

Today people are connected via E-mail for their communication and resource sharing purpose, creating authoritative and non-authoritative documents through internet browsers, making a virtual collection to transfer and store their photos and recollections. Something as basic as entering in a website page is the main thing a client needs to start to utilize administrations that live on a remote server and gives him a chance to share private and classified data, or utilizing registering cycles of a heap of servers that he will ever witness firsthand. This is occurring through the innovation called Cloud Computer Services.

"Cloud," this name is introduced to the world as a metaphor because like the real world, you can see the cloud shape, but you don't see what is inside. These services are available at both free and paid simply like other services method around the world. It is practically like the apparatus of a virtual machine with its OS, running applications, and extra rooms. This innovation offers adaptability to numerous clients and associations that they can skip introducing other superfluous applications on their gadgets by which they can have increasingly computational power applying Cloud Computer through web, or they can likewise set up their own private cloud, or the clients can likewise utilize the two choices as per their requests.



- Assuring Data Confidentiality and Principle
- Assuring Convenient Connection Control
- Assuring the Opportunity of Internet-Facing Resources
- Network-Level Mitigation
- IaaS, SaaS and PaaS Host Security

As the world is moving towards cloud computing, it becomes more sophisticated, and attackers look to follow it. Some of the potential attacks on cloud computing are:-

## 4.1 Denial of Service (DoS) attacks

In a Denial of Service (DoS) attack, the intruder intentionally targeted a network system and flooded and overloaded with various service requests to stop replying to any new further claims. It creates a deadlock situation to many resources by making them unavailable to the users. Technological Expert identifies that DoS attacks are more vulnerable than any other attacks because it is so much connected to many users that make it severe harmful.

There are many kinds of DoS Attacks. Some of them are:

- An Intruder/Attacker can flood their marked object with a vast number of junk/unused files that dominate the system resources as well as bandwidth. For example, UDP flooding, ICMP flooding, etc.
- By using blank space, an attacker makes it associate with a much different network protocol to encounter marked resources. Let's Say, Ping of death, Segment resource attack, SYN floods, etc.
- By requesting HTTP requests in a huge number, an attacker can also make a system fully deadlock, for instance, XML DDOS attack, HTTP DDOS attack, etc.

For constraining DoS ambush, we can amass traffic dependent on endorsement, so we can limit traffic that is recognized as unapproved and grant traffic that is perceived as affirmed. For such assaults, firewalls can be used to allow or deny traffic dependent on getting to shows, ports, or IP addresses. Today the more noteworthy piece of the switches have the capacity of rate-compelling dependent on Access Control List that can give modified rate confining, trick IP isolating, shape traffic, legitimate, and can significantly evaluate packs. Like switches have in like manner some limit like ACL and rate-confining, which can be set physically to make rules and rules.

Application front end gear can be used on frameworks in colligation with switches and switches that can separate data packages as they go into the framework structure to check their capacity and need so stream of traffic can be controlled.

After DoS ambush, one can communicate all the traffic on the attacked pack to an invalid interface or a non-existing interface, and this abatements the effect of DoS attack.

## **Possible Solutions Against DoS Attacks**

The basic initiative for blocking DoS Attack is the utilization of Classification of users based on authorization. Authorization blockage will help us to identify unauthorized intruders in our system and get make a firewall for them. By implementing this firewall, we can permit or deny

traffic dependent on getting to conventions access protocols, IP locations, ports, etc. As of late, the vast majority of the switches possess the effectiveness of rate-restricting on the base of the Access Control list that fundamentally gives counterfeit IP sifting, official, programmed rate constraining, and can profoundly review parcels and shape traffic, and so on. Regardless of having similar features, Routers have some extra capacity like rate-restricting and ACL, which can be set physically to make rules and guidelines.

Once more, Apps front end equipment can likewise be utilized on secure systems in relationship with routers and switches that can assess programs since they go into the approved system framework to check their genuine position and need with the goal that the progression of traffic can be estimated.

In the wake of sifting DoS assault, the framework can broadcast all the traffic on the sullied parcel to an invalid interface or to a clear interface; this lessens the impact of DoS assault.

## **4.2 Cloud Malware Injection Attack**

Cloud Malware Injection occurs when an hacker intends to push to implant a vulnerable program or something created virtual machine into the cloud network. By creating his vulnerable program module or virtual machine instance, the attacker injects it into the cloud network. When the injection is done once, then the attacker behaves normally to make his programs as a valid implementation of service to the cloud system. It seems so natural and real to the new service holders that they could be easily convinced by such particular programs to use it.

At the point when the attacker gets the opportunity to prevail in this, the cloud framework diverts the solicitations of that client to the harmful program, and the assailant begins doing his code to apply it. If the assailant prevails in this, the Cloud naturally diverts the solicitations of the substantial client to the pernicious assistance usage, and the aggressor code begins to execute.

The technique behind this assault is that an aggressor attempts to spread an evil program into the Cloud as it can reach to the administration solicitation of the injured individual's assistance.

For this usage, the aggressor needs to disengage the authority over the unfortunate casualty's information or assets on the Cloud.

Cloud Malware Injection is considered as a massive kind of abusing the cloud assault administration. The motivation behind cloud malware infusion assault can be anything in which an aggressor is intrigued; it might incorporate information alterations, full usefulness changes/invertor blocking.

## **Possible Solutions Against Malware Injection Attacks**

Cloud Computing Technology made their application that can run by the client are examined with high respectability and productivity. For the prevention of cloud from such malware infusion assault, we can relate the respectability level high with equipment or some equipment can be utilized for uprightness reason since it gets hard for an assailant to attack in the IaaS level.

For comprehending such sorts of issues, we can use a document assignment table (FAT) framework. By utilizing this framework, we can decide the honesty and legitimacy of another occurrence by contrasting separate and present and past circumstances.

So now go to the Execution Part. From the start, we need to actualize a hypervisor on the supplier's end. In cloud framework innovation, a hypervisor is perceived as the most debase and secure framework by which security can't be broken using any means. The obligation of Hypervisor is planning every one of the administrations and cases so we can send Hypervisor to break down the record designation table (FAT) to incorporate and approve an example of a client.

Another methodology we can pursue is that we can keep up the data of the stage type form that a client uses to get to the cloud in the primary stage when a client opens a record and can utilize that data to check the legitimacy of a new example of the client.

## 4.3 Side-Channel Attacks

When an assailant expects to put a vindictive virtual machine to bargain the cloud framework near a focused on cloud framework and afterward dispatch the program, this sort of attack is known as Side-Channel Attack. This Attack has grown adequately that has become a noteworthy risk to actualizing cryptographic calculations.

Side Channel Attack can be executed through different technique and they are:

- Power-Monitoring Attack
- Cache Attack
- Differential Fault Analysis
- Timing Attack

### Possible Solutions Against Side-Channel Attacks

Implementing a combination of virtual firewall appliances is the initial step to prevent cloud side-channel attack.

Amazon EC2 administration distributed a report where they demonstrated an assailant could acquaint another virtual machine with a distinguished focused on a VC in the cloud, and it is conceivable to extricate private assets. Conveying a firewall can guard the framework from the endeavor of an arrangement of the malignant VC during a side-channel attack.

Be that as it may, a virtual firewall avoids this endeavor of the position of the malignant VM during a side-channel assault. Again by utilizing arbitrarily encryption-unscrambling can shield the second step extraction of side-channel attack. The encryption-decryption technique is called confusion. Here the confusion alludes to make a connection among plain and ciphertext increasingly hard, and it makes intricacy.

By diffusion, we intend to disperse the scientific architecture of plaintext over the more significant part of the ciphertext. Such a sort of complex blend gives protection from both the front end and back end side of distributed computing engineering, and it additionally offers



RAS By utilizing encryption-decoding arbitrarily (Diffusion and Confusion Method), client information or data is encoded through an encryption calculation, so the assailant faces more challenges to recognize or separate the cryptography key.

## 4.4 Authentication Attacks

Verification is considered the weakest point in distributed computing administrations, and it is getting often focused on by an assailant. All things considered, the vast majority of the specialist organizations utilize the commonplace username and password validation. Be that as it may, some exceptional cases, we can discover in money related associations and organizations where they are utilizing different types of validation, for example, site keys, virtual consoles, shared mystery questions, and so on. This sort of security design makes it progressively convoluted for executing a phishing assault.

Some well-known authentication attacks are:

**Brute Force Attacks:** All potential mixes of the secret word is applied in this sort of assault to break the secret key. It is utilized to break the encoded passwords where the passwords are spared as scrambled content structure.

**Dictionary Attack:** Notwithstanding every one of the highlights of Brute Force Attacks, the dictionary assault attempts to coordinate the secret phrase with the most generally utilized expressions of day by day life utilization. This Attack type is usually quicker than the brute power attack.

**Replay Attacks:** The another name of replay assault is the reflection assaults. It is a plan to assault the test reaction client validation structure.

**Phishing Attacks:** It is a web electronic application assault where the assailant diverts the client requests to own created to malicious websites getting passwords/Pin Codes of the client.

### Possible solutions against Authentication attacks

**Delayed Reaction:** After providing a login-name/secret phrase pair, the server gives a marginally postponed yes/no answer. This technique ought to keep an attacker from checking adequately different passwords in a sensible time.

**Biometrics:** Biometric is a picture preparing based validation framework where fingerprints, iris, retinal, speech, signature, face confirmation are utilized to check against the first example. The given image is preprocessed first, and afterward, the characterization of pictures is finished.

**Advantages:**

- Real and authentic signature and cannot be copied/temperd at any cost.
- Biometric technology is less exposed to damage and sudden changes.

**Disadvantages:**

- It is quite money investing method and challenging to execution.
- It is not a perfectly demonstrated system, and it can be easily tempered and time-wasting as well.

## CHAPTER-5

### MAIN SECURITY ISSUES IN CLOUD COMPUTING

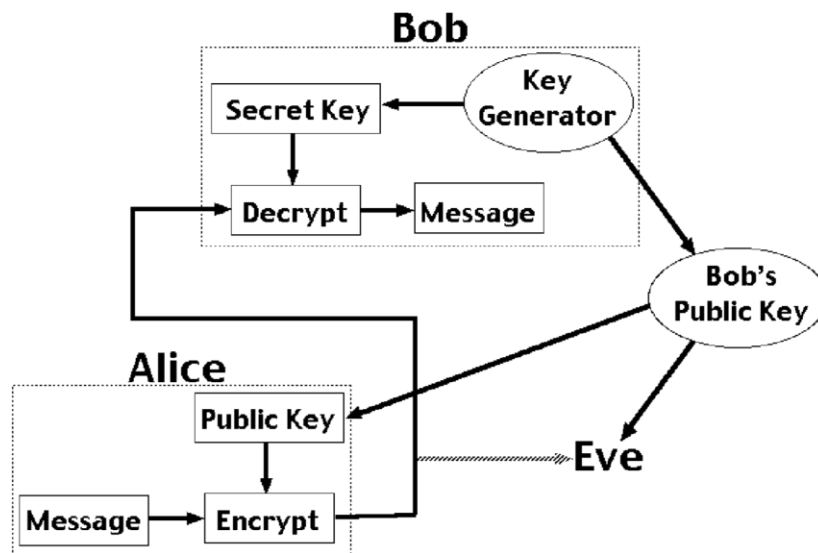
#### 5.1 Privacy Management

Most of the privacy management in cloud computing emphasizes the use of the cloud by implementing the management component in the cloud server. So, there is a new type of privacy manager based on users providing a trust model in terms of users. With the assistance of the service provider, users can control their sensitive information. By using obfuscation, even without the help of a service provider or malicious action of the service provider, users still can secure their private data. Another privacy manager provides encryption to privacy data and transfers the encryption to the cloud by a privacy manager. This mechanism is based upon a shared key by a user and a privacy manager, which proceed obfuscation and de-obfuscation to conceal the real content in the cloud but display the authentic result in the client-side. Moreover, the privacy manager completely utilizes TPM to protect the obfuscation key, strengthening the privacy protection feature.

The above-mentioned privacy managers are all used obfuscation technology. Generally, obfuscation means that the user creates a function  $f(x)$  in terms of  $x$ , which indicates privacy data and upload  $f(x)$  to the server. In the meantime, the service provider calculates  $f'(x)$  with acquired  $f(x)$  but not knowing of  $x$  in a definite cloud service. Then, the service provider will broadcast  $f'(x)$  as the result of service to the user for extra processing. Though obfuscation is an excellent method, there are still some mistakes in calculation due to the unaware of input data. Besides, it will increase the calculation obstacle on the user's information processing with various computations.

For cloud-stored data, on the one hand, users wish for a service provider that can give correct results according to their inquiries. Besides, they do not want the respective cloud service provider to get certain content, namely, implementing encrypted data queries. Therefore, a keyword search with a protected privacy feature that could use PEKS has been created. In this scenario where B sends mail to A by implementing the side door provided by A, the third-party analysis, if exact word got out in the email without aware of that content. This scheme allows

for a service provider partially participating in content decryption and search but is not able to read whole plain text, which helps with releasing pressure on user information processing with protected privacy. The figure shows the process of public-key encryption.



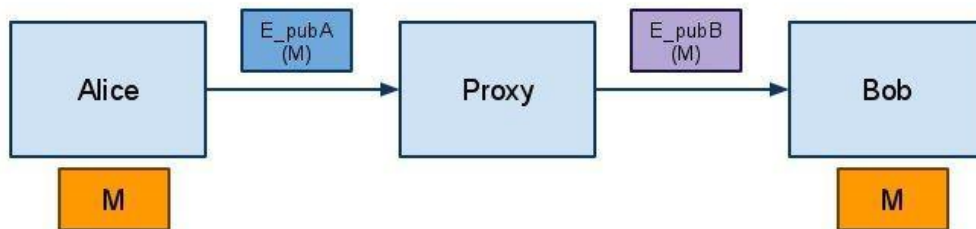
**Fig 5.1: Public key encryption**

## 5.4 Authentication and Access Control Policy

SSLAP was used in cloud computing authentication, but this protocol is quite sophisticated and overloads communication. In cloud computing, each user has its own digital ID. Thus the main and primary possible solutions are to use digitalized Identification as the fundamental of authentication. Based on IBS and IBE and, a protocol that has signature and encryption and was adopted in cloud computing, and cloud service, which is also based on identity authentication has been proposed. Compared to SSLAP, it does not ask for an authentication certificate and perfectly satisfies the requirements of cloud computing. By verifying on a simulation platform Grid-Sim, it shows more advantages than SSLAP in a minor load.

In terms of data attribute, the companies should define Access control policy. There is a policy which was created based on LRE,PRE, and ABE, in which ABE is a one-to-many public-key scheme by implementing discrete logarithm and bilinear mapping. That allows security data

distribution among the multiple data owners and single data owners. Where PRE is an encryption mechanism, whose nominal-trusted proxy could transfer cipher that creates the public key of a person from A to another cipher, without knowing the original simple plain text, it could be decrypted by person B's private key scheme. Figure 15 illustrates this process.



**Fig 5.4: Proxy re-encryption**

## 5.5 Virtual Machine Security and Automated Management

Virtualization and virtual machine technology are one of the fundamentals in building the cloud computing concept. In SaaS, the application is created on the visualized platform, and users share physical computing resources with others in a transparent way. In IaaS and PaaS mode, the application is served as a virtual machine or virtualized platform. Except for the traditional network, system, and software, different virtual machines should be isolated when sharing physical computing resources and storage resources. Besides, the virtual machine surveillance program is supposed to be trustable and not refer to user privacy information.

In many situations, a cloud service provider does not offer a virtual machine image. Hence, it is necessary to have a better way to manage it. VMware Virtual Appliance Market Place and Amazon EC2 came up with the idea of the image library. However, it has only the basic save and extraction function. Therefore, an image management system Mirage was created to control the access of image and trace the source of an image, which provides an active image filter and scans for cloud users and administrators to detect and fix image leaks.

According to the configuration requirements of a virtual machine, monitor, and physical resources, a new concept VMC was brought forward. It is achieved by extending the OVF to express VMC and manage them in a unified way. OVF is an industry-standard supported by VMware and other large manufacturers. It contains the OVF descriptor in XML format to refer to the metadata configuration of virtual devices as well as a virtual disk file set. VMC demonstrates a path of automated control and management for the virtual machine in large datacenter and cloud computing environment. Besides, it assists in implementing virtual machine detection, virtual network access control, and disaster recovery.

# CHAPTER-6

## Cloud Security Framework and Network Simulation

### 6.1 Introduction

In this chapter, we show and analyze the Proposed Cloud Security Model and Proposed secure network design of an organization and simulation of this network design.

### 6.2 Proposed Cloud Security Model

The Cloud Security cannot reach at a single stage. Our proposed model of cloud security consists of number of stages and domains, every stage has different security level to secure the cloud services need to ensure all stages high level of security. Fig. 6.2 defines our proposed model for cloud security.

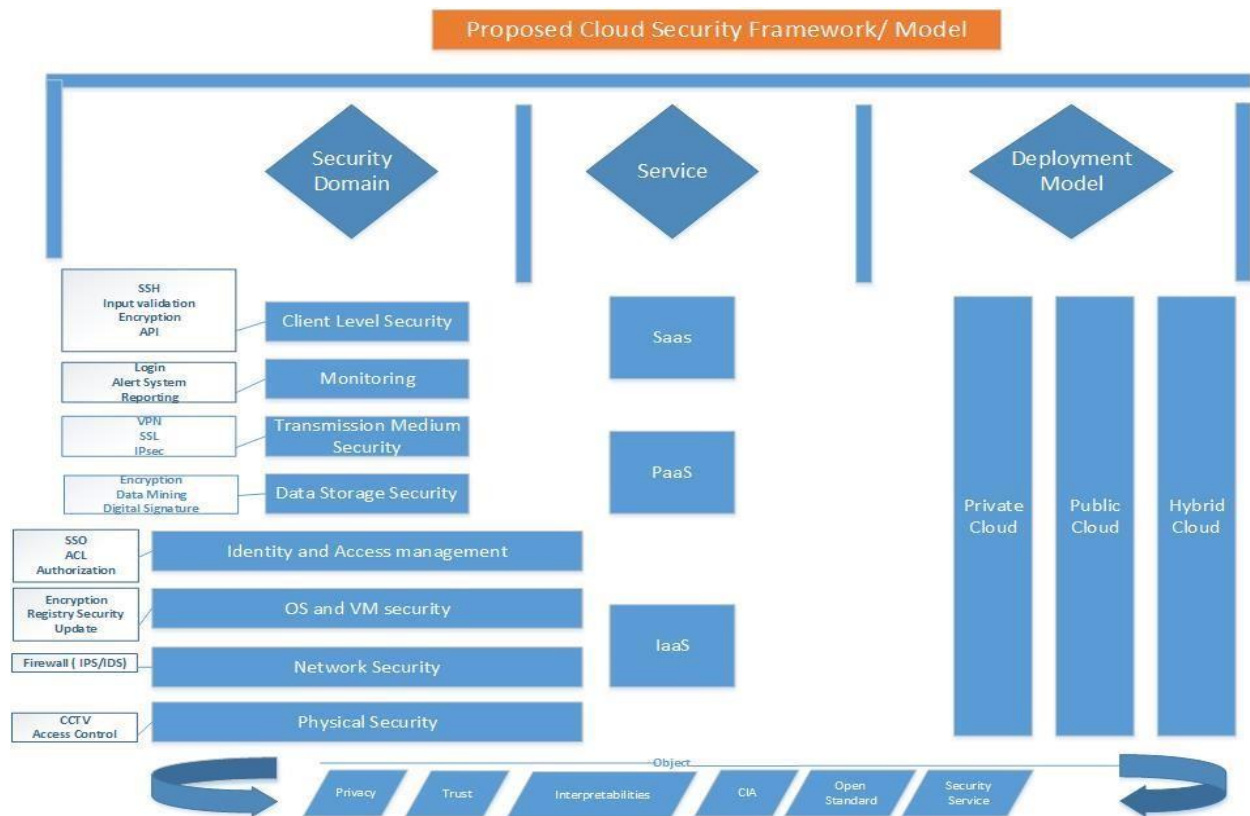


Fig 6.2: proposed model for cloud security

This proposed model we have categorized three types Security Domain, Services and Deployment Model. In the Security domain have 8 categories and every category security level is different. In the service level three types of service in the cloud. In the deployment field of the cloud there are Private Cloud, Hybrid Cloud and Public Cloud.

### **6.3 Physical Security**

This space tends to the security of physical resources, for example, server farms, servers, stockpiling gadgets, control supplies, organize gadgets, and different parts that aid the proficient administration of cloud administrations. Assets can be ensured by an assortment of controls eg - introducing biometric gadgets of CCTV gear, keeping up get to control registers.

### **6.4 Network and Perimeter Security**

This domain speaks of the logical security of routers, switches, other devices and locations where data or virtual images are effectively configured to be stored in a data center. To achieve this protection, various controls such as firewalls, IDS / IPS can be set up to manage network security by denying unauthorized access. We can set up AAA (Authentication, Authentication and Accountability) server for strong authentication.

### **6.5 Virtual OS/Image Security**

This area talks about the security and uprightness of the virtual pictures. As virtual pictures contain client information, so it ought to be considered as basic resources and security ought to be given to shield these virtual pictures. Every one of the pictures are made on server and an assailant or vindictive code can abuse these pictures. Cloud gives chance to aggressors that they can make vindictive pictures, in which they can execute malevolent code on a similar stage where the other customer's pictures exist. The pictures can likewise be altered by interior representatives of specialist organization as they have direct access to every one of the pictures and furthermore by inner workers of customer who take a shot at those pictures. To sift through this issue, encryption of virtual pictures, data validation convention, provenance following and access control have been proposed. Picture name itself ought to be encoded in picture library which gives connecting pointer between picture name and physical area.

### **6.6 Identity and Access Management (IAM)**

IAM improves operational proficiency, administrative consistence the board by overseeing AAA administrations. Not many specialists recommended IAM as a Service to be another



assistance model to accomplish more prominent security and protection objectives in distributed computing. To make it extremely successful excess character the executives, provisioning of cloud administrations, benefit the board ought to be computerized. It gives comfort to recover, oversee, refresh and inquiry for any data. It ought to guarantee that the clients have solid, quick, practical access of assets and data recovery is in a protected way. There ought to be programmed character provisioning when another client is going to benefit the administrations. Mechanized provisioning, validation and approval are the significant worry for security.

We can take care of this issue by utilizing different arrangements, for example, single sign-on, unified character, get to control list, index based help, access based on properties.

## **6.7 Data Security and Storage Security**

This space clarifies security of information put away on servers for example from information age to utilization and after use, legitimate transfer of information. The information ought to be sufficient shrewd with the end goal that on the off chance that it is unveiled by any unapproved element it ought to be good for nothing. The objective can be accomplished by utilizing solid encryption and information covering strategies, great key administration program and to keep up the respectability, advanced mark method can be picked. The correct reinforcement administration ought to be given to customers with the goal that clients can back up their online information and if there should be an occurrence of any debacle they can reestablish their information. A dependable replication plot and proficient document framework ought to be selected. At the point when the customer's goal is met or the customer needs to cease the administration, customer's information ought to be expelled from server. There ought to be appropriate transfer instrument to arrange the information since that information may contain basic data and may cause chance whenever came to wrong individual. A unique consideration must be on the trash transfer from the virtual picture area.

## **6.8 Transmission**

This area clarifies security of information put away on servers for example from information age to use and after use, legitimate transfer of information. The information ought to be sufficient keen with the end goal that on the off chance that it is uncovered by any unapproved substance it ought to be good for nothing. The objective can be accomplished by utilizing solid encryption and information concealing strategies, great key administration program and to keep up the uprightness, advanced mark system can be selected. The correct reinforcement

administration ought to be given to customers with the goal that clients can back up their online information and if there should arise an occurrence of any calamity they can reestablish their information. A solid replication conspire and proficient record framework ought to be picked. At the point when the customer's goal is met or the customer needs to cease the administration, customer's information ought to be expelled from server. There ought to be appropriate transfer instrument to arrange the information since that information may contain basic data and may cause chance whenever came to wrong individual. An exceptional consideration must be on the trash transfer from the virtual picture area.

## **6.9 Monitoring**

This area discusses keeping up logs and keeping watches that could be utilized for evaluating and aides in examination of any disappointment. This can be accomplished by start to finish checking, server and system observing, exchange checking, application observing, occasion log observing, and so forth. There ought to be appropriate computerized log age and the executives framework to record every one of these kinds of checking. These logs ought to be evaluated and broke down occasionally by a specialist or some computerized instruments to produce reports for higher administration and number of security ruptures, and so on ought to be referenced in these reports. A caution framework ought to be executed when any irregularity is identified.

## **6.10 Client Level Security**

This area discusses different security procedures that must be applied at the customer side to shield from different assaults like SQL infusion, XSS, broken verification, and so forth. Utilization of restrictive based APIs ought to be limited and open standard based APIs or program ought to be utilized to get to cloud information. Each contribution from client ought to be approved and confirmed before submitting to the server.

## **CHAPTER-7**

### **A SECURE NETWORK SYTEM**

#### **7.1 Introduction**

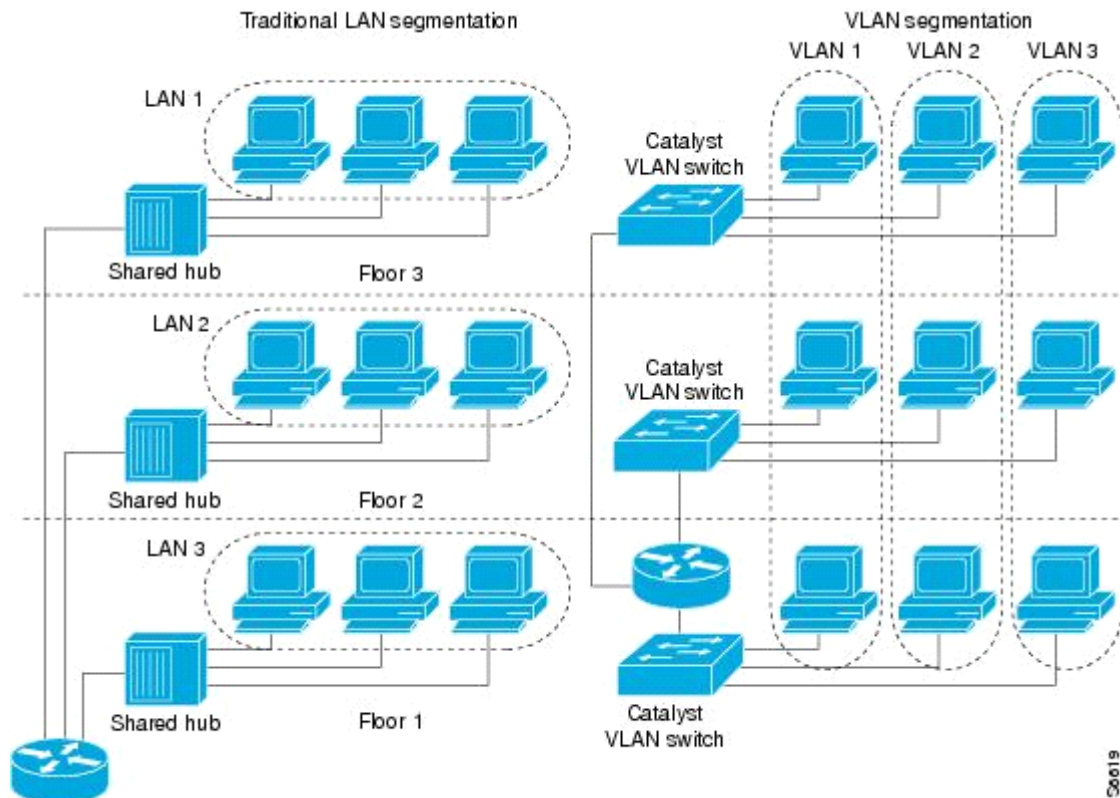
The Local Area Network is a broadly used network system method because a large number of applications is applied in the same broadcast domain of users. Virtual LAN, is one kind of LAN which is a sort of network a group of hosts with a set of common compulsions that provides secure communication. It is essential to give importance that the group of hosts should be in the same broadcast domain, despite the same place.

Other networks like Wide Area Network or Metropolitan Area Network are not relatable with virtual technologies, because the components of the VLAN usually share switching and routing.

#### **7.2 VLAN**

A virtual LAN summarizes the concept of the LAN.A VLAN might constitute a subset of the ports on a particular switch or subspace of ports on multiple switches. The mechanism of VLAN is the VLAN network don't care about the traffic connected with other systems on other VLANs on the same associate network.

VLANs permit arrange specialists to isolate their systems to coordinate the security and useful determinations of their sent frameworks without running new wires or roll out huge improvements in their present system engineering. IEEE 802.1Q is the standard characterizing VLANs; the VLAN identifier or label comprises of 12 bits in the Ethernet outline, making a natural farthest point of 4,096 VLANs on a LAN.



**Fig 7.2: Difference Between Traditional Lan Segmentation and Vlan Segmentation**

## 7.3 Hardware

Computer

Cisco Router

Cisco Switch which supports VLAN's

## 7.4 Software

### Cisco packet tracer:

Cisco Tracer is a cross-stage visual reproduction program structured by Cisco Systems that enables clients to make organize topologies and mimic present day PC systems. The product enables clients to reproduce the setup of Cisco switches and switches utilizing a mimicked direction line interface

## 7.5 Use Case

We are using Enterprises Network Model to show the use case of Vlan and how Real Scenario works when Different Branches of Enterprises are located in Different Cities.

### Proposed Network Design:

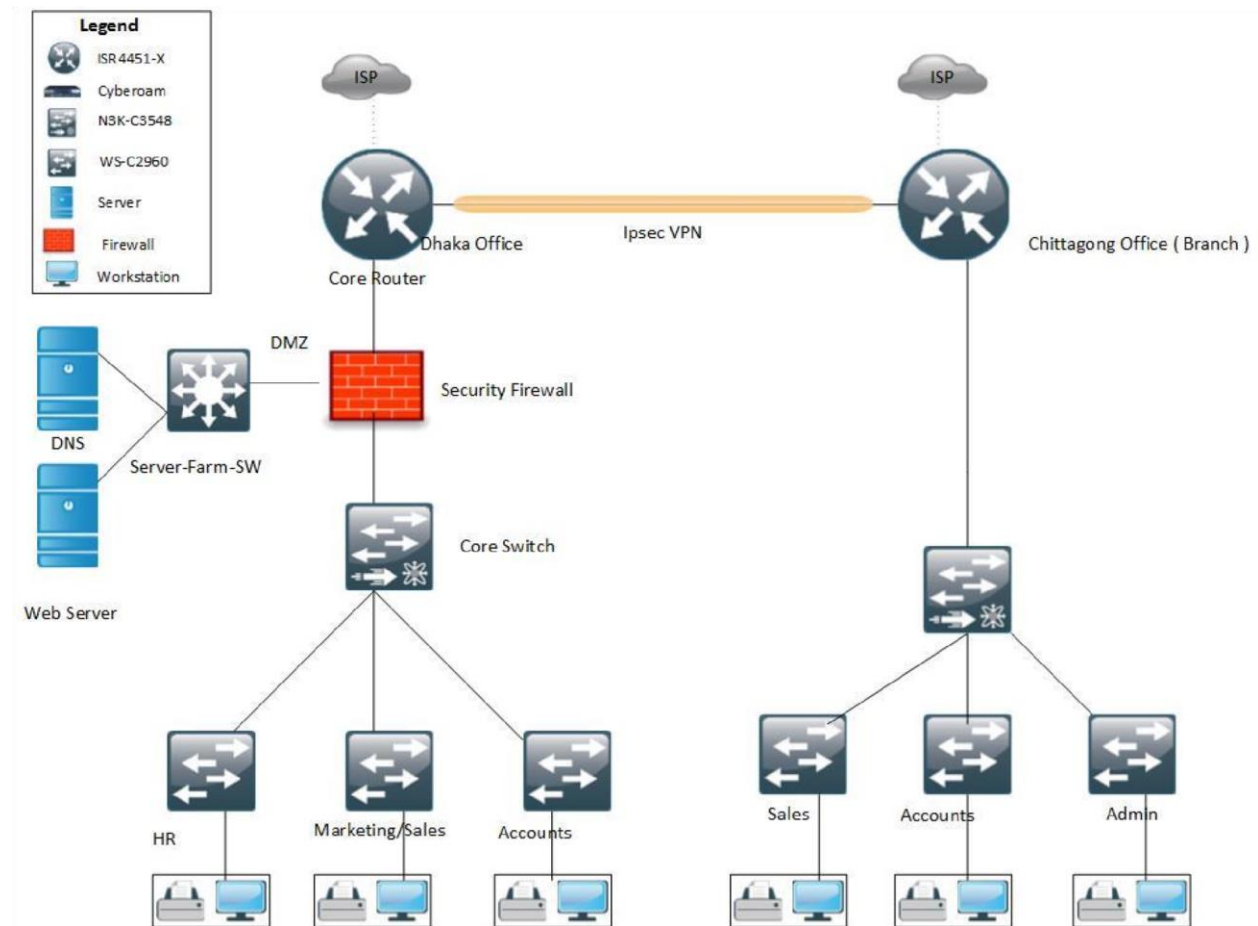


Fig 7.5.1: Proposed Secured Network Design

Network is the important part of the cloud infrastructure security. Our proposed network design for ensuring the organizational network security and web access. This proposed model included the next generation security firewall and all server in the DMZ zone also added number of access control policy for internal and external access. The security feature that are consider of this proposed network model that are:

- ✓ Virtual local area network
- ✓ Security Firewall
- ✓ Intrusion detection systems

- ✓ Intrusion prevention systems
- ✓ Malware protection
- ✓ Advance threat protection
- ✓ DMZ zone
- ✓ Virtual Private network

### Simulation of the Network model:

A simulation has been done using packet tracer simulation software. Our network scenario is the organization head office in Dhaka and one branch office in Chittagong. Head office has web based cloud server that can be access to the branch office of Chittagong. Other service are not accessible to the branch office.

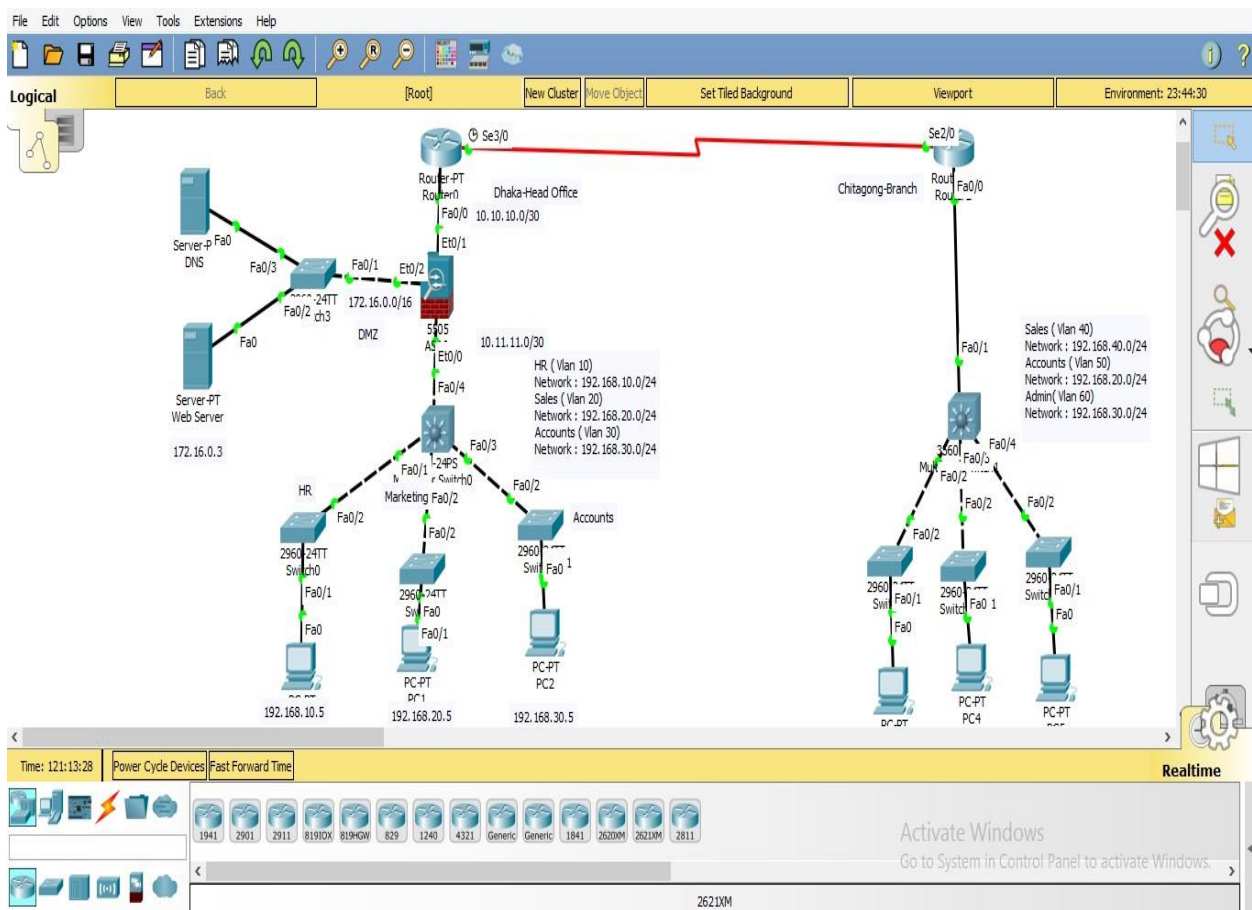


Fig 7.5.2: Simulation of Proposed Network design

### Virtual Local Area Network

Head Office		Chittagong Branch	
VLAN ID	Name	VLAN ID	Name

10	HR	40	Sales
20	Marketing	50	Marketing
30	Accounts	60	Admin

### Security Firewall Implementation

In the realm of PC firewall security, a firewall alludes to a system gadget which hinders specific sorts of system traffic, framing an obstruction between a trusted and an untrusted organize. It is closely resembling a physical firewall as in firewall security endeavors to hinder the spread of PC assaults. A solid edge security shields your system from outer assaults. The primary component on the edge security front is a system firewall. We have incorporated security firewall in this reenactment.

Table: Zone of the Security Firewall

VLAN	Zone	Security Level
VLAN 1	Inside	100
VLAN 2	Outside	0
VLAN 3	DMZ	50

### Access Control Policy for Security Firewall:

We have created different access control rule for implement security. As example:

#### Rule list:

```
access-list internet extended permit tcp any any access-list
internet extended permit icmp any any access-list dmz
extended permit icmp any host 172.16.0.3 access-list dmz
extended permit tcp any host 172.16.0.3 eq www DMZ
```

#### Zone created for Server:

In the firewall we have created DMZ zone for Server and assign security level 50.

```
interface Vlan3 no
forward interface
Vlan1 nameif DMZ
security-level 50 ip
address 172.16.0.1
255.255.0.0
```

## All VLAN communication:

All VLAN are communicated each other fig 8 show the result

The screenshot shows a network simulation interface. On the left, a network topology diagram is displayed. It features a central router labeled 'Dhaka-Head Office' with interfaces Fa0/0 (10.10.10.0/30), Et0/1, and Et0/2 (172.16.0.0/16). A DMZ is connected to Et0/2. The router is connected to a 'Server-PT Web Server' (172.16.0.3) via Fa0/3. Below the router, there are three switches: 'HR' (2960-24TT Switch0), 'Marketing' (2960-24TT Sw), and 'Accounts' (2960 Sw). The HR switch is connected to the router via Et0/0 and has a PC-PT (192.168.10.5) connected to Fa0/1. The Marketing switch is connected to the router via Fa0/4 and has a PC-PT (192.168.20.5) connected to Fa0/1. The Accounts switch is connected to the router via Fa0/3 and has a PC-PT (192.168.30.5) connected to Fa0/1. A 'Server-PT DNS' is also connected to the HR switch via Fa0/3. On the right, a 'Command Prompt' window is open, showing the following output:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.20.5

Pinging 192.168.20.5 with 32 bytes of data:

Reply from 192.168.20.5: bytes=32 time=1ms TTL=127
Reply from 192.168.20.5: bytes=32 time=1ms TTL=127
Reply from 192.168.20.5: bytes=32 time<1ms TTL=127
Reply from 192.168.20.5: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Fig 7.5.3: VLAN communication

## Head Office PC to Web Server:

Head office all PC can access to Web server and ping the Webserver. Fig 8 Show the ping replay of Head office PC to webserver.



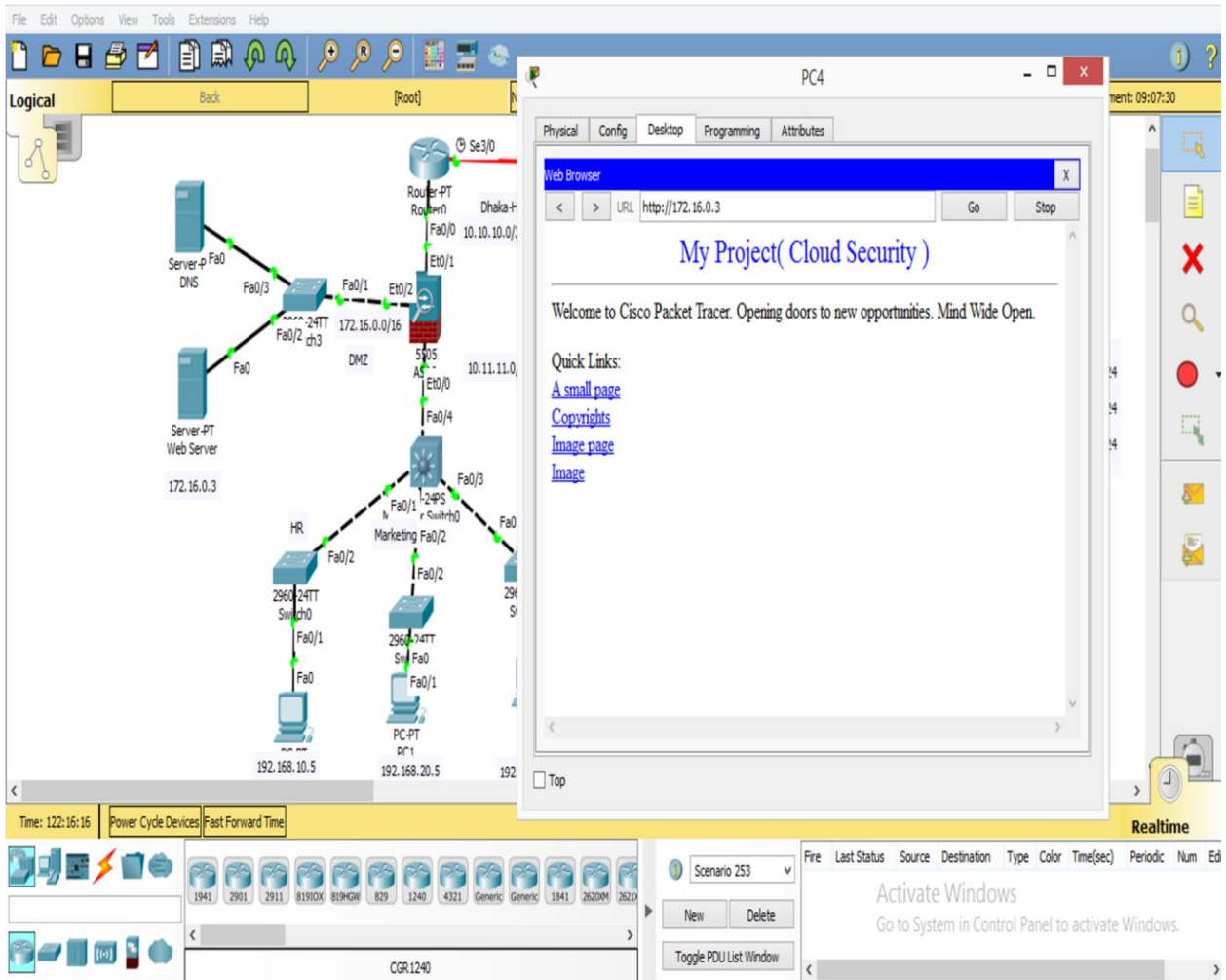
The screenshot displays a network simulation environment. On the left, a network diagram shows a central router labeled 'Dhaka-Head Office' with interfaces Fa0/0 (10.10.10.0/30) and Eto/1. It is connected to a 'Server-p DNS' and a 'Server-PT Web Server' (172.16.0.3) via a switch. The router also connects to a 'DMZ' (172.16.0.0/16) and a 'VLAN' (10.11.11.0/30). Below the router, there are three switches: 'HR (Vlan 10)', 'Marketing', and 'Accounts', each with its own PC (PC1, PC2, and Accounts respectively). The interface at the bottom shows a 'Realtime' table with the following data:

Time	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	N
	Successful	PC0	PC1	ICMP	Green	0.000	N	
	Successful	PC0	PC2	ICMP	Red	0.000	N	

Fig 7.5.4: Head Office PC to Web Server

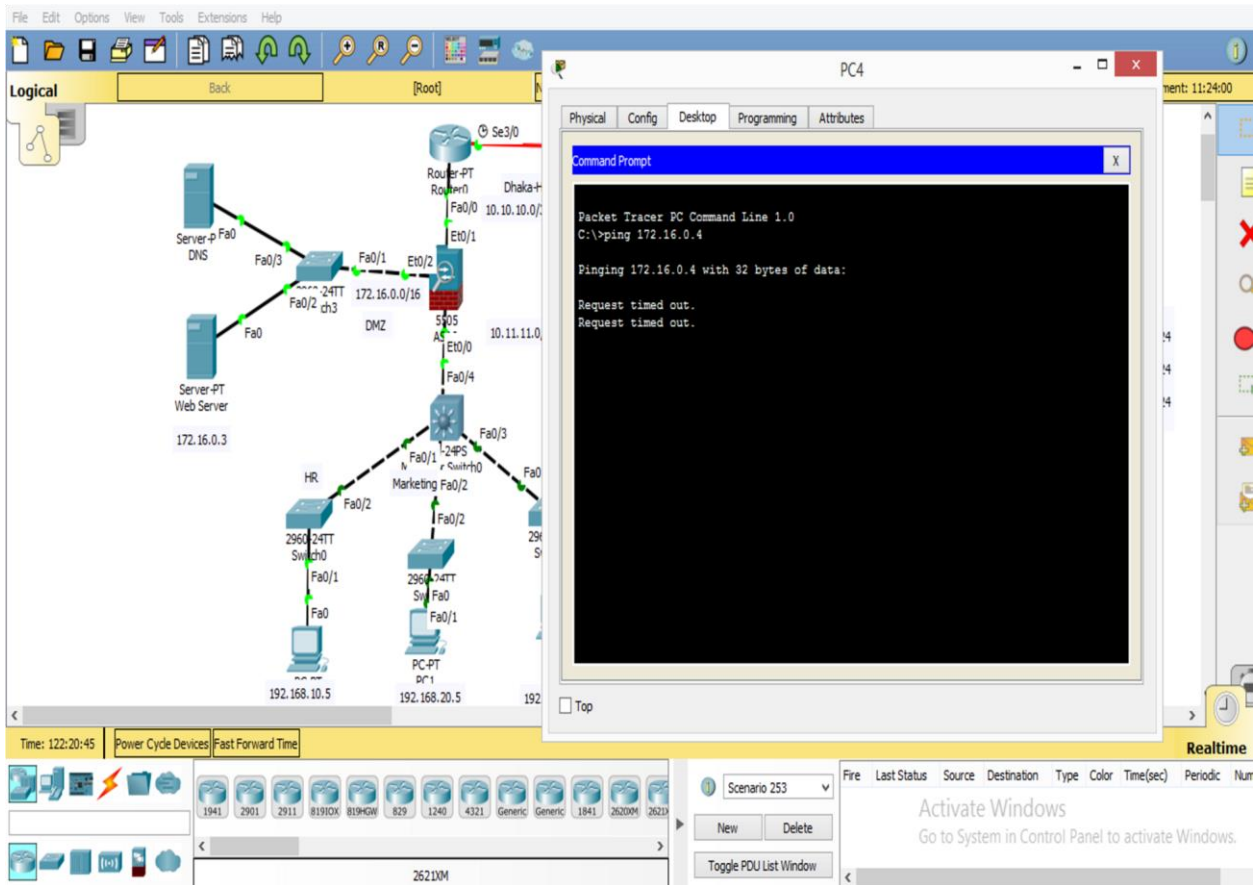
### Chittagong Branch Web Server Access:

Fig 7.5.5 Show the Chittagong Branch PC can Assess Web server.



### Chittagong Branch Other Server Access:

Fig 7.5.6 Show the Chittagong Branch PC cannot Access other server.



Through this networking system we have tried to make a secure network system and if we use cloud storage on this network system by optimizing the threats we can build a secure cloud storage system.

## CHAPTER-8

### Conclusion

Assessment of distributed computing recognizes the start of the new age of data innovation that means in the collected figuring model. In the meantime, this prompts the change of use from neighborhood to the cloud condition, which vigorously benefits our life and work. It has gotten celebrated, strange, and vague expert ideas, for example, conveyed processing, parallel figuring, virtualization, and furthermore.

Contrasting with different ideas and terms, word is "Cloud" is by all accounts dynamic and fanciful, and it is basic to envision the system among "Cloud" and IT. On the opposite side, it will be so a lot of adequate and reasonable for people in general to depict the innovation outwardly. Further, this dynamic creating industry will have an impact on different areas later on. For instance, Cloud processing will effectively support the improvement of on the web and Internet exchange since it is the establishment of sending distributed computing. In the interim, it has spread an extraordinary effect on the equipment business that can be anticipated on the grounds that distributed computing has arranged modern calculation and conveyed results to customers.

Distributed computing is another example dependent on the development, and association of the Internet. The proposal has expounded the on structure, idea, regular use, organization, and head security issues of distributed computing altogether. Hence, coherent answers have been given to the inquiries in the presentation section. The motivation behind this proposition was to center and examine the show of distributed computing and at present primary security issues just as clarify them in straightforward words rather than down to earth specialized terms. The eventual fate of distributed computing is boundless, and the development is incomprehensible in the field of E-business benefits just as the lifestyle, and the essential idea of distributed computing will frame the best approach to arrive at the summit of cloud innovation.

Since some outstanding associations receive distributed computing with a fast increment, framework security issues emerge. As distributed computing is enroute of rising, and principally because of its extreme fascination in sorted out lawbreakers, we can hope to build up a great deal of security occurrences and new sorts of security dangers around it inside the

decades to come. Cloud security issues are an as of late dynamic region of research and experimentation. Heaps of research and examination is proceeding to recognize the issues like cloud security, virtualization, seclusion, and information insurance of assets. In this proposition paper, we have talked about Denial of Service (DoS) assaults, Cloud Malware Injection Attack, Side-Channel Attacks, Authentication Attacks and Man-In-The-Middle Cryptographic Attacks of distributed computing and furthermore give some potential arrangements. The ideas we have examined here will manufacture a vigorous engineering for security in the field of cloud calculation.

## REFERENCES

1. [http://aws.amazon.com/ec2/?nc1=f\\_ls](http://aws.amazon.com/ec2/?nc1=f_ls)
2. <http://aws.amazon.com/solutions/case-studies/parse/>
3. <http://googlecloudplatform.blogspot.fi/2013/12/an-ode-to-sharkon.html>
4. [http://www.ibm.com/developerworks/websphere/techjournal/1206\\_dejesus/1206\\_dejesus.html](http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html)
5. <https://kongwenbin.wordpress.com/2012/07/30/parallel-vs-distributed-computing/>
6. <http://www.turbotekcomputer.com/resources/small-business-it-blog/bid/58074/Difference-Between-NAS-and-SAN-3-Considerations>
7. <http://mc.cs.ut.ee/mcsite/theses>
8. <http://techilistic.blogspot.fi/>
9. <https://www.pcmag.com/article2/0,2817,2372163,00.asp>
10. Bao, L. and Liu, W. (2010) PhD thesis. Shandong University of Technology.
11. Study on Cloud Computing Security' by Feng, D., Zhang, M., Zhang, Y. and Xu, Z. (2011) ' , *Journal of Software*, 22 (1): 71-83.
12. Equn.com (2015). *What Is Distributed Computing?* Available at: <http://www.equn.com/wiki/%E6%96%B0%E6%89%8B%E6%8C%87%E5%8D%97:%E4%BB%80%E4%B9%88%E6%98%AF%E5%88%86%E5%B8%83%E5%BC%8F%E8%AE%A1%E7%A E%97> (Accessed 29 May 2015).
13. <http://www.chinacloud.cn/show.aspx?id=14668&cid=17>
14. 'AMD Invests in a Cloud Gaming Company' by Murariu, C. (2012), SOFTPEDIA, [Internet]. Available from: <http://news.softpedia.com/news/AMD-Invests-in-a-Cloud-Gaming-Company291523.shtml> [accessed 3 May 2015].
15. <http://phdprojects.org/cloud-computing-thesis/>
16. <https://msdn.microsoft.com/en>
17. Godfrey, M., Zulkernine, M.: A server-side solution to cache-based side-channel attacks in the cloud. In: Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on, pp. 163–170. IEEE, 2013.
18. <http://www.ali213.net/news/html/2015-5/156039.html>
19. *Basic review of Cloud Computing* by Gu, X. (2014). Available at: <http://www.51testing.com/html/41/n-867441.html> (accessed 25 April 2015).
20. <https://www.salesforce.com/what-is-cloud-computing/>
21. *Cloud Computing: ICT's Tower of Babel* ,Zhou, H. (2011). Beijing: Publishing House of Electronics Industry.
22. <http://www.slideshare.net/zinnov/internet-of-things-by-samsung>
23. <http://azure.microsoft.com/en-us/>

24. <https://wacnstorage.blob.core.chinacloudapi.cn/marketing>
25. <https://www.openstack.org>
26. <http://news.softpedia.com/news/AMD-Invests-in-a-Cloud-Gaming-Company-291523.html>
27. [http://semanticcommunity.info/Big\\_Data\\_at\\_NIST](http://semanticcommunity.info/Big_Data_at_NIST)
28. <http://www.51testing.com/html/41/n-867441.html>
29. <http://clouddriveconsulting.restoreup.com/2014/01/types>
30. <http://www.equn.com/wiki/%E6%96%B0%E6%89%8B%E6%8C%87%E5%8D%97:%E4%BB%80%E4%B9%88%E6%98%AF%E5%88%86%E5%B8%83%E5%BC%8F%E8%AE%A1%E7%AE%97>
31. Cloud computing: Principles and paradigms ,Buyya, R., Broberg, J., Goscinski, A.M.:, John Wiley & Sons,2010.vol. 87.
32. Improving cloud network security using the tree-rule firewall, X., Chambira, T., Nanda, P., Tan, Z.: Future Generation Computer Systems 30, 116–126, 2014
33. *Securing and Controlling Sensitive Data in the Cloud* by Trend Micro (2014) *Trend Micro SecureCloud*:. Available at: [http://www.trendmicro.com/cloudcontent/us/pdfs/business/datasheets/ds\\_securecloud.pdf](http://www.trendmicro.com/cloudcontent/us/pdfs/business/datasheets/ds_securecloud.pdf) (accessed 6 May 2015).
34. Mobile Services’, *Microsoft Developer Network* by Microsoft (2012/2015) 9 May. Available at: <https://msdn.microsoft.com/en-us/library/azure/jj554228.aspx> (accessed 1 May 2015).
35. *Microsoft Azure* ,Microsoft Azure (2008/2015).. Available at: <http://azure.microsoft.com/en-us/> (accessed 26 April 2015).
36. Improving cloud network security using the tree-rule firewall, X., Chambira, T., Nanda, P., Tan, Z.: Future Generation Computer Systems 30, 116–126, 2014
37. Cloud Computing: benefits,Catteddu, Springer, 2010,D.: risks and recommendations for information security.
38. Open security system for cloud architecture., Koushik, S., Patil, A.P.: Springer, 2014 In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I, pp. 467–471.
- 39.40. Counteracting security attacks in virtual machines in the cloud using property-based attestation. Journal of Network and Computer Applications by Varadharajan, V., Tupakula, U.: 2013.
41. “Security Issues in Cloud Computing and Countermeasures,” by D. Jamil and H. Zaki, International Journal of 2001
42. Manavi, S., Mohammadalian, S., Udzir, N.I., Abdullah, A.: Hierarchical secure virtualization model for cloud. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pp. 219–224. IEEE, 2012.
43. *Public Cloud vs Private Cloud* by Skali Group (2011). Available at: <http://skali.net/public-cloud-vsprivate-cloud> (accessed 27 April 2015).
44. Types of Cloud Computing’, Cloud Drive Consulting, [Internet]. Moosa, F. (2014) ‘ Available from: <http://clouddriveconsulting.restoreup.com/2014/01/types-of-cloud-computing.html> [accessed 28 April 2015].

45. Wong, A. (2011) *How to Secure Cloud Files With Trend Micro Secure Cloud*. Available at: <http://www.bqjournal.com/%E4%BF%9D%E8%AD%B7%E9%9B%B2%E7%AB%AF%E8%B3%87%E6%96%99%E5%AE%89%E5%85%A8-trend-micro-securecloud> (accessed 4 May 2015).
46. A filter tree approach to protect cloud computing against xml ddos and http ddos attack ,Karnwal, T. 459–469. Springer, 2013., Thandapanii, S., Gnanasekaran, A.: In: Intelligent Informatics, pp.
47. An intrusion detection and prevention system in cloud computing: A systematic review, Patel, A., Taghavi, M., Bakhtiyar, K., Celestino J´uNior, J.: *Journal of Network and Computer Applications* 36(1), 25–41, 2013
49. *Cryptography and Network Security*, Stallings, W.: 4/E. Pearson Education India, 2006.
50. <http://mohamednabeel.blogspot.fi/2011/03/proxy-re-encryption.html> (accessed 9 May 2015). Yoosuf, N. (2011/2015) ‘Proxy Re-Encryption’, *Blog Spot*, 2 March. Available at: Cloud computer Security techniques and tactics by Winkler, 2011. V.J.: *Securing the Cloud*:. Elsevier,
51. Improving cloud network security using the tree-rule firewall, X., Chambira, T., Nanda, P., Tan, Z.: *Future Generation Computer Systems* 30, 116–126, 2014
52. Encryption, Cryptanalysis and Hash Functions’ by Prabhu, M. (2011/2014) ‘, *Blog Spot*, 6 July. Available at: <http://techilistic.blogspot.fi/> (accessed 7 May 2015).
- 53‘The Concept and Connotation of Cloud Computing’, China Cloud, by Liu, P. (2014) [Internet]. Available from: <http://www.chinacloud.cn/show.aspx?id=14668&cid=17> [accessed 26 April 2015].
- .54. The Future and Application of PaaS’, *Tech Target Cloud Computing* by Teng, X. (2014) ‘, [Internet]. Available from: [http://www.searchcloudcomputing.com.cn/showcontent\\_84737.htm](http://www.searchcloudcomputing.com.cn/showcontent_84737.htm) [accessed 29 April 2015].
55. *Big Data Ecosystem Reference Architecture* , Levin, O. (2013). Available at: [http://semanticcommunity.info/Big\\_Data\\_at\\_NIST](http://semanticcommunity.info/Big_Data_at_NIST) (accessed 7 May 2015).
56. Security in Cloud Computing Kazi Zunnurhain<sup>1</sup>, and Susan V. Vrbsky<sup>2</sup> Department of Computer Science The University of Alabama . Q.Luo and Y. Fei, “Algorithmic collision analysis for evaluating cryptographic systems and sidechannel attacks,” in *Hardware-Oriented Security and Trust (HOST)*, 2011 IEEE International Symposium on, pp. 75–80, IEEE, 2011
57. *Difference between NAS and SAN - 3 Considerations* by Kline, S. (2011). Available at: <http://www.turbotekcomputer.com/resources/small-business-it-blog/bid/58074/DifferenceBetween-NAS-and-SAN-3-Considerations> (accessed 26 April 2015).
- 58.. Amazon (2012) *AWS Case Study: Parse*. Available at: <http://aws.amazon.com/solutions/casestudies/parse/> (accessed 1 May 2015).
- OpenStack (2010/2015). *OpenStack*. Available at: <https://www.openstack.org/> (accessed 26 April 2015).
- Internet security glossary Shirey, R.: Rfc 2828:.The Internet Society, 2000.



Proceedings of the International Conference on Advances in Computing, Bedi, H.S., Shiva, 463–469. ACM, 2012.S.: Securing cloud infrastructure against co-resident dos attacks using game theoretic defense mechanisms. In: Communications and Informatics, pp.

*Design and Implementation of Enhanced Parallel Computing Framework System.*, Tu, H., Zou, H. and Lin, R. (2010) PhD thesis. Beijing University of Posts and Telecommunications.

*Understanding of Cloud Computing*, Microsoft (2013). Available at:

<https://wacnstorage.blob.core.chinacloudapi.cn/marketing-resource/documents/1%20%E8%AE%A4%E8%AF%86%E4%BA%91%E8%AE%A1%E7%AE%97.pdf> (accessed 27 April 2015).

Cross-vm side channels and their use to extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: pp. 305–316. ACM, 2012.

Navigating the IBM Cloud, Part 1: A primer on Cloud Technologies’, IBM Developer Work, by Jesús. J.D. (2012) ‘ [Internet]. Available from:

[http://www.ibm.com/developerworks/websphere/techjournal/1206\\_dejesus/1206\\_dejesus.html](http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html) [accessed 27 April 2015].

Cloud computing security issues and challenge” by Popovic K; Hocenski Z; (2010), “, 5533317searchabstractMIPRO, 2010 Proceedings of the 33rd International Convention , pp 344,24-28 May 2010.

Trust management framework for attenuation of application layer ddos attack in cloud computing ,Contractor, D. 201–208. Springer, 2012., Patel, D.R.: In: Trust Management VI, pp.

Amazon (2007/2015) Amazon web services. Available at: [http://aws.amazon.com/ec2/?nc1=f\\_ls](http://aws.amazon.com/ec2/?nc1=f_ls) (accessed 26 April 2015).

An ode to Sharkon’, *Google Cloud Platform Blog*, by Bechtolsheim, B. (2011/2015) ‘6 December. Available at: <http://googlecloudplatform.blogspot.fi/2013/12/an-ode-to-sharkon.html> (accessed 1 May 2015).

*Introduction to Cloud Security* by Fang, J. (2009).

*Principled Design of the Modern Web Architecture* by Fielding, R. and Taylor, R. (2000) New York: ACM.

*Big Data Storage*: Beijing: Posts & Telecom Press. By *Practical Guide to MongoDB* by Guo, Y. (2015)

*The NIST Definition of Cloud*, U.S. Department of Commerce (2011) ‘. Gaithersburg: National Institute of Standards and Technology. Available at:

<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (accessed 25 April 2015).

Wikipedia (2015) *Cloud computing*. Available at: [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing) (accessed 25 April 2015).

*Securing the Cloud* by Winkler, V. (2011). Waltham: Elsevier.

*Cloud Computing: Cloud Security to Trusted Cloud* by Wu, J., Shen, Q., Zhang, J., Shen Z. and Ping, L. (2011). PhD thesis. Hangzhou Normal University and Zhejiang University.

*Parallel vs Distributed Computing* by Kong, W. (2012). Available at: <https://kongwenbin.wordpress.com/2012/07/30/parallel-vs-distributed-computing/> (accessed 26 April 2015).  
*Analysis of Cloud Architecture in Technical View* by Wu, Z. (2010). Available at: <http://www.infoq.com/cn/articles/analyze-cloud-architecture/> (accessed 27 April 2015).

Survey on Security Issues of Cloud Computing' by Yang, J., Wang, H., Wang, J. and Yu, D. (2012) ' , *Journal of Chinese Computer Systems*, 33 (3): 473-479.

*Cloud Computing and the Internet of Things* by Yang, Z. and Zhou, F. (2011). Beijing: Tsinghua University press.

Samsung (2014) *Internet of things service model*. Available at: <http://www.slideshare.net/zinnov/internet-of-things-by-samsung> (accessed 30 April 2015).

Richardson, L. and Ruby, S. (2007) *RESTful Web Services*. Sebastopol: O'Reilly Media.

Time Sharing in Large Fast Computers', Proceedings of the International Conference on Information processing, by Strachey, C. (1959). 'UNESCO, B.2.19: 336–341.

*New Development in NVIDIA Cloud Game Service* by Le, L. (2015). Available at: <http://www.ali213.net/news/html/2015>

## Security Issues and Solutions

---

### ORIGINALITY REPORT

---

**25%**

SIMILARITY INDEX

**18%**

INTERNET SOURCES

**1%**

PUBLICATIONS

**15%**

STUDENT PAPERS

---

### PRIMARY SOURCES

---

<b>1</b>	<b>publications.theseus.fi</b> Internet Source	<b>10%</b>
<b>2</b>	<b>Submitted to Harrisburg University of Science and Technology</b> Student Paper	<b>3%</b>
<b>3</b>	<b>ijarcsse.com</b> Internet Source	<b>3%</b>
<b>4</b>	<b>Submitted to Daffodil International University</b> Student Paper	<b>2%</b>
<b>5</b>	<b>Submitted to Asia Pacific University College of Technology and Innovation (UCTI)</b> Student Paper	<b>1%</b>
<b>6</b>	<b>Submitted to Victoria University</b> Student Paper	<b>1%</b>
<b>7</b>	<b>Submitted to Sheffield Hallam University</b> Student Paper	<b>1%</b>

---