DETECTION AND MITIGATION SECURITY THREATS IN CLOUD SYSTEMS

BY:

ADDY ANDRENE NII AYITEY

A THESIS PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY IN PARTIAL FULFILLMENT OF THE REQUIREMENT OF

MASTER OF SCIENCE (INFORMATION TECHNOLOGY)

JULY 2019

DECLARATION

I state that the material submitted for assessment is my own work, except where credit is unambiguously given to others by citation or acknowledgement. In presenting this project to

the Kwame Nkrumah University of Science and Technology, I give permission for it to be made available for use in accordance with the regulations of the University. I also give permission for the title and abstract to be published and for copies of the report to be made and supplied to any bona fide library or research worker, and to be made available on the World Wide Web.

DEDICATION

This thesis is dedicated to my mother, who worked hard to support his son's educational endeavors. May she rest in peace.

ACKNOWLEDGEMENT

I would like to express my gratitude to my colleagues, friends and family, who gave me great support to complete this dissertation. First and foremost, I would like to thank my supervisor. Dr Michael Asante the Head of Department. This dissertation would not be possible without his continuous support throughout my project. I am deeply impressed by his enthusiasm for research, attention to details and diligent work ethic. His encouragement helped me overcome the difficulties in research. His guidance helped me improve the skills of critical thinking, writing and presenting, which will bring significant benefits to my future career. I am extremely lucky to have Dr Michael Asante as my Supervisor.

I would like to express my sincere gratitude to Dr Edward Ansong who served as my dissertation partner. He gave me technical support in my research His valuable feedback helped improve this dissertation. He provided me with new and priceless perspectives in research. He also served as one dissertation reader and offered useful suggestions to improve this dissertation.

Last but most important, I want to thank my family. I would like to thank my wife and kids for their unconditional support both emotionally and financially over the years. They make enormous sacrifices to help me make the achievements today. I cannot imagine a life without their love and blessings.

TABLE OF CONTENT

Contents

LIST OF FIGURES

ABSTRACT

Clouds systems provide computation and storage services to organizations and individuals with improved flexibility and low cost. Cloud customers hire resources in the form of virtual machines (VMs) within the cloud. However, these VMs may face various security threats. In this paper, three scenarios were created using RIVERBed simulation tool to detect and mitigate potential security threats targeting cloud systems. The primary objective of these scenarios is to evaluate the performance of database and web application under three different scenarios (no firewall, firewall and firewall blocking the web traffic). To demonstrate how these three scenarios can enhance cloud security, where there is no firewall, another scenario where firewall is created to filter database and web application packets and the third scenario is made to block the web traffic across the cloud. The performance metrics selected at the three levels (global level, node level and link level) is used to evaluate the performance for the database and web application from the simulations using two applications the database and web application, it is seen that the database application performance is improved when the web traffic is blocked. Even against the packet latency and the security policies the database point to point utilization is enhanced.

.

CHAPTER ONE

INTRODUCTION

1.0 Introduction

The Cloud Service System has undergone several transformations from mundane data storage to rendering Artificial Intelligent services, execution of applications, virtual Hardware Infrastructure among others. Cloud Security and Privacy has become one of the most prevalent areas in security research because of the associated threats it poses. The desire of businesses

and organizations is to reduce cost while improving efficiency has placed so much pressure on cloud service providers which has also promulgated to the astronomical increase in cloud service threats. The typical Client – Service registration through cloud tunnelling make it susceptible to the same various forms of attacks like applications systems. There are however various forms of clouds. These are Private, Public, Community and Hybrid Clouds.

Generally, private clouds run within private networks. This is where a business entity or organization's network remains inaccessible from outside of the business network. On such networks, accessing the internet will require a different connection to enable internet access. Since private clouds are usually owned by an organization, its access also comes with a certain level of security restrictions. Public Clouds can be generally referred to as a simple internet based clouds that can be accessed publicly. Currently, public clouds have gone beyond conventional file storage and file sharing to Artificial Intelligent led business processing services among others.

There has also been a growing trend in Cloud computing where organizations harness related resources to create a community of Cloud. This is referred to as Community cloud, where organizations leverage on the resource needs of each other to create a domain of cloud community to share similar resources. The final form of cloud is the Hybrid Clouds which goes beyond just amalgamation of the different forms of cloud to the integration of highly advanced heterogeneous convoluted security policies and service operations to form unit architecture.

The main concern in cloud computing is security, where the key issues ranges from Confidentiality, Integrity, Availability, Access control and Trust. This situation exists because at every instance, cloud service resources are shared among multiple clients which may end up being business competitors and as such, a technical failure in confidentiality could expose company secrets. The next security issue in cloud computing is Integrity, which is the assurance that, something is, what it says it is. In business environment, where data integrity is key to the

sustenance of the business success, an organization committing its entire business data to a remote server infrastructure is really a risky venture to engage in which also adds to the issues raised about the use of cloud infrastructure. Access control has also been one of the many major challenges in this area because of the numerous application level attacks. This threat has also contributed to the various quagmire business owners have about cloud computing services. All these issues discussed settles down on Trust, which is the principal motivation as most businesses have issues with cloud service architecture.

1.2. Statement of problem

Over the past decade, there has been an increase in the number of reported incidents of cloud computing breaches. These attacks appear in two folds: namely the security related issues associated with the end user of cloud services and the cloud service providers itself who serve as the cloud hosting companies (White 2009). Provision of a secured trusted infrastructure has also become a serious challenge especially when it is situated as a public system irrespective of the security policies which are attached.

Beyond the use of cloud server infrastructure, another technology which has been successful with its integration with cloud systems is Virtualization. This technology adds another layer to the cloud system architecture to provide virtual environment where an extra security policy could be integrated additionally and multiple instance of the same resource again could be replicated among other clients (Atayero 2011). Even though the security of client's business information is given a high priority in virtual server environment (refference3), there are however some weaknesses associated with it. These limitations include virtual server attacks. The vulnerability usually located at the authentication policy implementation level and the read write operation. The other form of vulnerability in virtual server is that of frequent updates (Rehman Amjad 2014). These attacks could lead to several security issues in the virtual services

such as illegal read and write operations among others. There is therefore a need to carry out a simulation implementing three firewall scenarios to model the various level of issues related to these stated problems and the tool we intend to adopt is the University Edition of Open IT guru which detail the simulation and the implementation procedure to arrive at the result.

1.3 Justification of the study

There are growing challenges in cloud computing environment due to their data storage architecture. Various security related issues such as Confidentiality, Data Integrity, Availability and Data Privacy have become key issues surrounding cloud computing environment. Research around the field from academia and industry are being carried out to provide solution to these security issues. There have been numerous proposed techniques that have been adopted to enhance the security of cloud system environment; however, many of these have still not been able to provide the enhancement customers of cloud computing systems have always expected. This study makes comparative analysis of cloud computing security techniques and examine the techniques through simulations to give assertions on the simulated concepts.

1.4 Aim and Objectives

The aim of this research is to assess the various performance levels of three cloud platfomrs scenarios namely No firewall, Firewall and firewall with blocking access in cloud computing environments.

The objectives of this research are

1. To identify existing cloud computing security challenges and their solutions from reviewing of literature in the field.
2. To simulate three scenarios of cloud architecture with No Firewall, With Firewall and with blocking access on Firewall

3. To carry out a comparative analysis of the various scenarios and to evaluate the performance of cloud and understand the level of security requirements.

1.5 Research Questions

With respect to the objectives stated above and for them to be realized, the questions relevant to achieving the anticipated resolutions must be addressed. The questions to be asked in this research include:

1. What are the current cloud security challenges?
2. Does firewall eradicate the security threats on Cloud computing
3. Which cloud security model provides the best solution for security?

1.6 Contribution to Knowledge

This study provides enough documentation for network engineers and administrators as well as other stakeholders to have hands on knowledge regarding the choice of cloud architecture to sign up for. The study also introduces the readers to the benefits associated with the scenarios discussed to give administrators and network managers' prior knowledge to keep them informed in the instances of making decision around the field. In addition, the study throws more light on prominent works done in the field of cloud computing security and provides rich literature in the field of cloud computing security.

1.7 Organization of the study

This document is divided into five chapters. In the first chapter, the research scope is introduced while the goal and objectives is discussed. The research problem, justification and research questions were all discussed. The chapter ends with the organization of the study.

In the second chapter, several related articles were reviewed along with their approach. The third chapter describes the research methodology used for the study. The fourth chapter, focuses on the empirical results obtained and the discussions of these results. The final chapter provides concluding discussions and recommendations for further academic research.

CHAPTER TWO

LITERATURE REVIEW

2.0 Overview

The chapter reviews a couple of literature in cloud computing with theoretical background in to give a deeper understanding of the importance and role of information security in the space of cloud computing and a multi stage process for countering security risks and disaster recovery. This study aims at presenting a broad introduction to cloud computing, data security challenges and opportunities in the cloud.

2.1 Definition of Cloud Computing

Cloud is a model architecture designed to aid computing services over the public or private network and usually priced on a pay per use or pay as you go bases and offered to individuals or group on shared resources over a period of time (Srivastava, 2014).

The concept has evolved from various technologies like grid computing, virtualization, cluster computing, and utility computing and among others. Cloud computing enables ubiquitous and on-demand access to network resources and shares a pool of configurable computing resources that can be provisioned and released without much technical expertise (Mell & Grance, 2011).

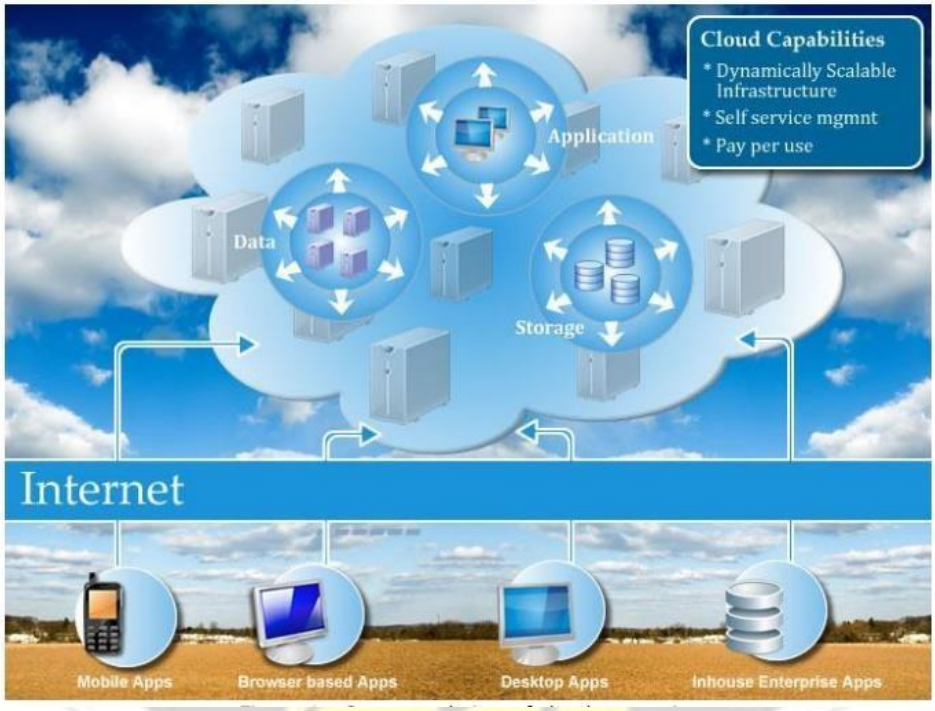


Figure 2.1 Conceptual View of Cloud Computing Source: (Wu et al., 2009)

2.1.1 Evolution of Cloud Computing

J. C. R. Licklider proposed a framework through the usage of public networks to offer computational services to individuals and enterprises which is no different from todays' Cloud computing philosophy. Several researchers are of the view that cloud computing was first presented by John McCarthy who proposed the provision of computing been delivered as a

public utility. Figure 2.1 depicts the trend of how computational model has evolved over time from the 70s to presenting showing the move from centralized systems through distributed systems into Internet and Mobile computing and finally cloud computing (Srivastava, 2014).

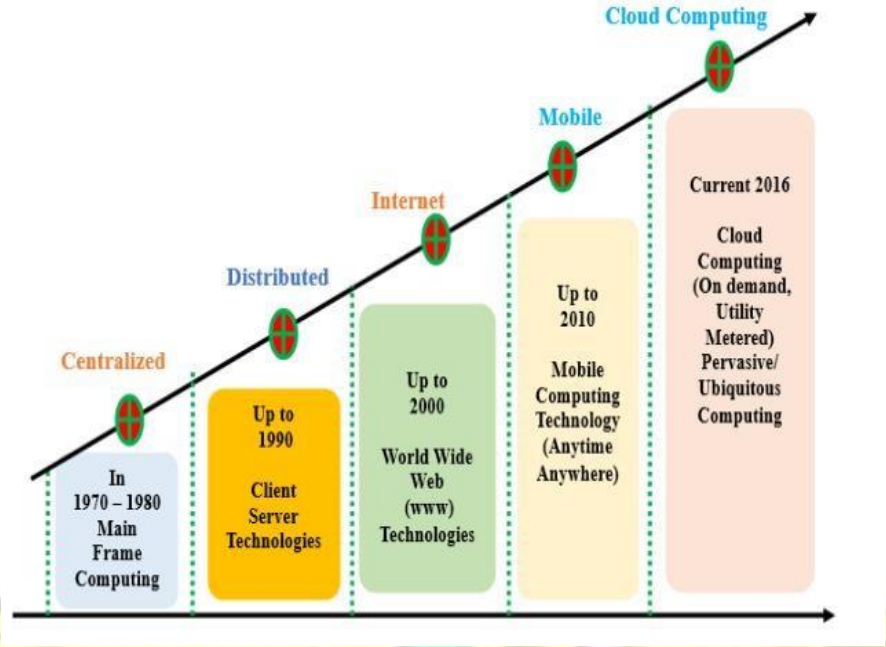


Figure 2.2 Evolution of Cloud Computing Source: (Srivastava, 2014)

Several other concepts or models have been in use before cloud computing which are believed to have orchestrated today's cloud. Utility Computing is credited to have been proposed by John McCarty in his speech at MIT said "If computes of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone is". Utility computing is nothing more than metered usage of computing services and cloud is no different from this analogy.

Grid computing involves achieving or arriving at a common computational goal through the use of distributed computer resources and Autonomic computing is basically developing a computer system that is able to self-manage itself in order to overcome or curb the high rate growth of computing systems management.

2.1.2 Enabling Technologies

For every technology to be invasive and disruptive there must be several factors in place to see to its successful acceptance in space. Several factors made cloud computing a success and below are some major enabling technologies that made cloud computing a success(IEEE, 2010).

a. *Broadband Networks and Internet Architecture:* Cloud can never be in existence without Networks, Cloud seamlessly is referred to by other people as the Internet. The major network and Internet technologies have contributed to the success of Cloud computing.

Cloud thus cannot successfully exist with Networks. Broad and Baseband and other Network technologies have served as the spring board for Cloud computing to thrive. Basically, all clouds need to be connected to a network of which the largest is the Internet. ISPs that help connect the globe are infrastructures that are helping Cloud to be implemented successfully without users worrying about these technologies. Connectionless packet switching coupled with Router-based interconnectivity are two fundamental components of Networks that's making Cloud a success(Pfarr, Buckel, & Winkelmann, 2014).

b. *Data Center Technology*: data centres is a facility for housing computer systems and associated components like but not limited to telecommunications and storage systems with technologies like Virtualization, standardization and modularity, Automation and remote operation management. The department in any organisational setup responsible for housing and maintaining the back-end of the IT infrastructure and data storage is referred to as the Data Center. They contain servers and databases and usually run on mainframes. Big Data platforms like Hadoop and Spark are all amazing technologies that have made the implementation of cloud very easy. Data center technologies coupled with

Storage technologies have immensely provided the requisite technologies which has made cloud implementation a success. Distributed File systems coupled with advance Database technologies are all contributing technologies to the implementation of Cloud(Sharma et al., 2017).

c. *Virtualization Technology:* This technology involves conversion of Physical IT resources into virtual ones and is now implementable with servers, storage, networks and power. Virtualization is required to address to provide resources that can be dynamically repurposed, which application they serve and how they are used. Virtualization has made it very easy to easily implement any service expected of an enterprise without investing so much into hardware infrastructure. Several services can now be deployed on a single cloud component without realizing the complexity of the infrastructure.

d. *Web Technology:* Dynamic resource provision (scheduling) like mesos, yarn and among others are and Software technologies have provided the base for Cloud. Programming paradigm shifts from central and standalone platforms unto more decentralized networked systems have contributed to the success or have enabled Cloud (Srivastava, 2014).

e. *Multitenant Technology:* this is the technology that enables multiple users to access the same application logic concurrently without much difficulties most especially in the area of databases. The technology sees to it that end users or tenants do not have direct access to data and configuration logs that isn't their own(Gai & Li, 2012).

2.1.3 Benefits of Cloud Computing

Every breaking technology comes with its own advantages that sparks its' interest among several users. Cloud computing is no different and it is evident in how the term is been heard in several news articles, technology magazines and among technology enthusiasts (Müller, Holm, & Søndergaard, 2015). The technology offers most businesses and other institutions some merits beyond their costs. Cloud aids the establishment of virtual offices that offers flexibility of connecting easily with your business and other businesses within any part of the world (QLD, 2017). The growth in web-enabled computers within today's business world makes access to data easier. Some of the major benefits associated with Cloud includes but not limited to the following.

a. Flexibility: services provided via cloud platforms are usual advantageous for enterprises which have growing bandwidth demand. Scalability is very easier on cloud services as compared to implementing onsite. Scaling up or down on cloud infrastructure is as easy as picking up a phone.
b. Disaster Recovery: In the event of disasters and other natural unforeseen events, recovering your data from the cloud is a major advantage enjoyed by enterprises on cloud services. Data recovery becomes easier as most cloud services have several backups on and offsite. Some database backups are even continental in that a server in the United States could have its backup in Europe or somewhere in Asia. This provides a lot of assurance of data recovery in the events of disasters.
c. Automatic Software Updates: administrators have limited work to do regarding software update and upgrades. Patches are automatically installed with less or no notice on the part of the end user. Administrators are thus freed from periodic manual updates.
d. Capital-expenditure Free: Implementing cloud or signing up on cloud usually reduces the high cost of purchase, installation training of technical staff to support and maintain

infrastructures. These drastically reduce the cost involved in using these services as opposed to keeping one's own setup.

e. Increased collaboration: Collaboration among staff is high with enterprises running on cloud. Cloud provides the possibility of a platform for people from different geographical location to work on the same project without difficulties.

f. Security: It is very hectic for companies to loose most of their physical infrastructures like laptops and other storage devices due to the data that may be present on them. Signing up to cloud is one of the best ways to curb the fear of loss of data when companies' resources are affected by theft, damaged or natural disasters. Cloud provides the chance to have copies of such information been backed up and also been encrypted with highly sophisticated and complex algorithms. A loss of a device thus not threated data that is stored in the cloud.

According to a blogpost by IBM, cloud basically provides a virtualized environment for internet connectivity increasing accessibility to resource and speeding market through cloud enabled users. Cloud also ensures data security with no hardware failure on premises due to networked backups. Provides savings on equipment due to enjoyment of infrastructure as a service. This merit gives efficiency to businesses and provides a competitive advantage against other enterprises. Other strategic views includes but not limited to streamlined work, regular updates and collaboration (IBM, 2018).

2.1.4 Characteristics of Cloud Computing

a. *On-Demand Self-Services:* Cloud computing provides resources *on demand*, i.e. when the consumer wants it. This is made possible by *self-service* and *automation*. Self-service means that the consumer performs all the actions needed to acquire the service herself, instead of going through an IT department, for example. The consumer's request is then automatically processed by the cloud infrastructure, without human intervention on the provider's side(Srivastava, 2014).

b. *Broad Network Access:* Cloud is highly characterized by is availability across the globe. In most cases than not, cloud resources reside on the Internet and other private networks which makes access to these resources easily accessible from any geographical location and from different kinds of devices. These resources are also accessible from a wide range of locations that offer online access.

c. *Resource Pooling:* is an IT term used in cloud computing environments to describe a situation in which providers serve multiple clients, customers or "tenants" with provisional and scalable services(El-gazzar, 2014).

d. *Rapid Elasticity:* is a cloud computing term for scalable provisioning, or the ability to provide scalable services. Experts point to this kind of scalable model as one of five fundamental aspects of cloud computing.

e. *Measured Services:* is a term that IT professionals apply to cloud computing. This is a reference to services where the cloud provider measures or monitors the provision of services for various reasons, including billing, effective use of resources, or overall predictive planning (Techopedia, 2017).

2.2 Cloud Computing Deployment Model

a. *Private Cloud: to* the cynics, the "private cloud" looks a lot like what we used to simply call an on-premises data center. The difference is that you use virtualization, software, and automation to organize your infrastructure like the public cloud. While this offers some of the flexibility found in the public cloud, the big benefit for private cloud is that it gives you more control over security, data privacy, and compliance.

b. *Community Cloud:* Community clouds are a recent variation on the private cloud model that provides a complete cloud solution for specific business communities. Businesses share infrastructure provided by the CSP for software and development tools that are designed to meet community needs.

c. *Public Cloud:* this model is the most common way of cloud deployment like servers and storage and involves third party cloud service provider and usually deployed over the Internet. Microsoft Azure is a typical example of Public Cloud Model. It emerged as Software as a Service but now offers Server and virtualization and beyond.

d. *Hybrid Cloud:* A hybrid cloud includes a variety of public and private options with multiple providers. By spreading things out over a hybrid cloud, you keep each aspect at your business in the most efficient environment possible. The downside is that you have to keep track of multiple different security platforms and ensure that all aspects of your business can communicate with each other(Judith, Robin, Marcia, & Fern, 2017).

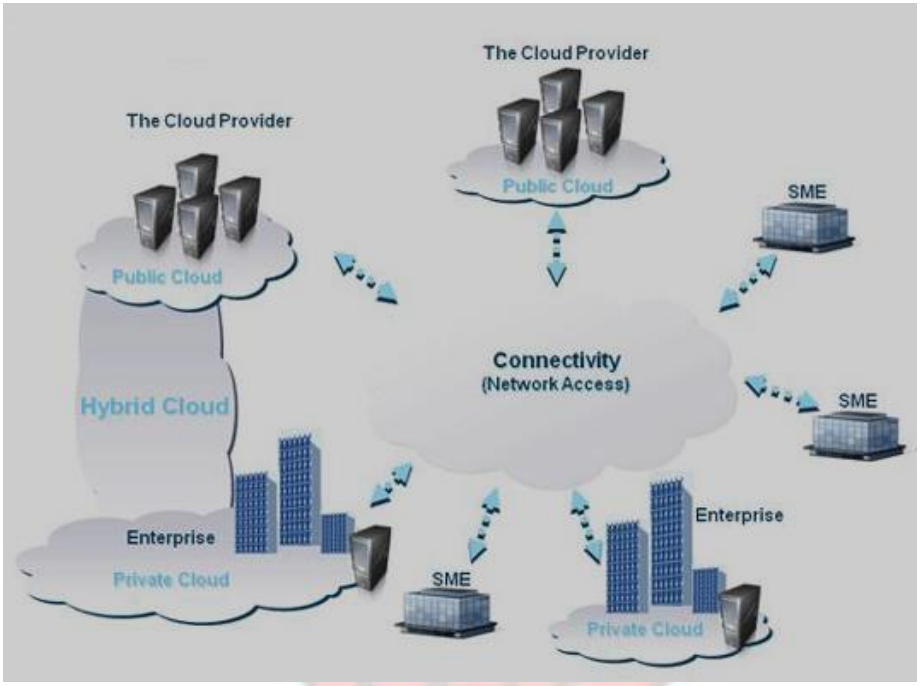


Figure 2.3 Cloud Deployment Models Source: (Judith et al., 2017)

2.3 Cloud Computing Service Model

e. Software as a Service (SaaS): This is a model that is highly scalable in Internet based applications with hosting on the cloud and offered to clients as services. A typical example of this kind of model is Google Docs, acrobat.com and salesforce.com

f. Platforms as a Service (PaaS): With PaaS, the model is usually used to design, develop and build as well as test applications that are provided by cloud infrastructure. Examples includes Azure Service Platform from Microsoft and Google App Engine

g. Infrastructure as a Service: IaaS is per per use model with services like storage, database management system which are offered on demand and example includes 3Tera and GoGrid.

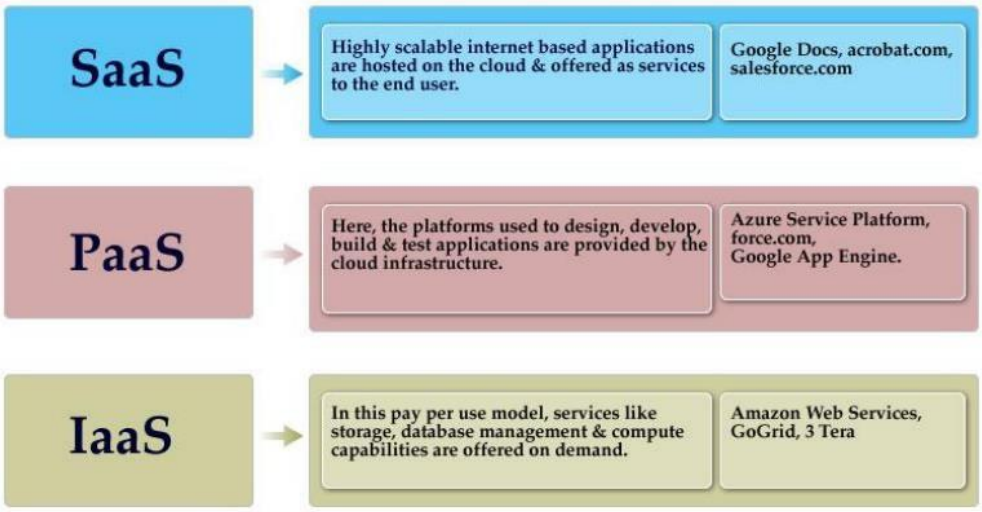


Figure 2.4 Cloud Models Source: (Wu et al., 2009)

2.4 Cloud Security Standards and Issues

Cloud security encompasses principles and procedures applied to protect data, applications and infrastructure within cloud computing environments. A study by Yu et al (2017) shows that Security issues are one of the biggest obstacles to the widespread adoption of cloud computing services among enterprises. The study selected a couple of papers and analysed the article based on publication year, outlet, keywords and research perspectives and data sources. The outcome showed current research providing useful information about security in the cloud (Yu, Wang, Wang, Su, & Ge, 2017).

Figure 2.4 Visualization analysis on keywords Source: (Yu et al., 2017)

Market analysis on Global Security Market Growth Analysis shows a rise in value from US$425.4 Million to US$963.4 Million in between the years 2012 and 2014.

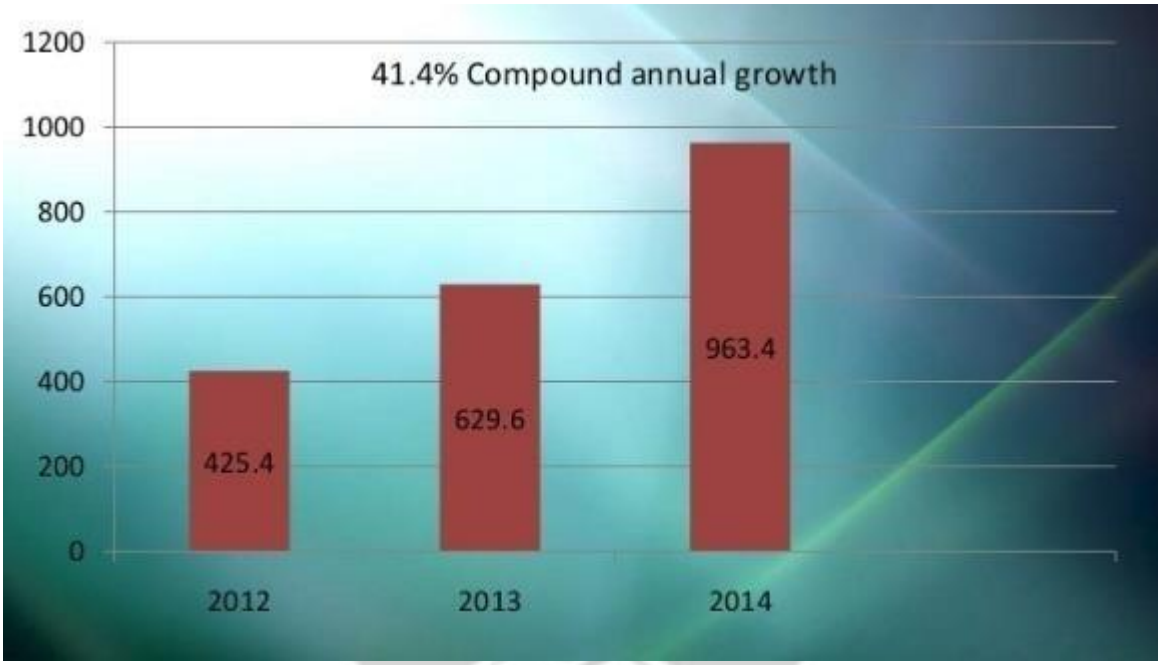


Figure 2.5 Global Cloud Security Market Growth Analysis 2012 – 2014 Source (Cision, 2015)

There has been increasing partnership among Cloud Service Providers and Security solutions providers to see to a safe and sound security among data in the cloud as most companies find it difficult entrusting their classified and sensitive in the cloud. There is been a rise in research in the field of security in the cloud which shows the concern among users of cloud services. There are several existing protocols to seek data protection in the cloud but since TCP/IP protocol governing network still has its drawbacks there need to be further implementation to give enough confidence among users of the cloud. Security in the cloud is essential in that there is been exponential rise in the usage of cloud services among academia, government and corporate world as well as rise in Cloud service-specific attacks. These are major reason to give attention to security in the cloud. Among some of the challenges with cloud security are believe among CSPs that security is an end user issue. Moreover there is lack of awareness about cloud security coupled with inconsistent network connection issues. To curb this issue, there should

be strong overall security from CSPs by offering a suite of security solution with encryption features. There are several Cloud security programs available offered as a Cloud service in its own. McAfee Cloud Security is one such platform that offers endpoint, email, and web and network protection through the cloud.

2.5 Review of Related Literature

This summarizes prominent reviews on cloud systems provision for computation most especially on storage services. It looks at the security strength and weaknesses associated with cloud infrastructures on remote attestation, resource contention attacks and cache-side channel attacks.

2.5.1 Remote Attestation

Remote attestation is defined as "the procedure of making claims about the security conditions of a targeted system based on the evidence supplied by that system" [72]. It often involves three entities: an attester is the targeted system which provides the evidence; a verifier is an entity which requests an attestation report for a given attester; an appraiser is an entity which makes decisions by evaluating the security conditions based on the attester's evidence. The two types of remote attestation are Binary Attestation and Property-based Attestation.

Binary Attestation was a breakthrough proposed by Trusted Computer Group to cater for attesting the platform integrity of a server. The Binary Attestation has been built on to develop several other remote enabled systems like Integrity Measurement Architecture (IMA), Policy Reduced Integrity Measurement Architecture (PRIMA) for measuring Mandatory Access Control (MAC), Trusted Virtual Machine Monitor and among others. Nonetheless Binary Attestation had its own shortcomings of Privacy Issue around binary measurement sent to verifier to provide configuration and implementation details of the attester leaving a loop hole for fingerprinting attacks. Secondly, the verifier (who is also the appraiser) must be aware of

the correct configurations of the target platform. Lastly with binary attestation, the target platforms may get updated leading to a change in configurations, and thus requiring the verifier to be notified about it each time.

2.5.2 Resource Contention Attack

Resource contention attacks such as Cloud DoS attacks, Cloud Resource Stealing attacks, Hardware resource contention studies and timing channels in clouds are some of the related security breaches associated with cloud infrastructure that is worth studying. DoS attacks for instance have the tendency of depleting or victimizing network bandwidths from its subnet Harkeerat et al(2012). designed a CPU resource attack where an attacker VM can exploit the boost mechanism in the Xen credit scheduler to obtain more CPU resource than paid for. Our attacks do not steal extra cloud resources. Rather, we aim to induce the maximum performance degradation to the co-located victim VM targets.

2.5.3 Cache-Side Channel Attacks

Dirk et al (2002) studied the effect of trace cache evictions on the victim's execution with Hyper-Threading enabled in an Intel Pentium 4 Xeon processor. They also explored frequently flushing shared L2 caches on multicore platforms to slow down a victim program. They studied saturation and locking of buses that connect L1/L2 caches and the main memory. Thomas et al (2007) studied contention attacks on the schedulers of memory controllers. However, due to advances in computer hardware design, caches and DRAMs are larger and their management policies more sophisticated, so these prior attacks may not work in modern cloud settings

2.5.3 Detection and Mitigation of Integrity Attacks

In the space of Integrity attacks detection and mitigation, several studies have been done by researchers. A prominent work by Garfinkel and Rosenblum (95) proposed the method of virtual machine introspection in finding attacks. Several other architectures and tools have been designed to work around virtual machine introspection techniques. Other honey pot tool based on virtual machine introspection to detect and analyse network-based attacks. This leverages the binary translation technique to intercept system calls and collect contextual information as needed. In the future, researchers should pay more attention to enterprise users, data security management and the data source of real business operation in enterprises.

2.6 Summary of Literature

Cloud computing adoption has been on the rise and the rise comes with associated security issues around the technology. Upon the advancement in securing the cloud there still are security threats around remote attestation, resource contention attacks, cache-side channel attacks and detection and mitigation of integrity attacks. This study uses simulation to prove the security threats associated with clouds with no firewall, with firewall and finally firewall with blocking of web and how to mitigate the threats.

CHAPTER THREE

METHODOLOGY

3.0 Overview

The methodology for this research is the design methodology is aimed at conducting a cloud performance evaluation and safety requirements using the RIVERBed Simulation tool. Various

network architectural scenarios were designed to simulate the various network set-ups and test the state of securities.

3.1 No firewall scenario

RIVERBed in general provides an option to design scenarios and in this simulation various scenarios are designed. The primary aim of this scenario is to enforce no firewall conditions across the network. The requisite cloud employed is the IP based cloud. The IP based cloud functions as the internet cloud and connects two or more subnets representing the service providers. The simulation process uses two routers among which one serves as the firewall router. This scenario involves two different applications, the database application and web application. The application configuration and profile configuration level are used in configuring the applications in order to produce the needed application traffic. The simulation makes use of a huge database access application which enforces more database queries over the database server. The needed configurations are executed at the application and profile config level. The performance of the cloud for both the database application and web application is analysed. Figure 3.1 shows the fundamental workspace of RIVERBed.

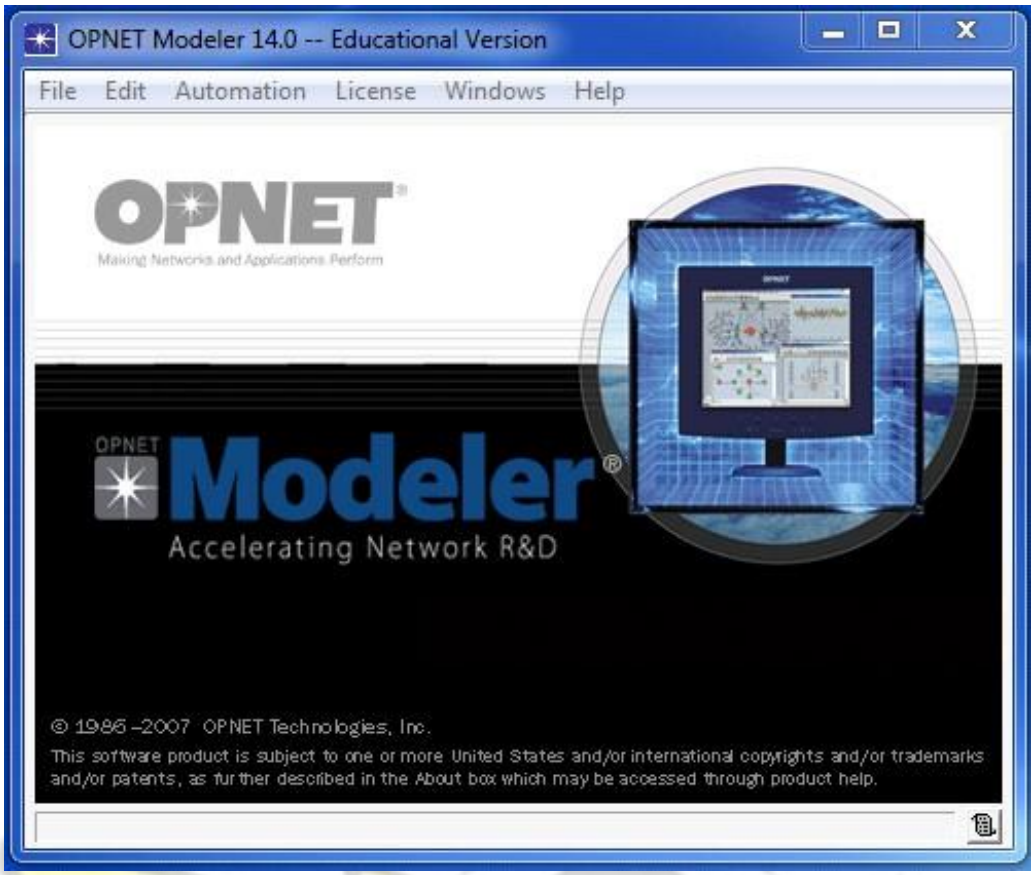


Fig 3.1: Home screen of RIVERBed

The file menu is used in creating a new project with the needed scenarios implemented at this level. Figure 3.2 shows the process.

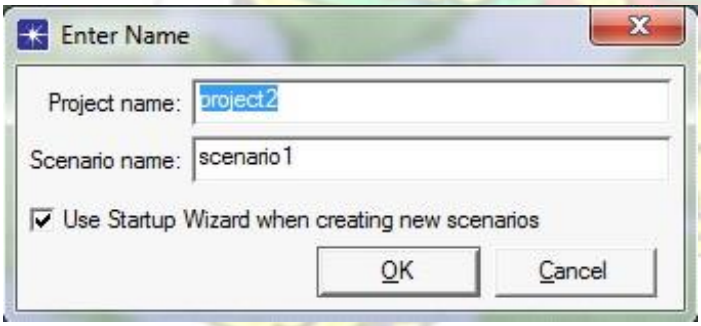


Fig 3.2: Creation of a new project

A number of workstations (150) implemented the cloud used for this simulation with all this workstations accessing the database and the web application. Preceding are the performance metrics used for the performance evaluation of cloud when there is no security across the cloud.

- HTTP page response time is estimated for the web application
- DB query time and response time is estimated for the database application
- Link level and utilization statistics are estimated
- Node level statistics like server DB query response time and load are estimated for the database application

This performance metrics is used for the other scenarios. Description needed is given below.

3.2 Firewall scenario

A firewall scenario is created for a duplicate of the first scenario. In this scenario a firewall router is created. A packet latency of 0.5 seconds is enforced for packet filtering. The same performance metrics used for the first scenario is applied in this scenario.

3.3 Firewall scenario: Block web access

This scenario's primary objective is to block unauthorized web access. It is created by duplicating the second scenario.

After the required three scenarios are made, the simulation is made to run for one hour with the corresponding performance of the cloud evaluated. The result of the simulation is discussed in later section.

3.3 Simulation Procedure

Three scenarios discussed in the former chapter using RIVERBed simulation tool and the simulation run for an hour. The performance of the database and web application under three different scenarios (no firewall, firewall and firewall blocking the web traffic) is the main objective evaluated. This chapter consist of a detailed description of the simulation procedure followed and design metrics.

3.4 RIVERBed as simulation tool

Wide range of models to create the required cloud model is provided by RIVERBed with good user interface. Users are able to use an object palette which contains different node models in the RIVERBed in creating required network model. Figure 3.4 below is a sample screen of object palette that contains the nodes for creating the cloud model.

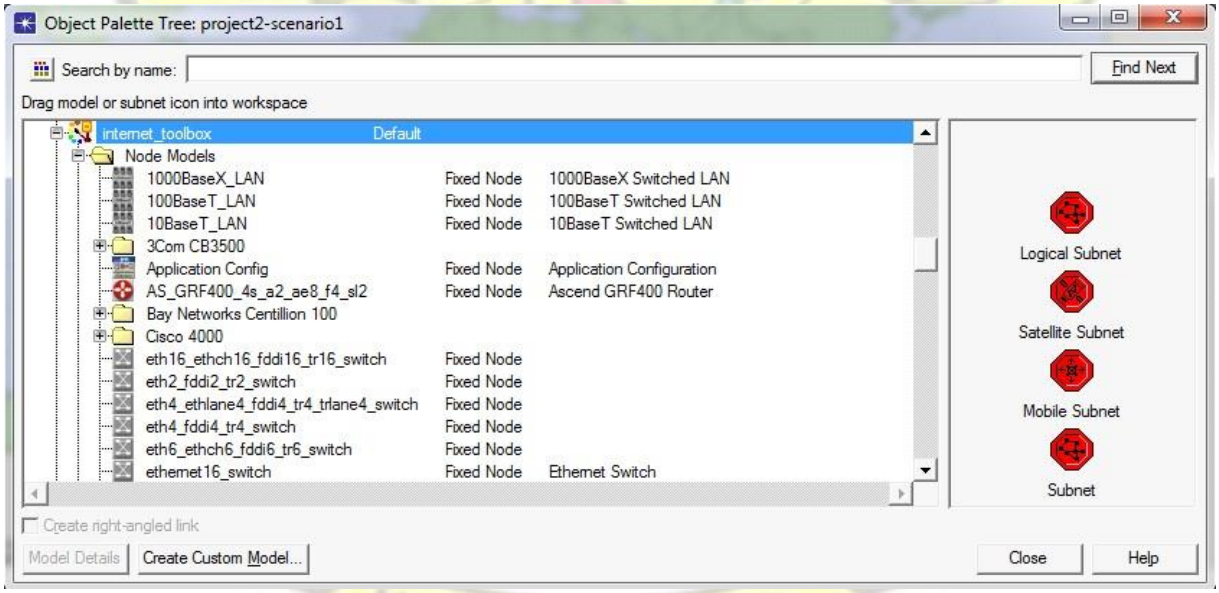


Figure 3.4: RIVERBed object palette

A required network is created by dragging object from object palette to workspace. RIVERBed provides scope for creating different scenarios, comparing scenarios and duplicating as well.

Individual statics at three levels can be used for the performance evaluation of the required network. The simulation tool has the Global level, node level, and link level statics.

Performance comparison can be done choosing desired metrics. An option is provided by RIVERBed to run simulation based on the requirement and the actual result is evaluated when simulation is run. Below are the procedures followed to create the simulation of the scenarios.

3.5 Simulation of No Firewalls scenario

In general a firewall is a network security device (router) that monitors incoming and outgoing network traffic based on a defined set of security rules. In this application a firewall that monitors and regulates the traffic that passes across the network and the internet is used. Home office LAN network is implemented as the destination in this simulation and all other communication achieved via the cloud and other routers. The step needed to create the simulation is given below.

A new project is created on the RIVERBed simulation tool. The name of the project is given as well as it corresponding scenario. In this scenario the project is given as No Firewalls, result is shown in Figure 3.5.

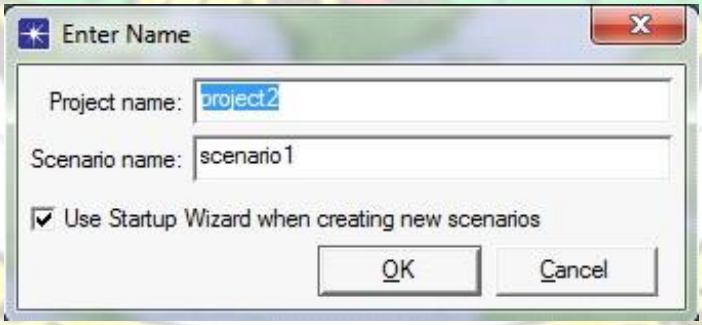


Figure 3.5: New project creation using RIVERBed

Once the name of the project and scenario name are done, the preceding steps are used to create the basic network.

-
-
-
  Create Empty scenario is selected as the initial topology option and next

  Select The world as the required network and then enter next

  US is selected in the maps and enter next

- Click on next twice, the basic workspace with the required object palette are displayed. The figure 3.6 below shows a screenshot of the process.

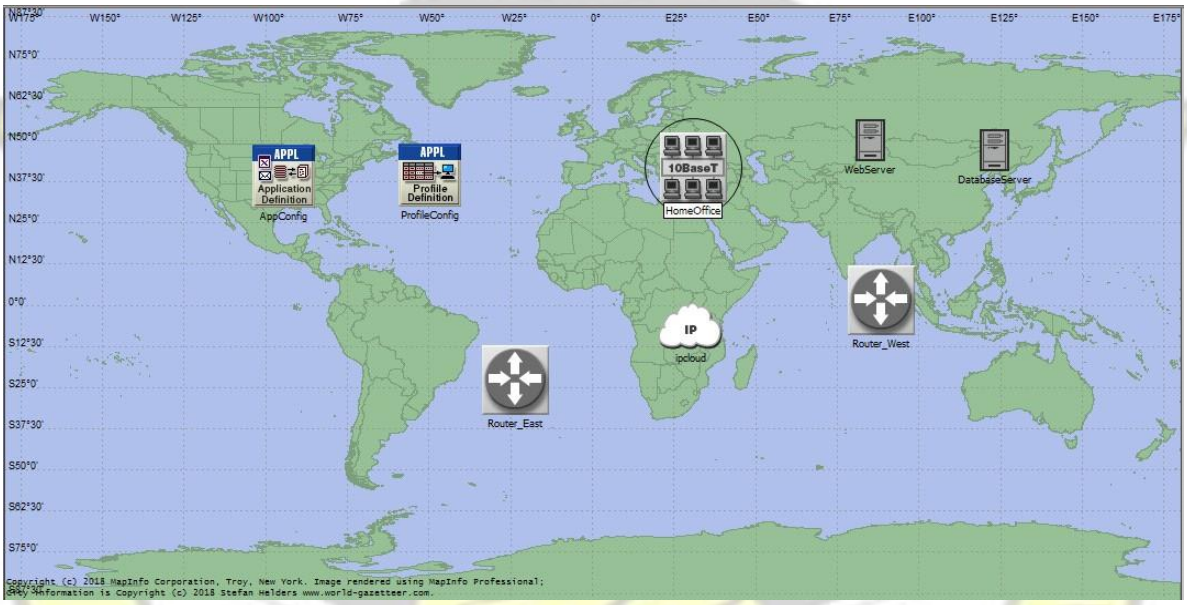


Figure 3.6: The network's basic workspace

After the workspace is set, the following objects are dragged from the object palette to the workspace. The objects used are as listed below:

-
-
-
- The application configuration object is used to define the applications. Database and Http applications are implemented in this simulation. Further detailed descriptions are given in later sections.
- The profile configuration object is used to application profiles
  The internet cloud used is Ip32_cloud object.

  Two ethernet4_slip8_gateways act as the west and east routers

  10BaseT_LAN object act as the home office which supports 150 workstations.
- Two ppp_server object act as the database server and web server

The resulting set up is shown below in Figure 3.7 once all the various objects are dragged to the workspace

-
-
-

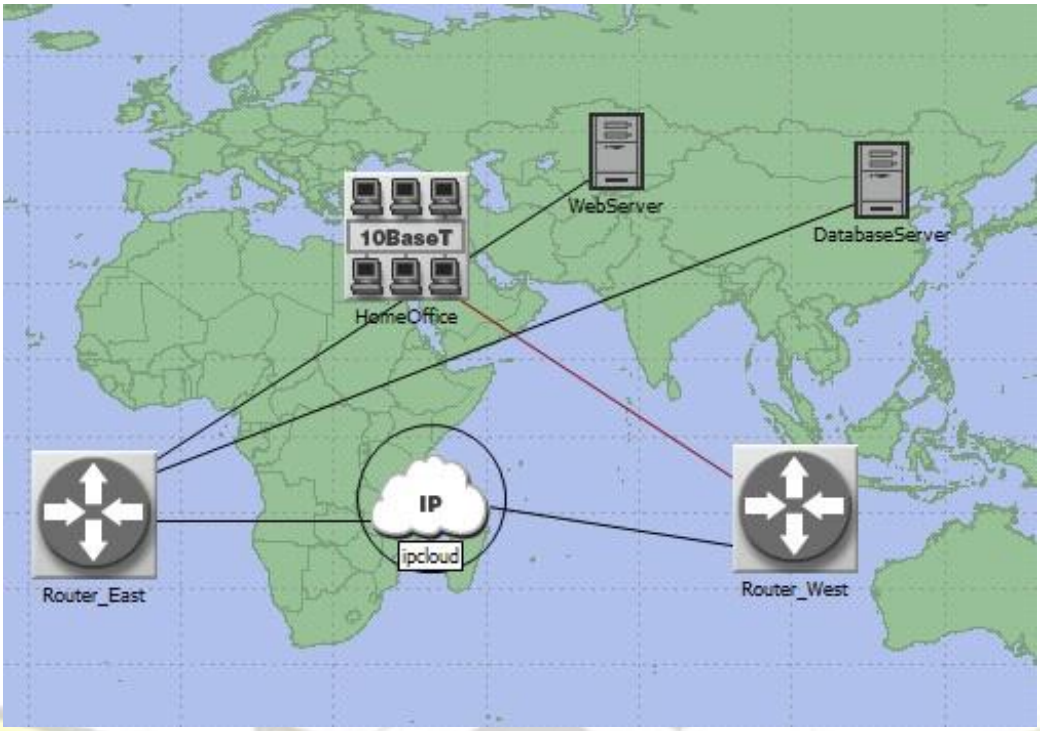


Figure 3.7 Setup of Basic Network

3.5.1 Application configuration settings

Two applications are created in this project in order or to generate the needed traffic over the cloud. RIVERBed provides object known application config. The needed application can be created at level. To add the applications, the application configuration object is dragged from the object palette and edited. Below are the corresponding steps:

Right click on the Application config object and select edit attributes

Add two row to the applications definitions tab, to create two applications

Rename a row as database; select the heavy load database against the Database application.

•

•

•

• Rename another row as web; select heavy browsing against HTTP application. Below in Figure 3.8 is a screenshot of the result.

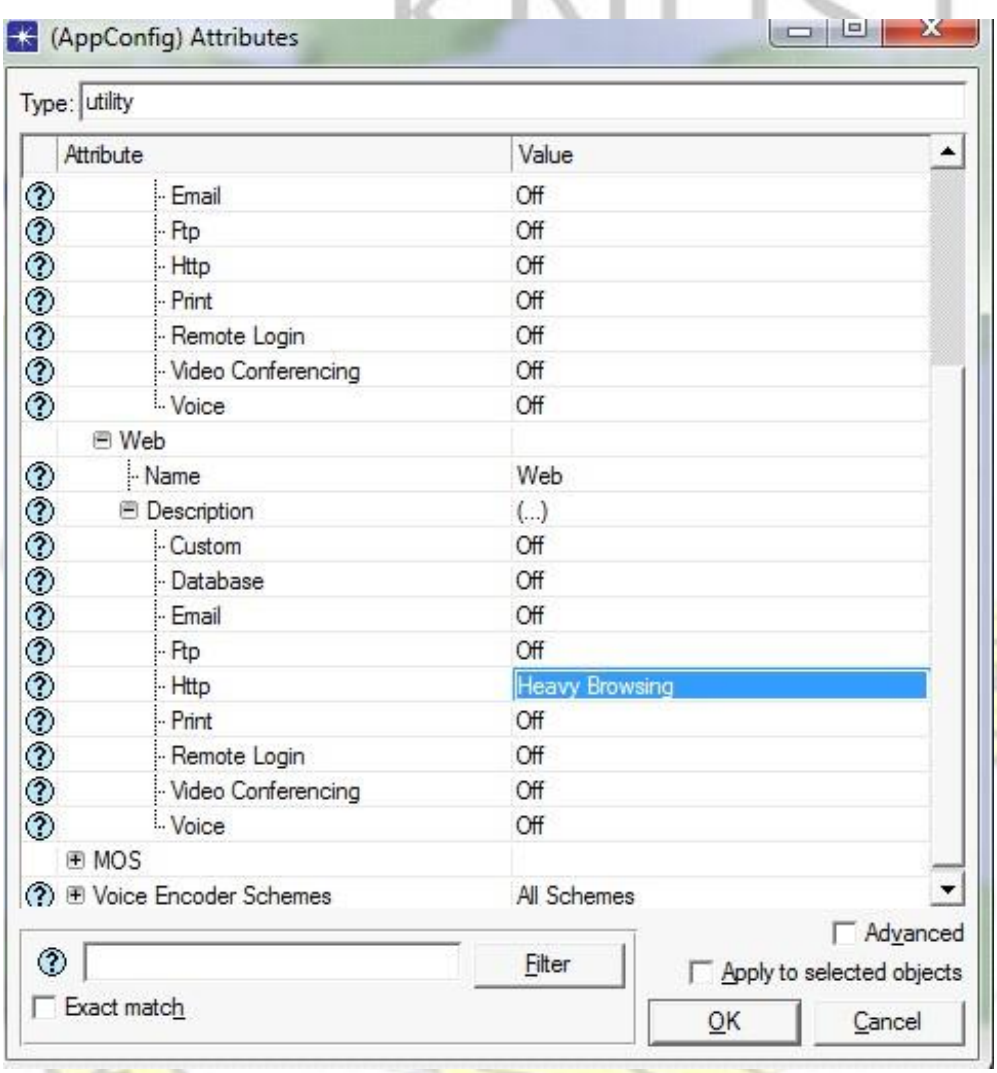


Figure 3.8: Settings of the Application configuration

Select OK and save project after application definitions are set. Next define the profiles of the applications.

3.5.2 Settings of profile configuration

The requisite application traffic over the network is generated for each application using it profile. A profile configuration object is provided by RIVERBed which can be gotten from the object palette by dragging. The profile definitions setting steps are given below:

- The profile configuration object is right clicked and edit attributes selected
- Two rows are added for profile.
- A row is named as Database_User; choose the database as the application.
- Another row as Web_User is named; the required application selected is Web. Below in Figure 3.9 and 3.10 is a screenshot of the result.

.

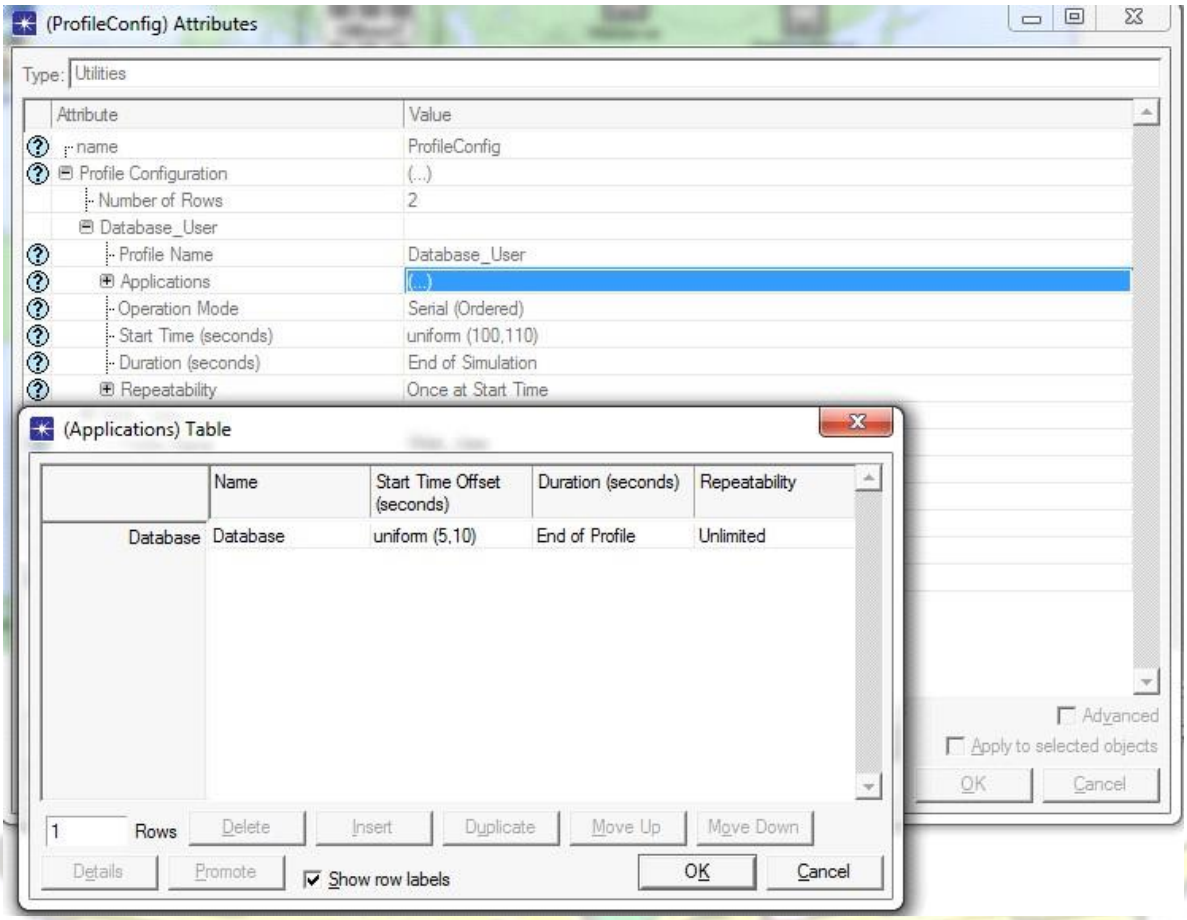


Figure 3.9: Profile Configuration of Database

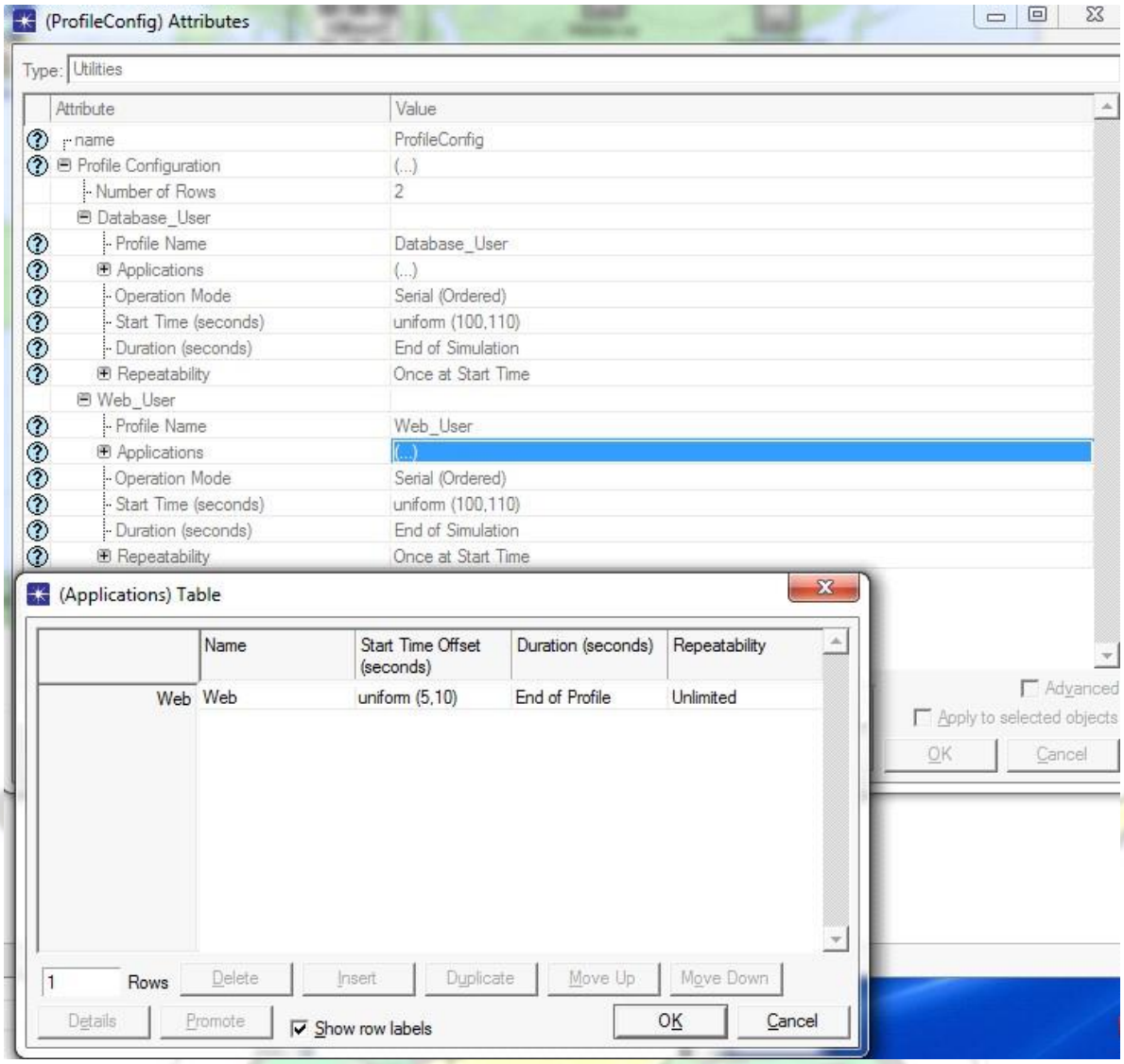


Figure 3.10: Profile Configuration of Web

The applications are set to generate the traffic after creating the respective profiles. The cloud is configured next.

3.5.3 Cloud configuration

A simple public internet based cloud is represented using IP32 cloud provided by the RIVERBed. The database and web applications are supported in this project using this cloud. IP32 _cloud object is drag to the workspace and it attributes edited. The steps are given below

- The cloud is right clicked and it attributes is edited

- The packet latency attribute is edited by setting a constant 0.05 seconds value. The Figure 3.11 shows a screenshot of it.

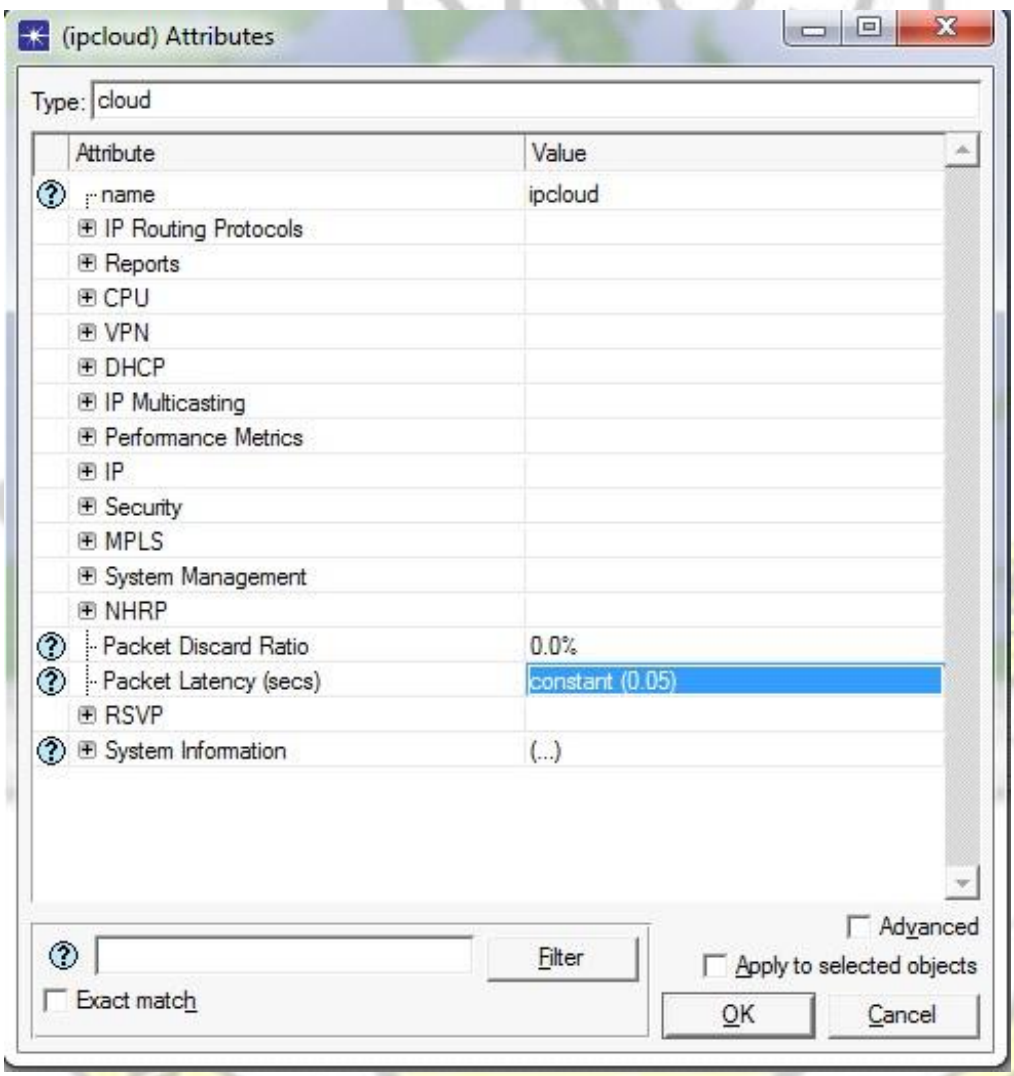


Figure 3.11: IP32 cloud configuration

The maximum packet delay across the cloud due to the web and database application is 50ms, when the packet latency is set to 0.05seconds. Every packet accross the cloud is processed with it limited delay. Next the west router attributes is edited.

3.5.4 West router and East router configuration

As stated earlier two routers are used in this simulation (West and East Routers). West router configuration is worked on in this section. Select an Ethernet4_slip8_gtwy object from object palette renaming it as Router_West. Another Ethernet4_slip8_gtwy object is selected to the workspace and renamed as Router_East. The IP32 cloud using PPP_SI links in the object palette are used in connecting both routers. Figure 3.12 below is the resulting connection.

Figure 3.12: Configuration of East and West router

3.5.5 Configuration of Home office

A 10BaseT_LAN object is selected from the object palette and configured as follows:

- The object is right clicked and the attributes edited.
- The number of workstations is set to 150
- Two rows are added by expanding application supported profiles
- 50 is set as the number of users and a database profile is included.

Web profile is set as the next profile and 100 setted as the number of users. Below (Figure 3.13) shows the result

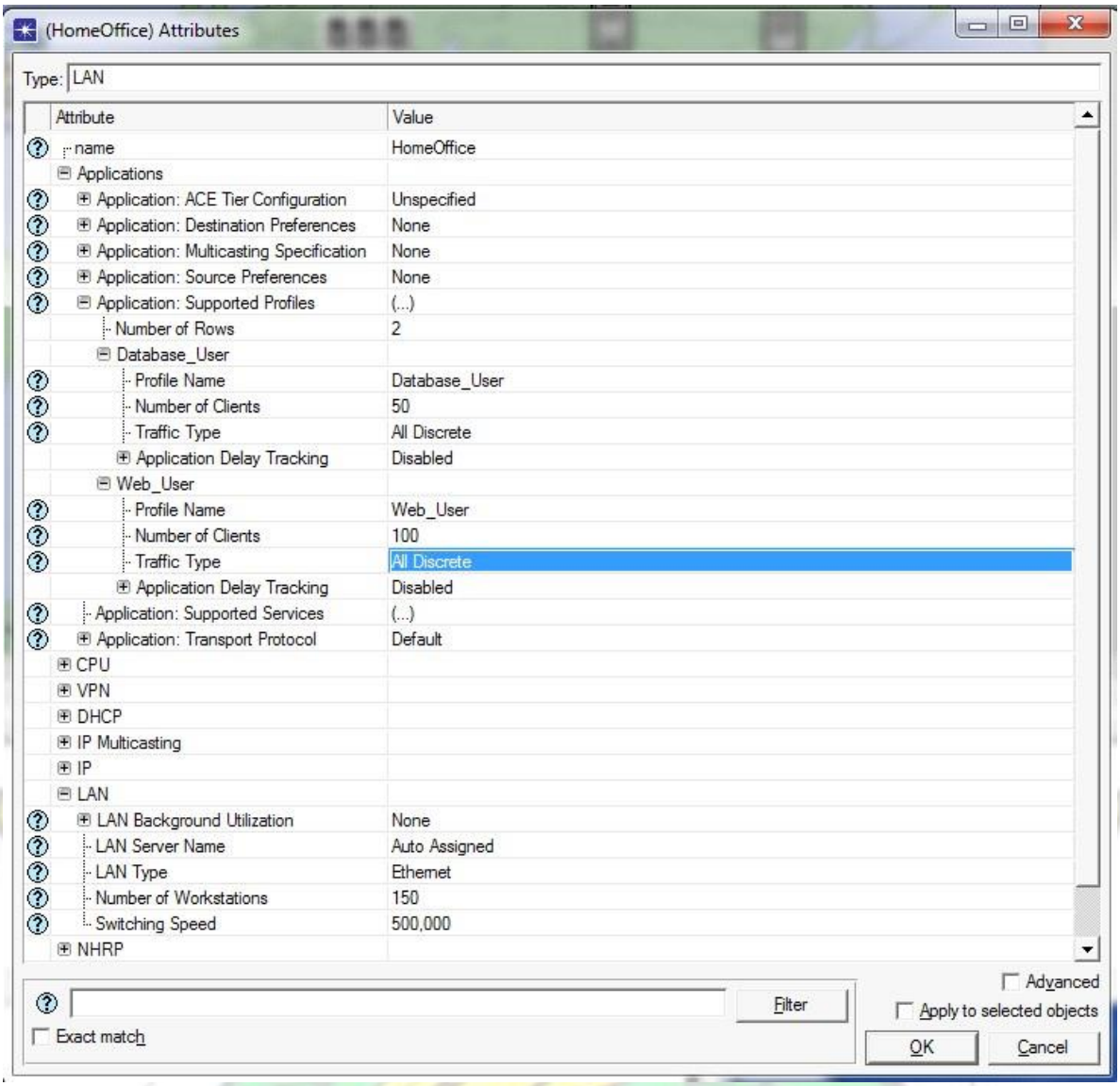


Figure 3.13: Configuration of Home Office

The Router_West is then by the home office using the 10BaseT links. Figure 3.14 below shows the result.

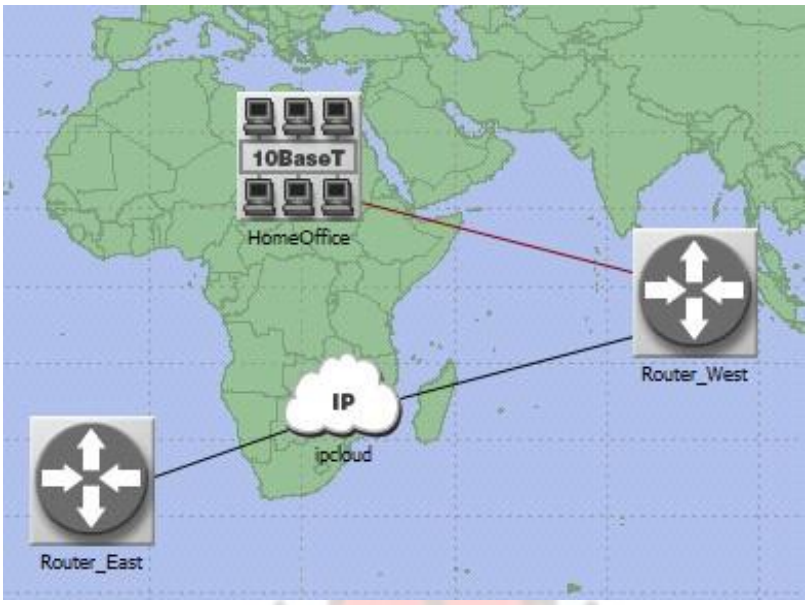


Figure 3.14: Home office connection to Router west

3.5.6 Server configurations

A database server and web server are represented by Two PPS servers. The applications are supported editing the servers from the object palette. Below are the steps;

- The database server is right clicked and it attributes edited.
- The profiles that support the application is edited and set database application as support.
- The web server configuration uses the same procedure. At this level the web application is supported. Figure 3.15 and 3.16 shows a screenshot of the configurations

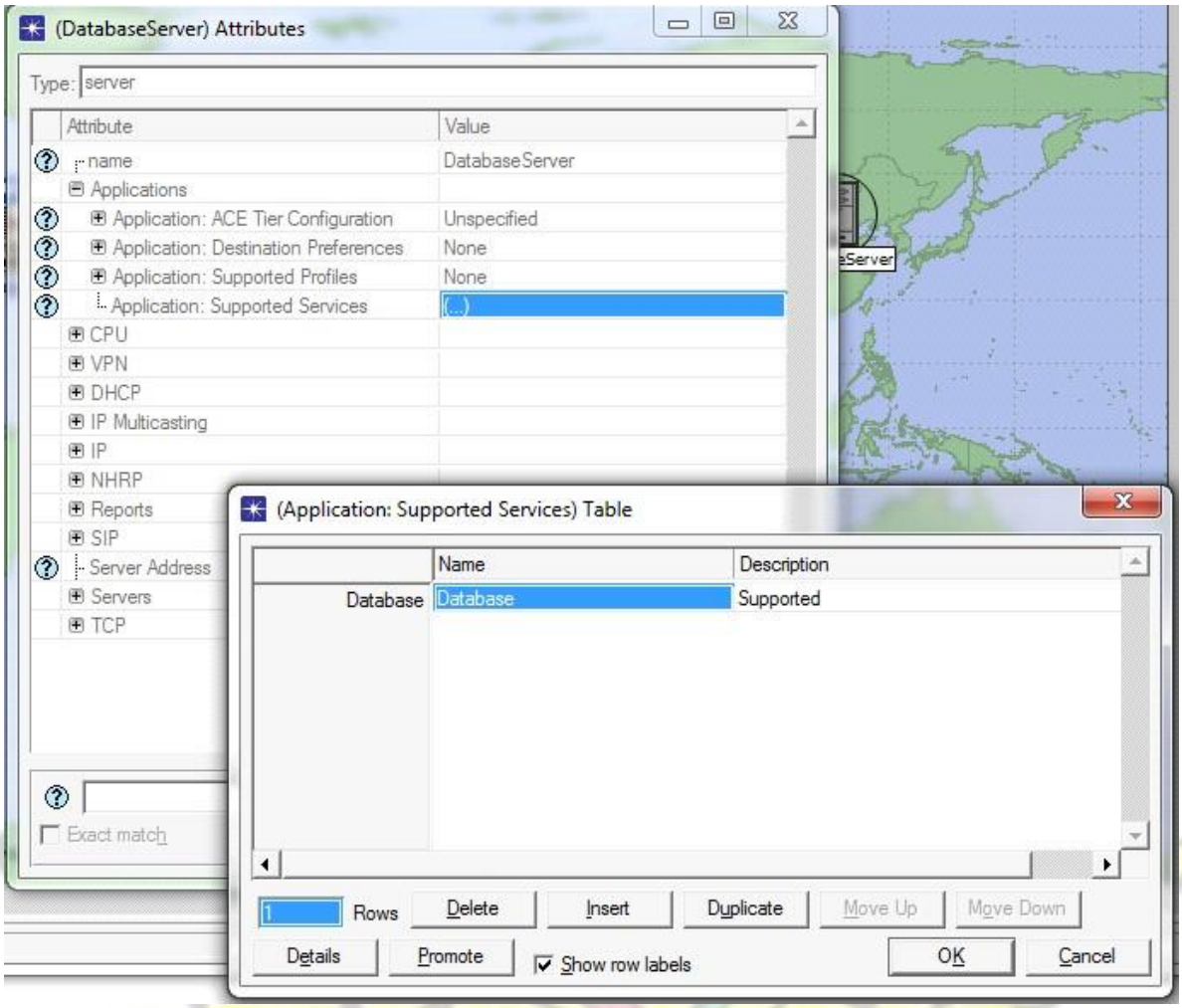


Figure 3.15: Configuration of Database server

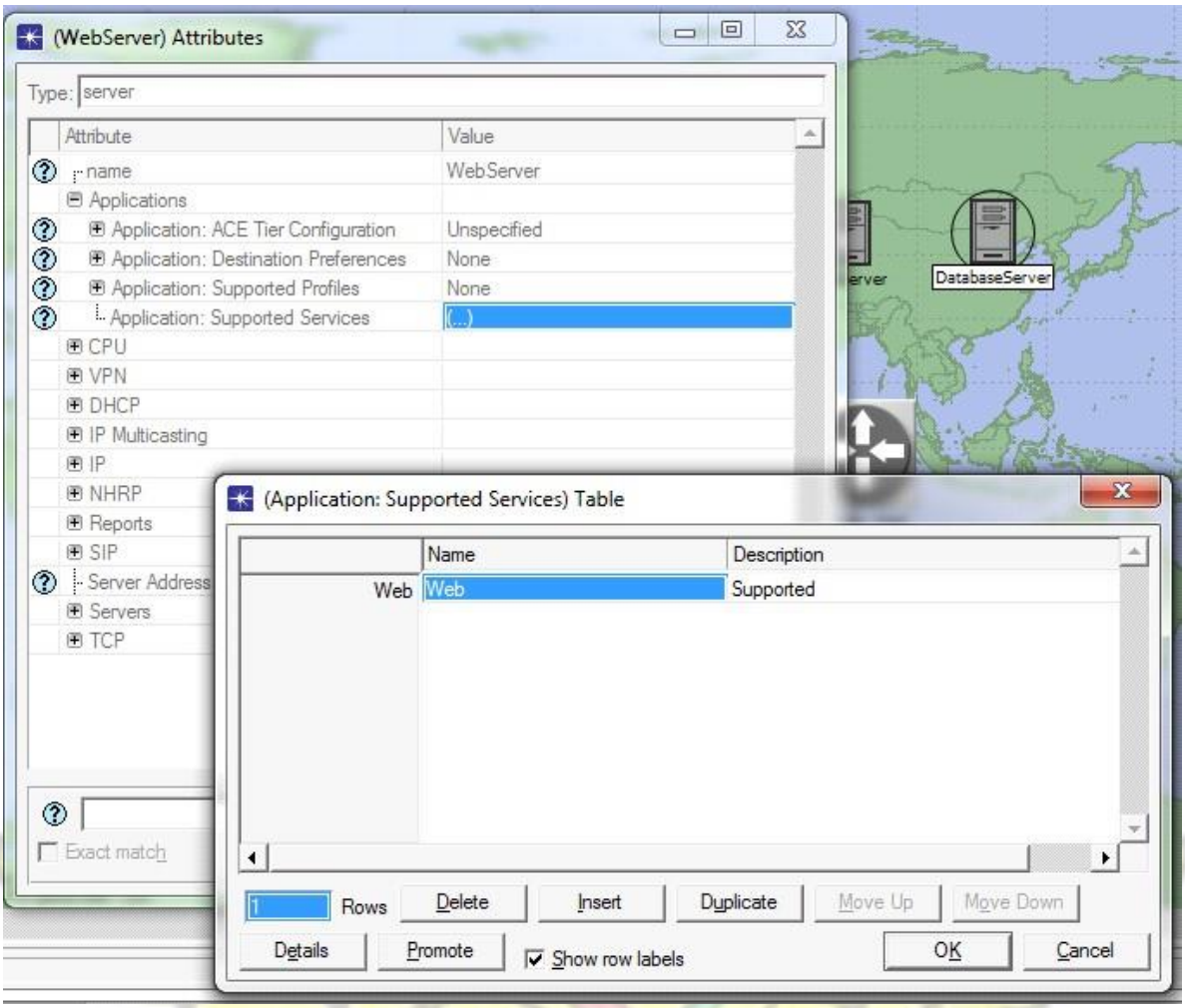


Figure 3.16: Configuration of Web server

The PPP_DSI links are used to connect the Router East to the server after configuring the server. Figure 3.17 shows a screenshot of the configuration

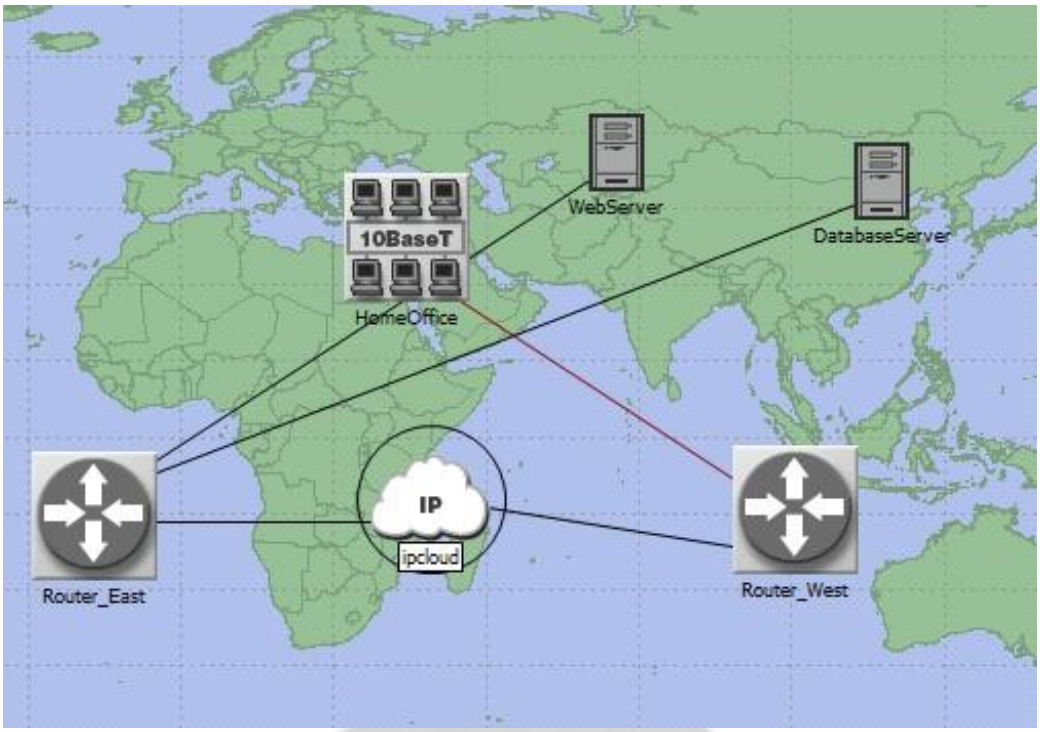


Figure 3.17: Router East connection to servers

3.5.7 Performance metrics

Previous sections included elaboration of the required configuration with a setup of complete network along with it configurations. Few arguments are needed to test the performance of cloud against the database and web applications. Global level, node level and link level are three levels of performance evaluation provided by RIVERBed. Performance metrics are set in the steps below:

- The workspace is right clicked; choose individual statistics from the option.
- Global, node and link level metrics are given in a new window that appears with the options to select any**.** Figure 3.18 shows corresponding steps.

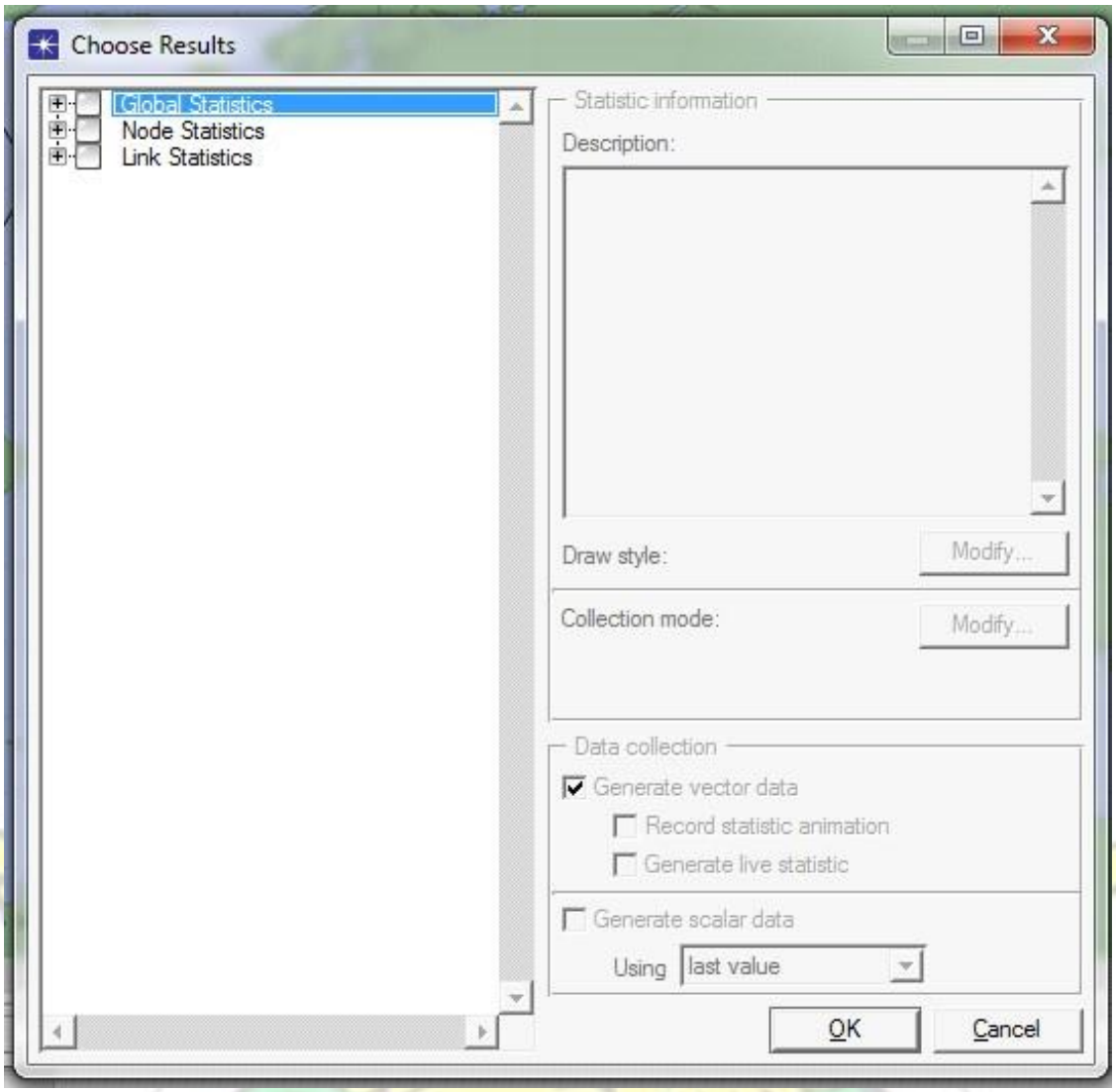


Figure 3.18: Three levels of performance metrics

For performance evaluation the following metrics are chosen:

- Expand the DB query from the global level statistics, the response time is selected
- Expand the Http option from the global level statistics; s page response time is selected.

Figure 3.19 below shows the process above.

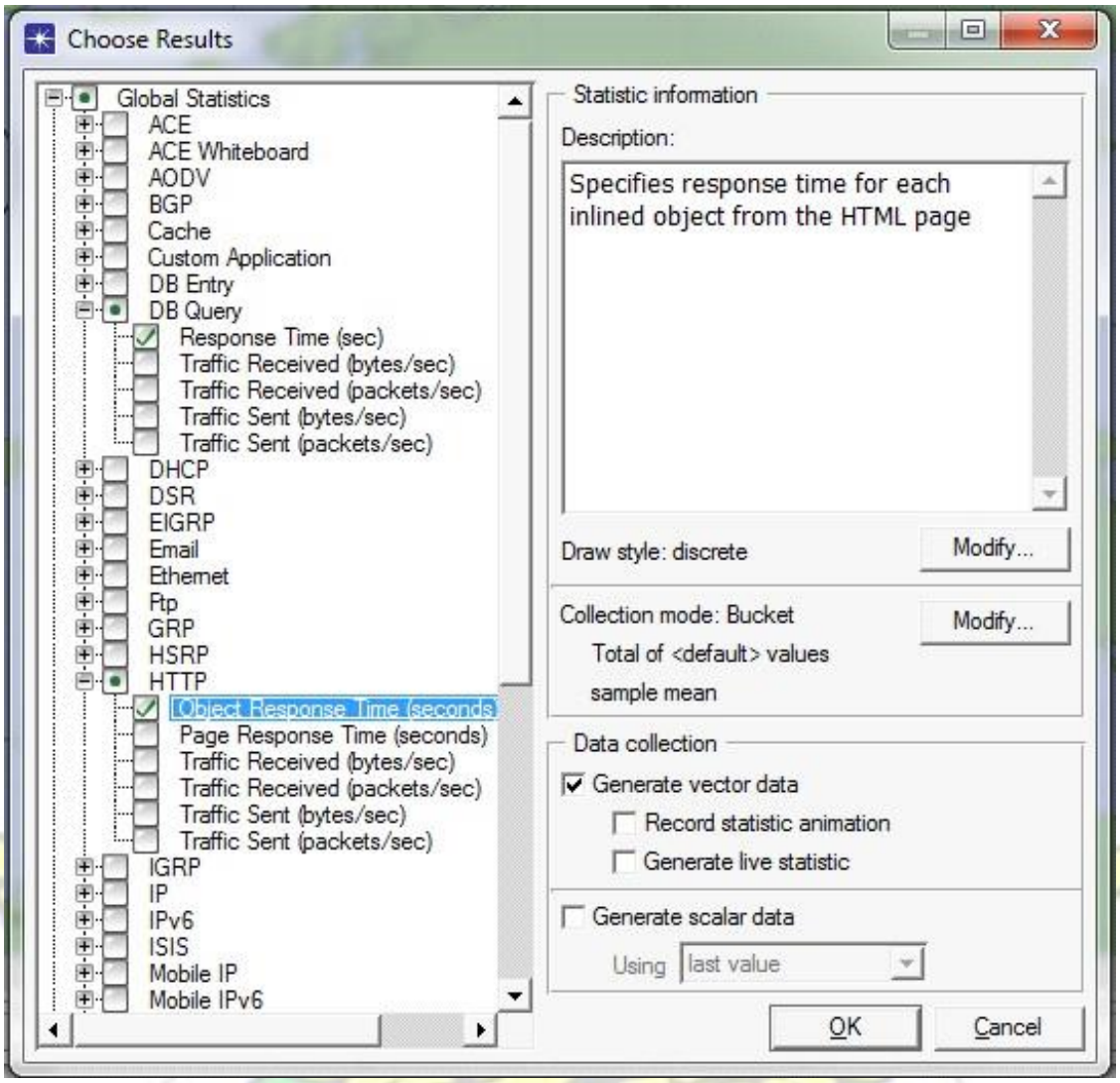


Figure 3.19: Global statistics

The following are selected for the node level statistics:

- DB query is expanded and load is selected
- Server HTTP is expanded, select load.S Figure 3.20 below shows the process above

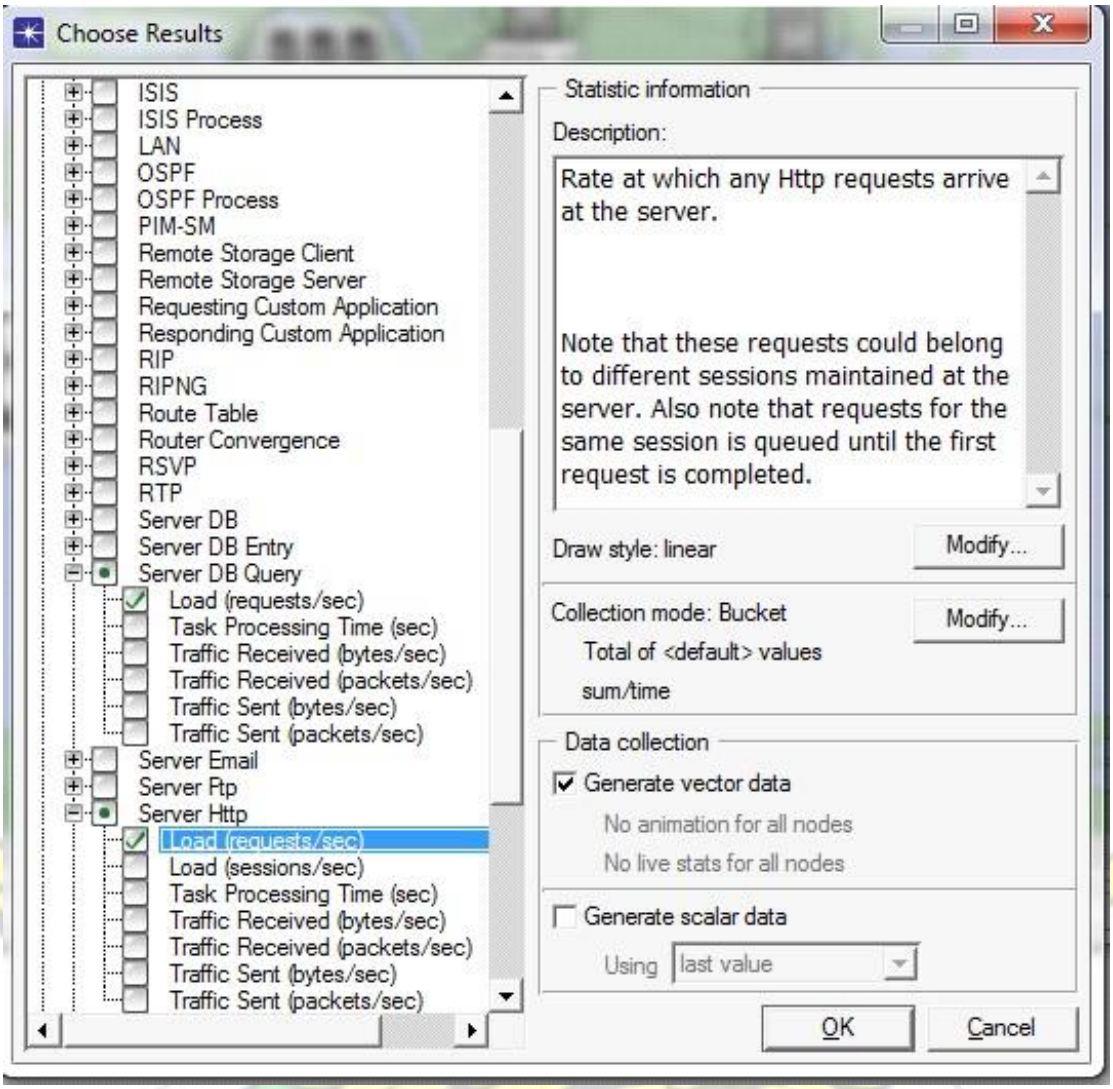


Figure 3.20: Statistics of Node level

The statistics of the link level are achieved from selecting the following:

Point to point option is expanded; both the utilization metrics are checked. Figure 3.21 shows the link level statistics

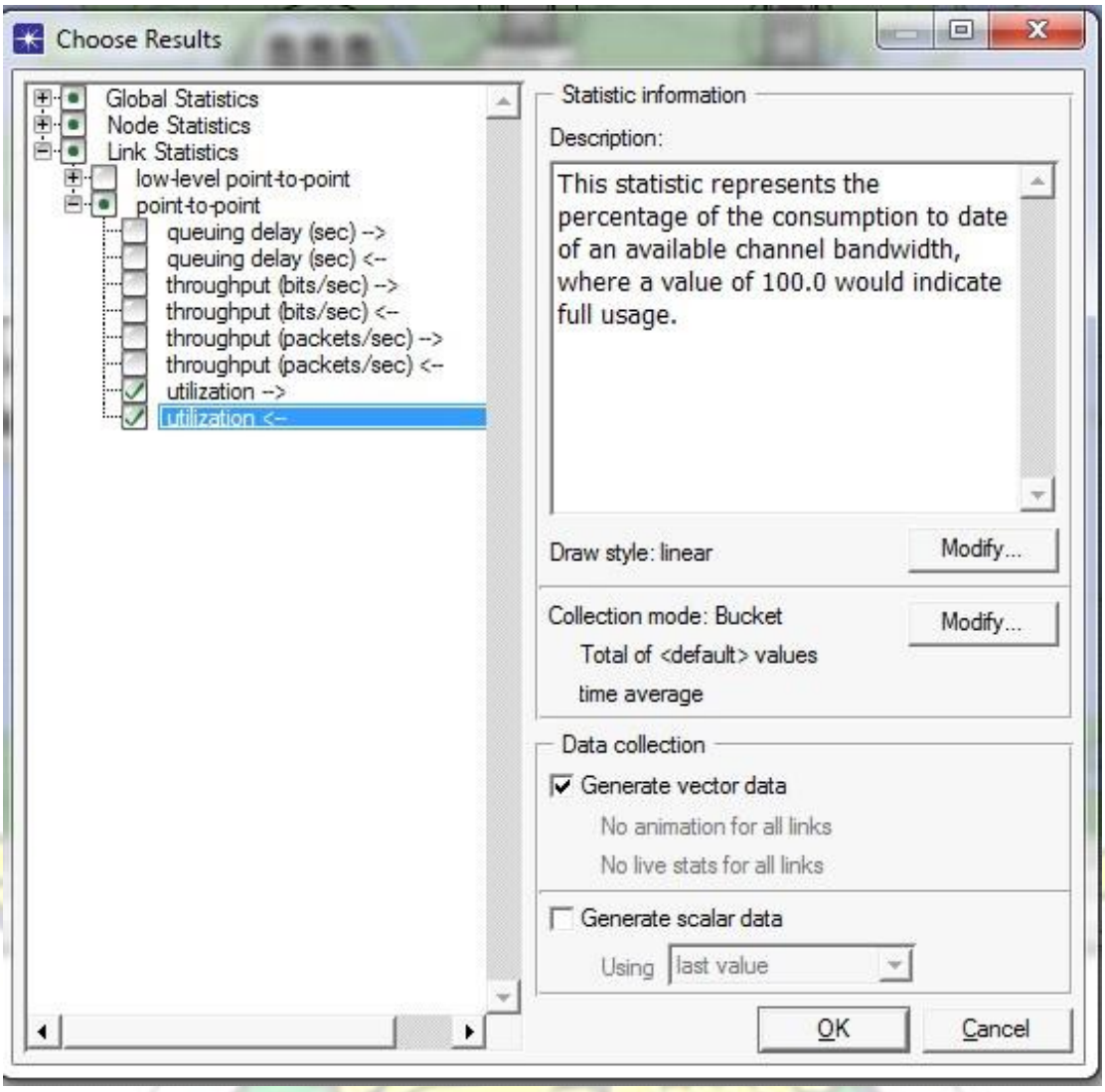


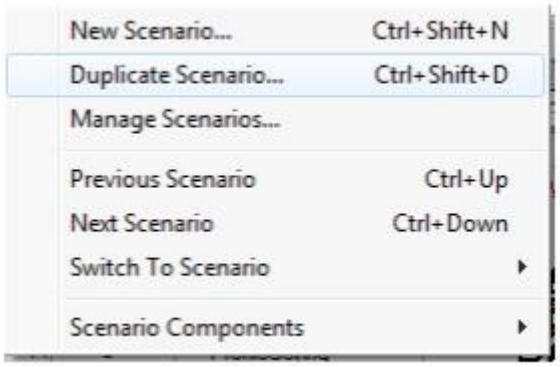
Figure 3.21: Statistics of Link level

When all the needed performance metrics is selected, the first scenario simulation is complete.

For the other scenarios similar performance metrics are implemented

3.6 Firewall scenario

In creating this scenario, the first scenario is duplicated. Enforcing the firewall policies over the cloud is the primary objective of this scenario. In this scenario the firewall permits packet filtering and the required traffic across the network. From the scenario menu the option to duplicate scenario is selected. Figure 3.22 below shows the duplicate process.



.

Figure 3.22: Procedure to duplicate the scenario

After duplication the steps below are followed to create the firewall scenario needed.

- Router West is right clicked and attributes edited.
- Select ethernet2_slip_firewall from the option model. The firewall here are the routers.
- The proxy server option is expanded and row 1 option edited to have a latency of value 0.05 at a constant rate.
- Row 4 is expanded and the latency set to a constant value of 0.05. Below (figure 3.23) shows the process above:

:

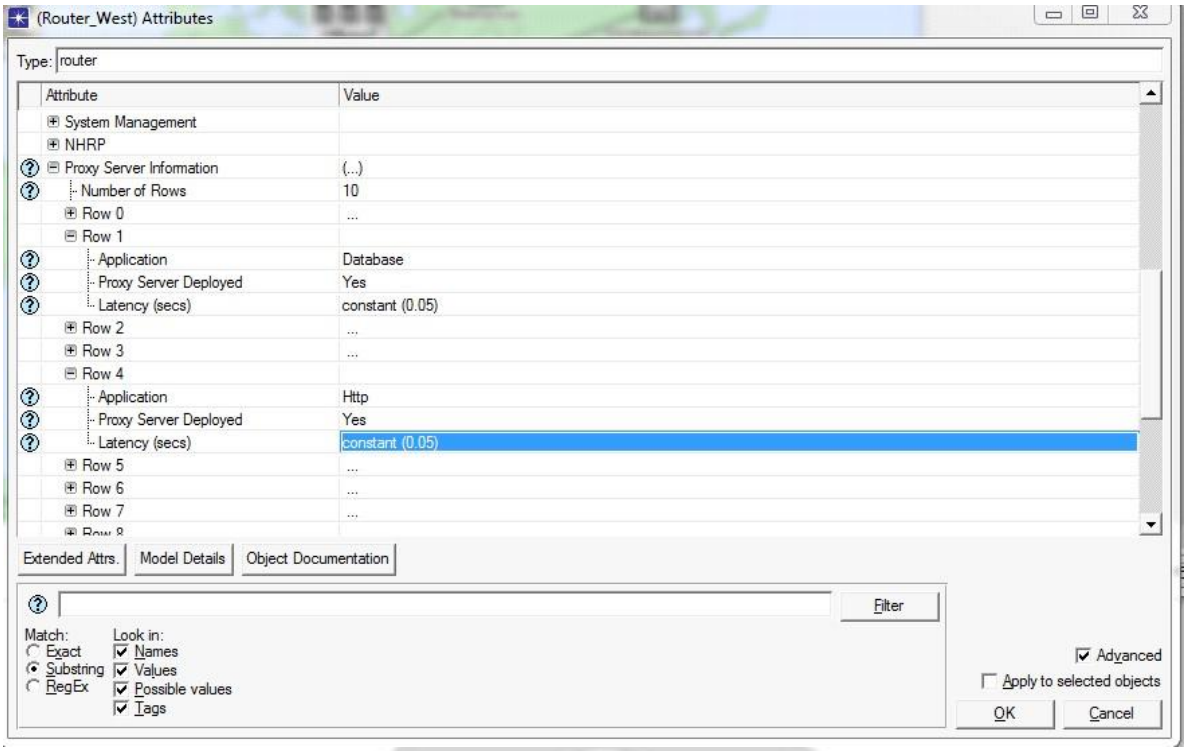


Figure 3.23: Firewall configuration

Value 0.05 latency is set as the constant for the web application and database. At the firewall a packet filtering is done with 50ms delay obtained over the router. Below is figure 3.24 showing the network after following the requisite firewall configuration steps.

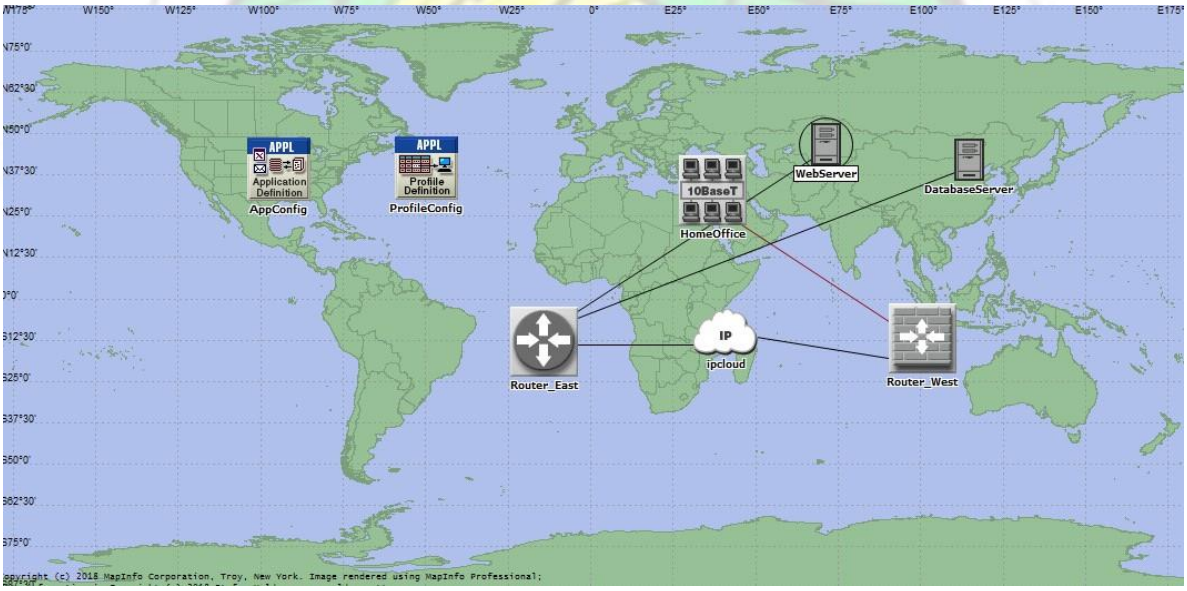


Figure 3.24: Firewall scenario setup

The similar performance metrics for the first scenario is used as well in this scenario

3.7 Firewall blocking scenario

Blocking the web traffic over the network is the primary goal in this scenario. Duplicating the second scenario is way to obtain this scenario. Below are the changes done:

- the router west is right clicked and the attributes edited
- The proxy server information is expanded, the row 4 (HTTP) is selected.
- The deployed proxy server option is set to no. below is Figure 3.25 showing the process

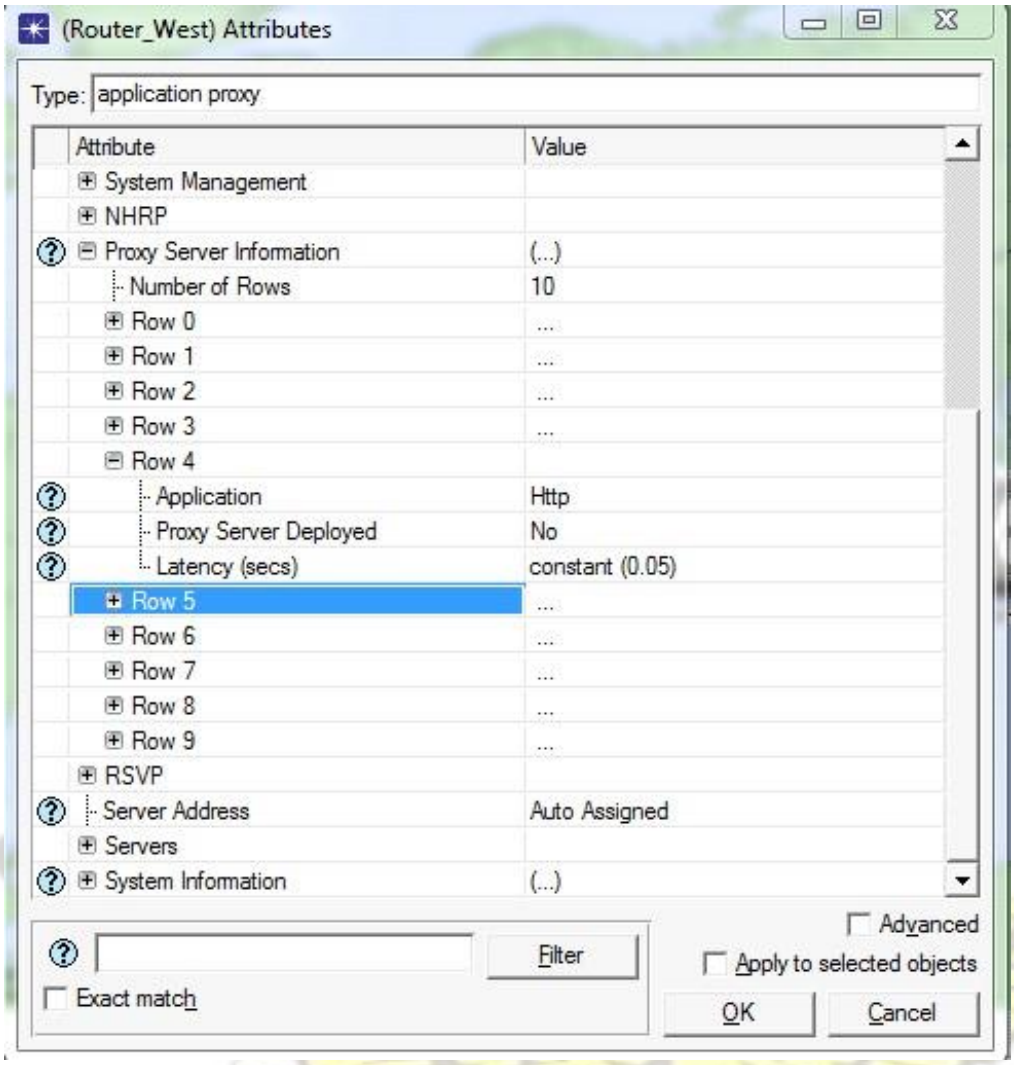


Figure 3.25 Blocking Web traffic

The web traffic across the cloud is blocked, firewall blocking scenario is complete in this simulation.

.3.8 Running the simulation

The simulation is run for an hour when the scenarios are all done. The manage scenarios option is selected from the menu to run simulation, the process is shown in Figure 3.26 below.

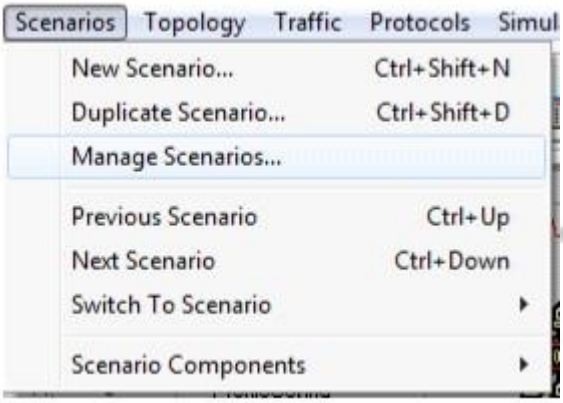


Figure 3.26: Manage scenarios

A new window appears after selection, the simulation is run for an hour. Figure 3.27 below shows the process

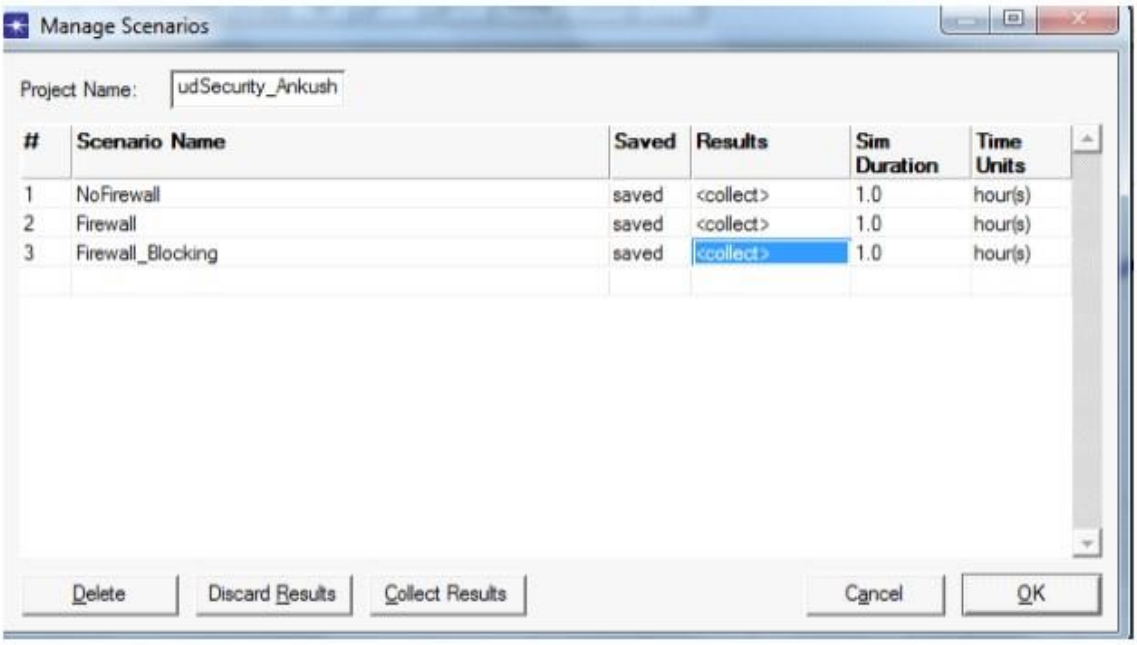


Figure 3.27: Running simulation for an hour

After completing simulation evaluate the results. The three scenarios are compared to the performance metrics selected. In the preceding chapter a detailed evaluation of results is used

CHAPTER FOUR

4.0 Results and Evaluation

Evaluating the results after simulation has run for an hour as elaborated in previous chapter is discussed in this chapter. In this simulation three scenarios are created as explained in the previous chapters; scenario with no firewall, another with firewall for filtering database and web application packets and last is the blocking of the web traffic across the cloud. At the three levels (global level, node level and link level) the performance metrics selected is used to evaluate the performance for the database and web application. Below is a detailed evaluation of the results.

4.1 Database Application Results

The database application performance evaluation is based on the scenarios described in the chapter above. First no firewall second has firewall to filter the database application packets, and the third completely blocks access to the web. The graphs given below shows the database performance against the scenarios.

.

4.2. Query response time of Database

The query response time determines the overall performance of the database application. The response time is very less if there are no security rules set across the network of the application. The resulting process is shown in Figure 4.1 below

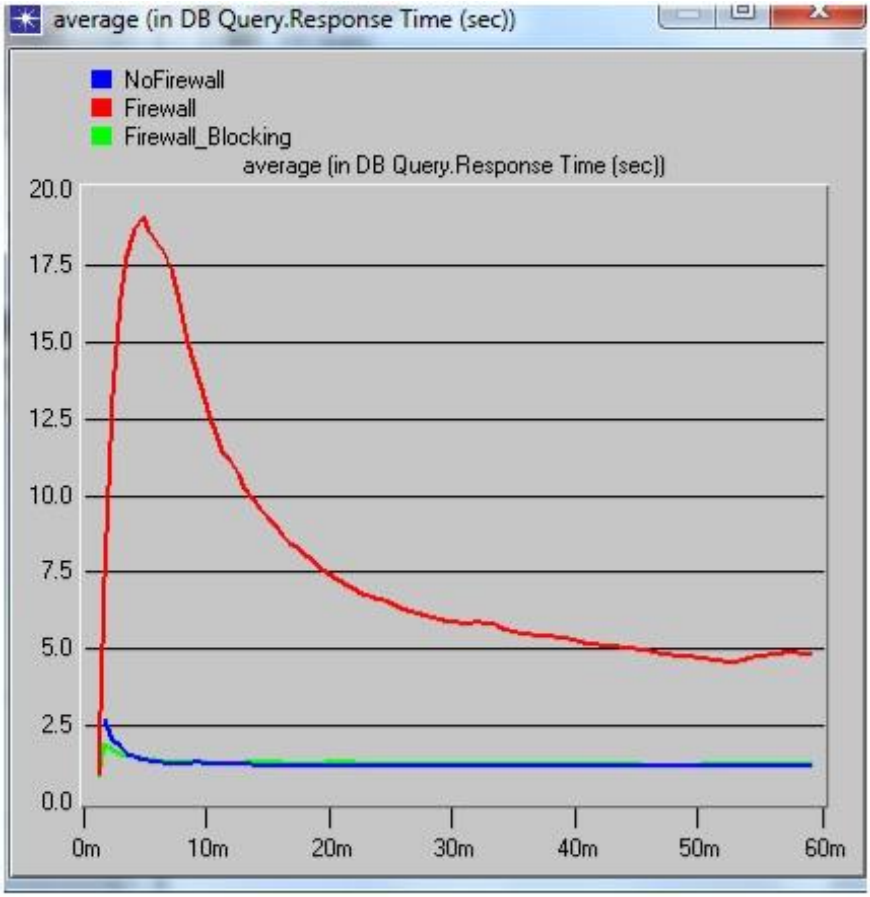


Figure 4.1: Response time

It can be deduced from above graph that the query response time is higher with the presence of firewall. The delay in response time is due to the initial packet filtering, it could be seen from the graph that the response time reduced after 10 minutes of simulation. With the no firewall scenario, the response time is less as compared to the scenario with firewall. With absence of packet delay at the west router, there is fast response time with good application performance.

The response time for the web application is less. Blocking the web traffic by firewall enhances the database application performance due to less load on the firewall. In the conclusion of the analysis, it can be deduced that, there is enhanced performance of the database application and security when the unwanted web traffic is blocked.

.

4.2.2 Query load of Server DB

The database server total load for the three scenarios is estimated in the figure 4.2 below

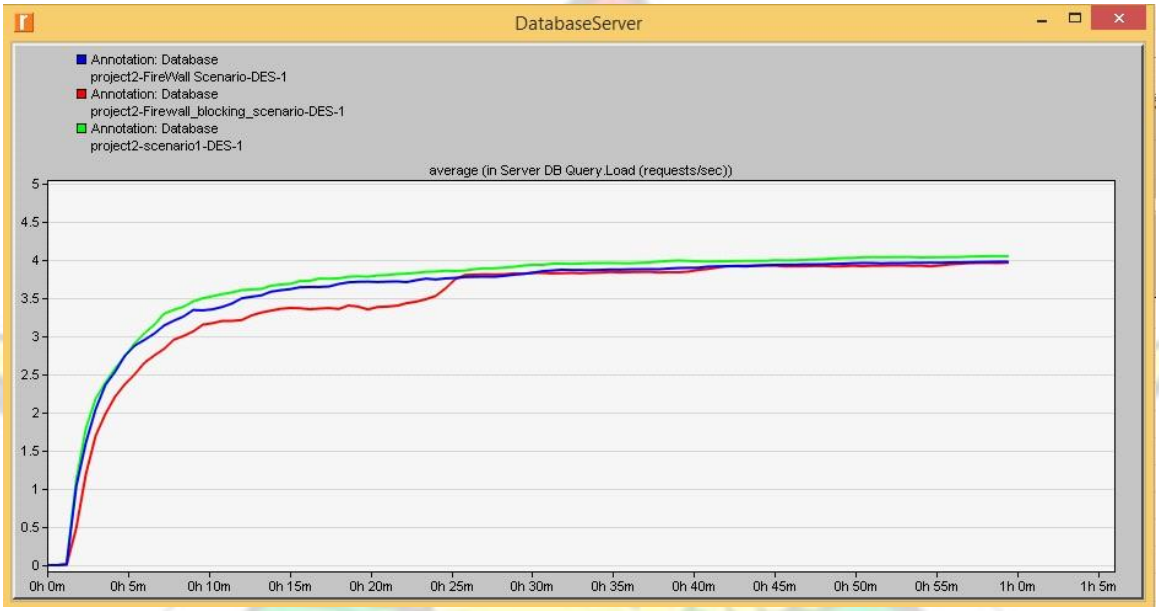


Figure 4.2 Database server Load

From the above graph there is less load when there is no firewall as compared to the other scenarios. For all the three scenarios the load on the database server is almost the same with the exception of the adding a firewall. The load in the case of the firewall could be some packet delay as they are filtered. The implementation of a firewall over the network increases the load on the database server

4.2.3 Database Server point to point utilization

The application performance against the key security issues indicates the utilization of the database server across the router. Figure 4.3 shows a comparison graph of the three scenarios.

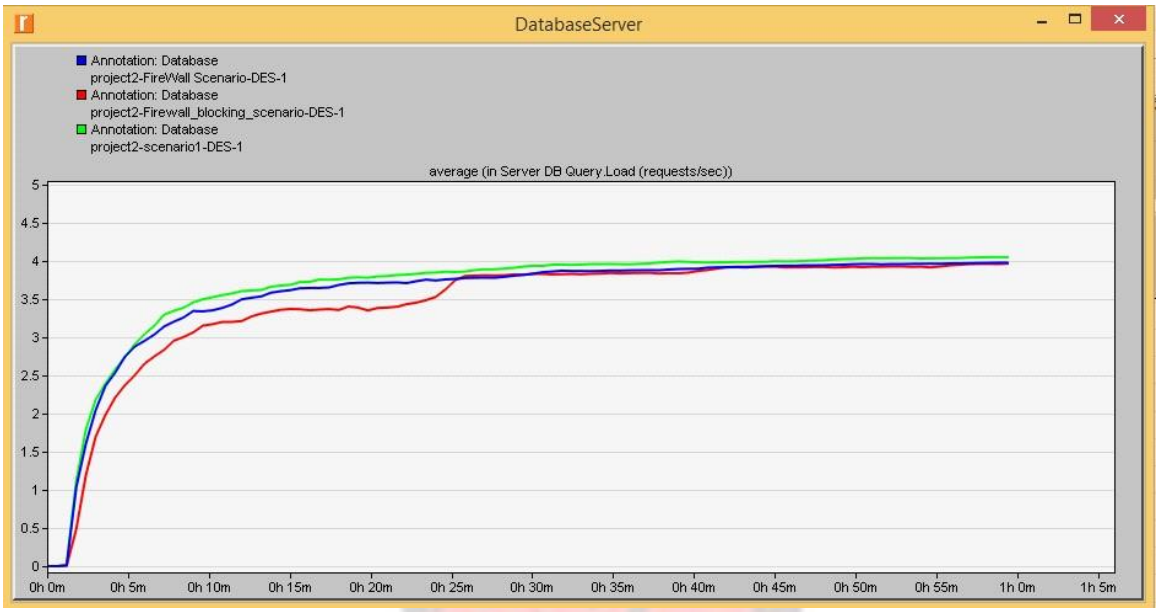


Figure 4.3: Database server across router

It can be deduced from the graph that the average utilization of the database server is more when there is firewall across the cloud. The point to point utilization can be observed to be less where there is no firewall. Also when there is no filtering of packet or firewall rules the utilization of the server is reduced. With the blocked web traffic it is observed to have an increased utilization of server. We can conclude that the point to point utilization of the database server is increased when no firewall is implemented across the cloud.

4.3 Results for web application

Web application performance is estimated against the page response time. Only the first two scenarios are evaluated while the web application in the third scenario is blocked, given below is the evaluation

4.3.1 No firewall scenario Page response time

Page response time result of the web application implementing no firewall is given in figure 4.4 below.

.

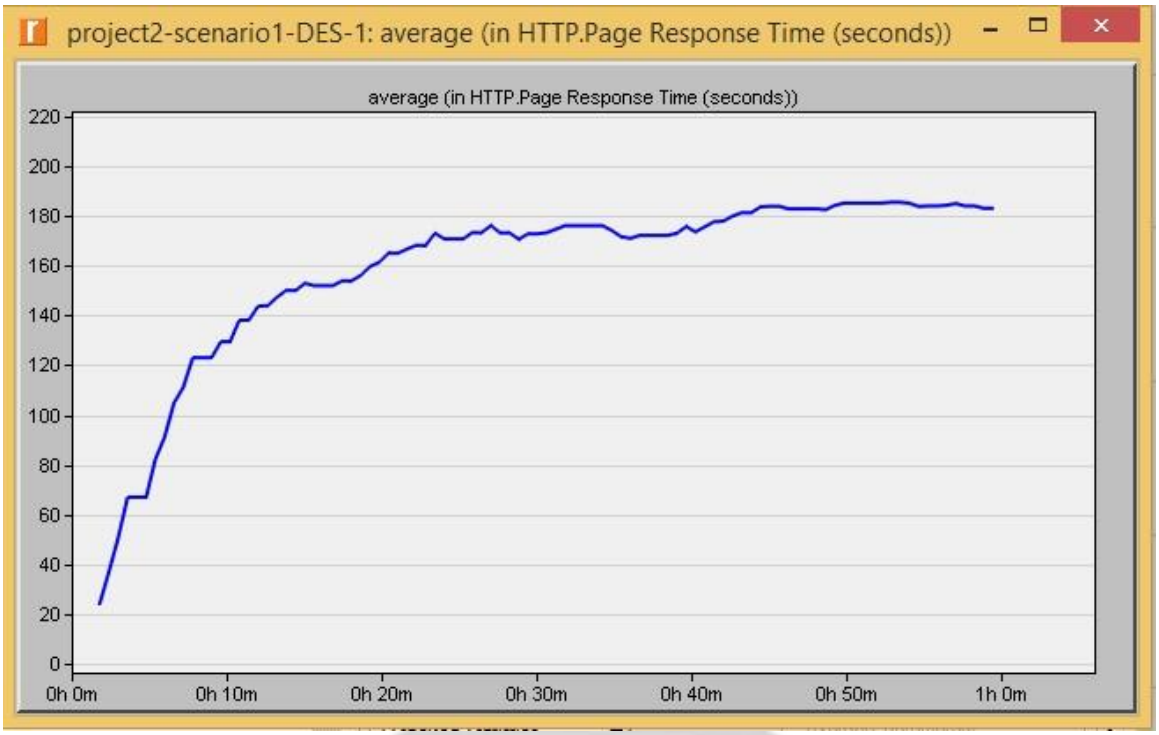


Figure 4.4: Response time across no firewall

From the graph above it can be deduced that with no firewall results there is constant general page response time, which shows a constant flow of the web application across the cloud.

.

4.3.2 Page response time across firewall scenarios

The figure 4.5 below show the page response time when there is firewall.

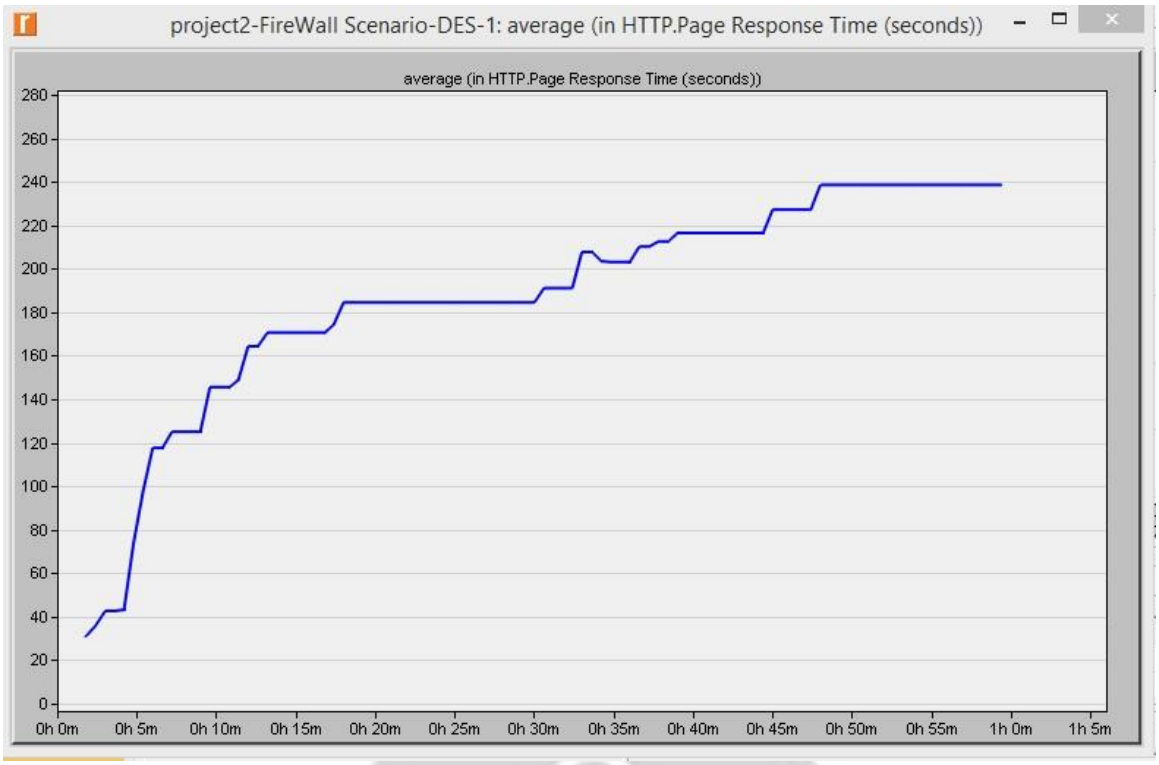


Figure 4.5: Response time across firewall

It is realized from the graph that the average maximum page response time across the web application is higher (240 seconds) as compared to the previous (180 seconds) scenario. It is also observed from the graph that the response time is varying due to packet latency against the packet filtering process.

It can be concluded from the values of the resulting graphs that firewall policies and the packet latency enforced over the firewall result in an increased response time. Hence blocking the web traffic increases the page response time.

4.4 Cloud performance

The complete performance of the cloud under the three scenarios is elaborated below

4.4.1 Point to point cloud utilization across west router

The general point to point cloud utilization across the west router is given in figure 4.6 below

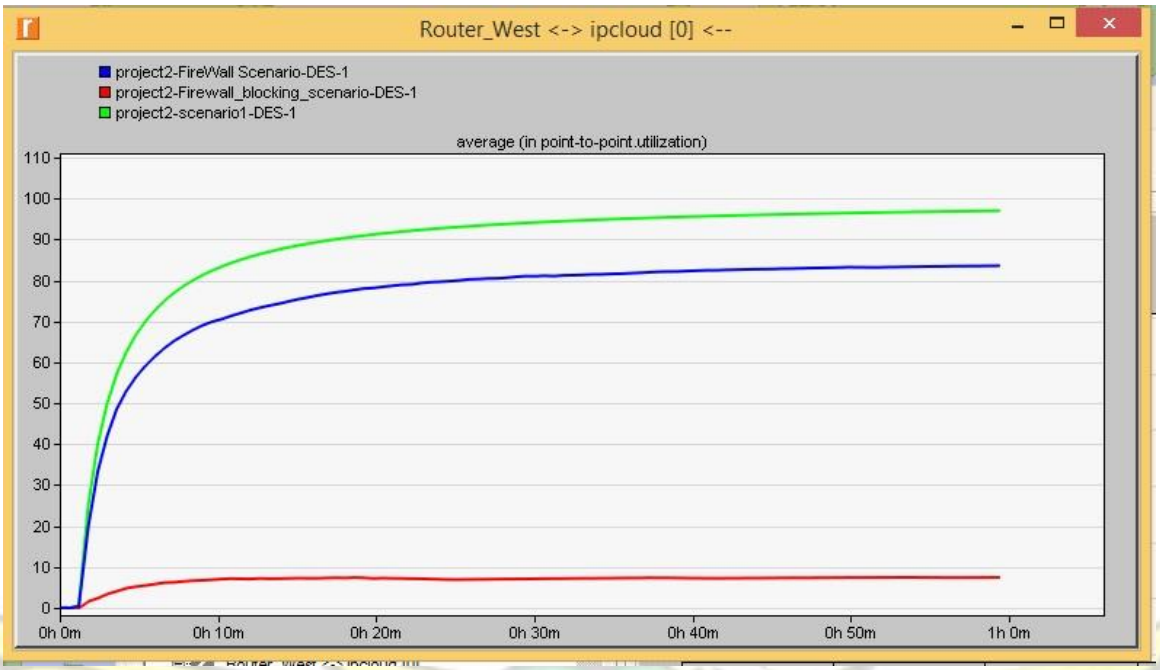


Figure 4.6 Point to point cloud utilization

It is observed from the graph that general point to point utilization of cloud is higher when the network has firewall set up in. The high utilization of cloud is due to security policies set by the firewall as well as delay in packet filtering. From the graph the cloud utilization is reduced with the third scenario (blocking of the web traffic) because small time is required in processing the database packets. With no firewall the cloud utilization is more due to database and Http packet processing. In general, we can derive that the overall cloud utilization is optimized when the web traffic is blocked using firewalls.

From the analysis of the proposed model the database application is enhanced when the firewall is used. From the simulations using two applications the database and web application, it is seen that the database application performance is improved when the web traffic is blocked. Even against the packet latency and the security policies the database point to point utilization is enhanced. Therefore, the objective of the project to improve the performance of the cloud

and security by blocking the web traffic is achieved from the analysis of the result. From the proposed model the database users are provided with fast the query response time and the general performance of the cloud is improved when the point to point utilization is decreased.

CHAPTER FIVE

5.0 Recommendation and Conclusion

In the outline of this work, I discussed about security which is a big concern in cloud computing Systems. Three scenarios are created in this simulation as explained in the previous chapters; scenario where there is no firewall, another scenario where firewall is created to filter database and web application packets and the third scenario is made to block the web traffic across the cloud. The performance metrics selected at the three levels (global level, node level and link

level) is used to evaluate the performance for the database and web application From the simulations using two applications the database and web application, it is seen that the database application performance is improved when the web traffic is blocked. Even against the packet latency and the security policies the database point to point utilization is enhanced. Therefore the objective of the project was to carry out a comparative analysis of the various scenarios and to evaluate the performance of cloud and understand the level of its security requirements

From the proposed model the database users are provided with fast the query response time and the general performance of the cloud is improved in terms of the decreasing the point to point utilization.

REFERENCES

Galen Gruman. (2009).What cloud computing really means. Journal of cloud computing. 21(1), p10-14.

Dave Asprey.(2010). Building a truly secure Cloud with Dell and Trend Micro. Journal of Computer Applications. 2(1), p9-15.

Richard Chow.(2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing control. International Journal of Network Security & Its Applications (IJNSA. 20(1), P7-12.

Alan Boehme.(2010). Top Threats to Cloud computing V1.0. Cloud Security Alliance. 10(2), p19-23.

CHEN Quan. (2009). Cloud Computing and its key techniques. Journal of Computer Applications. 20(1), p10-12.

Kevin Hamlen. (2010). Security Issues for cloud computing. International Journal of Information Security and Privacy. 4(2), p12-15.

ELIZABETH WHITE. (2009). Safeguarding Management and Security in the Cloud. Cloud Security Journal. 3(1), p8-12.

Aderemi A. Atayero. (2011). Security issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences. 2(10), p12-16.

David Binning. (2011). Top five Cloud Computing Security Issues. International Journal of Software engineering. 4(2),p20-24.

Terri Quinn-Andry. (2010). Pervasive Security Answers Cloud Computing Worries. Cisco cloud articles.2(1),p10-13.

Chaudhary,J., & Mishra, A. (2016). Literature Review: Cloud Computing- security Issues and Data Encryption Schemes, 6(1), 1-6. Retrieved from https://www.researchgate.net/profile/Carlos_Westphall/publication/313856926_CLOUD_COMPUTING_2017_The_Eighth_International_Conference_on_Cloud_Computing_GRIDs_and_Virtualization/links/58ab9e8092851cf0e3ca4f33/CLOUD-COMPUTING-2017-The-Eighth-International

Cision. (2015). Cloud Security Market – Global Industry Analysis, Size, Share, Growth, Trends and Forcast 2014 – 2022. Retrieved August 30, 2018 from https://www.prnewswire.com/news-releases/cloud-security-market---global industry-analysis-size-share-growth-trends-and-forcast-2014---2022300140401.html

Dirk Grunwald and Soraya Ghiasi. Microarchitectural Denial of Service: Insuring Microarchitectural Fairness. In ACM/IEEE International Symposium on Microarchitecture, 2002.

Dunfee, Esch, Driscoll, Hollman, & Plack. (2011). Background and Literature Review. *Sioanal Growth Chirema*, 10-43. https://doi.org/10.3928/01484834-20130613-03

El-gazzar, R. (2016). *A Literature Review on Cloud Computing Adoption Issues in Enterprises.* https://doi.org/10.1007/978-3-662-43459-8

El-gazzar, R.F. (2014). Creating Value for All Through IT. 429(December). https://doi.org/10.1007/978-3-662-43459-8

Fangfei Zhou, Manish Goel, Peter. Desnoyers, and Ravi Sundaram. Scheduler Vulnerabilities and Coordinated Attacks in Cloud Computing. In EEE International Symposium on Network Computing and Applications, 2011.

Gai, K., & Li, S. (2012). Towards Cloud Computing: A Literature Review in Cloud Computing and Its Development Trends. *2012 Fourth International Conference on Multimedia Information Networking and Security*, 142-146. https://doi.org/10.1109/MINES.2012.240

Ghanbari, Z. (2017). A Literature Review on Cloud Computing Issues. *International Journal of Information, Security and Systems management,* 6(1), 637-640.

Hartmann, S.B., Braae, L.q.N., Pedersen, S., & Khalid, M.s (2017). The potentials of using cloud computing in schools: A systematic literature review. *Turkish Online Journal of Education Technology – TOJET, 16*(1), 190-202.

Harkeerat Singh Bedi and Sajjan Shiva. Securing Cloud Infrastructure Against Coresident DoS Attacks Using Game Theoretic Defense Mechanisms. *In International Conference on Advances in Computing, Communications and Informatics, 2012*.

Iankoulova, I., & Daneva, M. (2012). Cloud computing security requirements: A systematic review. *Research Challenges in Information Science (RCIS), IEEE(2012 Sixth International Conference),* 1-7. https://doi.org/10.1109/RCIS.2012.6240421

IBM. (2018). Benefits of cloud computing / IBM Cloud. Retrieved August 29, 2018, from https://www.ibm.com/cloud/learn/benefits-of-cloud-computing

IEEE, C. (2010). Enabling Technologies for Cloud Computing. IEEE, (June), 1-12.

Ishaq, A., & Brohi, M.N. (2015). Literature Review of Cloud Computing in Education Sector: A survey with request to Qatar. *International Journal of Computer Applications, 132*(17), 9-14.

Judith, H., Robin, B., Marcia, K., & Fern, H. (2017). Comparing Public, Private, and Hybrid Cloud Computing Options. Retrieved August 30, 2018, from https://www.dummies.com/programming/networking/comparing-public-privateand-hybrid-cloud-computing-options/

Kayali, M.H., Safie, N., & Mukhtar, M. (2016). Literature Review of Cloud Based Elearning Adoption by Students: State of the Art and Direction for Future Work. *IOP Conference Series: Material Science and Engineering, 160*(1). https://doi.org/10.1088/1757-899X/160/1/012087

Lavanya, B. M., & Bindu, C.S.(2016). Systematic Literature Review on Resource Allocation and Resource Scheduling in Cloud Computing. *International Journal of Advanced Information Technology (IJAIT), 6*(4), 1-15.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.

Ming, T.M., Jabar, M. A., Sidi, F., & Wei, K.T. (2015). A systematic literature review of computer ethics issues. *Journal of Theoretical and Applied Information Technology, 78*(3), 360-372. https://doi.org/10.5121/hiij.2014.3402

Muller, S., Holm, S., & SØndergaard, J. (2015). Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. *Communications of the AIS*, 37, 851878.

Pfarr, F., Buckel, T., & Winkelmann, A. (2014). Cloud Computing Data Protection- A Literature Review and Analysis. *2014 47th Hawaii International Conference on System Sciences*, 5018-5027. https;//doi.org/10.1109/HICSS.2014.616

Priyadarshinee, P., Jha, M.K, & Raut, R. (2014). Cloud Computing Adoption in SMEs: A Literature Review. *Proceedings of the 12th AIMS International Conference on Management*, 1-5.

QLD. (2017). Benefits of cloud computing / Business Queensland. Retrieved August 29, 2018, from https://www.business.qld.gov.au/running-business/it/cloudcomputing/benefits

Samalekas, K. (2010). Network Forensics: Following the Digital Trail in a Virtual Environment, (October),64. Retrieved from https://publications.lib.chalmers.se/records/fulltext/12809.pdf

Shah, B., & Vania, J. (2014). A Literature Survey on Virtualization Security Threats in Cloud Computing,3(12), 2012-2015.

Sharma, P., Ii, P.P., Irwin, D., Shenoy, P., Goodhue, J., & Culbert, J. (2017). Design and Operational Analysis of a Green Data Center. *IEEE Internet Computing*, (Figure 1), 1-1. https://doi.org./10.1109/MIC.2017.265103636

Sheme, E., & Frasheri, N. (2013). A Literature Review: Cloud Computing Energy Aspects Research and Reports, 105-110.

Srivastava, A. (2014). A Detailed Literature Review on Cloud Computing. *Asian Journal of Technology and Management Research*, *04*, 2249-892.

Techopedia. (2017). What is Cloud Computing? – Definition from Techopedia. Retrieved August 30, 2018, from https://www.techopedia.com/definition/2/cloudcomputing

Thomas Moscibroda and Onur Mutlu. Memory Performance Attacks: Denial of Memory Service in Multi-core Systems. In USENIX Security Symposium, 2007.

Wu, D., Hugenholtz, P., Mavromatis, K., Pukall, R., dalin, E., Ivanova, N.N., ... Eisen, J. a. (2009). CLOUD COMPUTING – An Overview. *White Paper*, *462*(7276), 1-5. https://doi.org/10.1038/nature08656

Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for information Systems*, *31*(2), 35-60. https://doi.org/10.1.1.261.3070

Yu, Z., Wang, N., Su, X., &Ge, S. (2017). A Descriptive Literature Review about Cloud Computing Security Research in the IS Discipline, (Csae), 421-432. Retrieved from http://dpi-proceedings.com/index.php/dtcse/article/viewFile/17512/17019