Cloud Banking Security through Third Party Auditing with a digital signature

By

Kevin Mwamiri Kadogo

Master of Science in Data Communication

KCA UNIVERSITY 2013

DECLARATION:

I declare that this dissertation is my original work and has not been previously published or submitted elsewhere for an award of a degree. I also declare that this work contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: KEVIN MWAMIRI KADOGO REG. NO: 11/01769

Sign: _____Date: _____

SUPERVISOR APPROVAL

I do hereby confirm that I have examined the master's dissertation of

KEVIN MWAMIRI KADOGO

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Sign:…… Date: 1st October 2013

DR. PATRICK KANYI WAMUYU

Dissertation Supervisor

ABSTRACT

Cloud computing from the last few years has rapidly grown from a business initiative into one of the fastest growing Emerging Technologies of Information and Communication Technology. It is an Internet based model that allows customers and enterprises to have an appropriate service that is paid per use and there is a network access to a shared collection of resources such as services, storage area, networks, servers and application programs that may not require end-user know-how of the site location and other computing infrastructure details. Financial institutions, especially the banking sector have slowly but reluctantly started embracing this technology with a view of reaping these benefits. This diverse exemplar makes available other security huddles. This work looks at the dilemma of ensuring the integrity of customer data that is stored in Cloud through the realization of the Third Party Auditor (TPA) with a digital signature. For this, since the services offered by the cloud service providers are accessible through the web this work demonstrates a security scheme or model that permits only the required data through the web and database applications. The objective of this work is to evaluate the security of the cloud alongside the Third Party Auditor performance under two scenarios that are dissimilar. The simulation tool used is the OPNET IT guru and a set of two scenarios are fashioned. Scenario number one does not have security across the cloud and scenario two has the authentic TPA implementation and this particular TPA has security policies to allow only the required traffic. Traffic of the database and http are used as the required applications across the cloud as a source of data and the TPA will take action on these applications. Evaluation of the performance of the cloud will be done across the database and web applications are estimated alongside the TPA way or conditions for working. The two test scenarios are compared against the metrics for the individual applications and also the performance of the cloud is estimated. The protection of data to be done by other authorized parties apart from the Cloud Service Providers (CSP) and Cloud Clients (CC) in a way that provides better security and performance than the prevailing ones.

TABLE OF FIGURES

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 BACKGROUND

The United States of America's National Institute of Standards and Technology (NIST) has consolidated efforts in defining cloud computing. NIST (2009) defines cloud computing as a model for providing an enabled, convenient, on-demand, pay-as-you-use network access to a shared collection of a computing resourses that are configured that include applications and programs, storage, servers, services and networks among others that can be customized easily and with speed with limited management effort or interaction with the cloud service provider. NIST (2009) provides a pictorial presentation of this definition as indicated on figure 1.

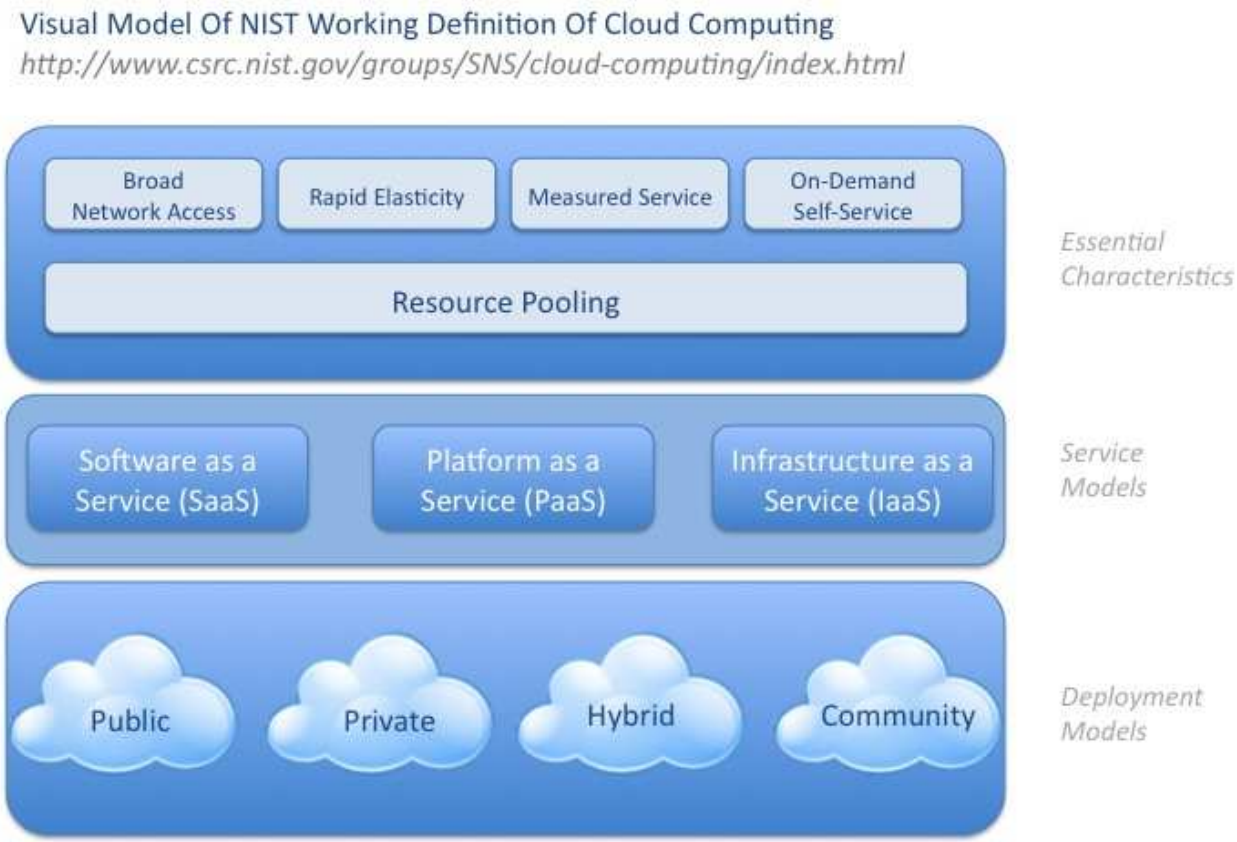


Figure 1: Visual Model of Cloud Computing Definition (NIST, 2009)

The above NIST definition is not in-depth and it is interestingly difficult to find two experts having the same definition of the cloud computing. Cloud computing is still an evolving standard. The characteristics, deployment and delivery models, as well as the underlying risks, technologies, issues and benefits will be refined by various analysis by both the public and the private sectors.

As with most new technologies and paradigms, one tends to look for the functionality first and only later on, one looks after the security of such functionality. However, cloud computing raises such an amount of questions concerning security guarantees that potential users including banks are waiting for clear answers before moving into the cloud.

Benefits of using Cloud in Core Banking Systems

According to Accenture (2012), there are many benefits that are accrued in implementation of the cloud for the core banking systems. Firstly, the high costs incurred in running in-house data centers are removed. The use of Pay-Per-Use model also offers operational agility when you need it. The resources can be scaled efficiently and volume can be increased according to demand of the customer. Many banks can target on their core business as opposed to bothering themselves about infrastructure scalability. Finally, banks can be faster and more agile in generating new offerings. They need not worry about finding additional computing power.

In banks, this important service is vulnerable to attacks or failures that would bring irretrievable losses to the clients since their data is stored in an uncertain storage pool outside the enterprises. The major concern in using cloud therefore is its security and specific integrity. Users can be freed from the burden of local data storage and maintenance by outsourcing the data. But this comes out as a very challenging task in protecting the data integrity in cloud computing. Thus, enabling the ability to be audited by cloud data storage to improve on its security is of key significance and it enables the users to have the ability to confirm the integrity of the data that is outsourced (Wang et. al., 2009).

It is also advantageous to make the cloud accountable through the audit process in both customer's and service provider's perspective.
Through auditing, the client can therefore sense if the cloud does not run the service as agreed, and can hold the cloud provider responsible. Moreover, it assists the service provider to proactively detect and diagnose the customer's problems (Shah et al., 2007). At the moment, security global auditing standards such as Statement on Auditing Standards (SAS) and also Health Insurance Portability and Accountability Act (HIPAA), ISO/IEC 27001 are available and it is important to note such information security management is obtainable but cloud-specific standards have yet to be delivered (Mell et al., 2009).

1.3 PROBLEM STATEMENT:

1.3.1 Overview

Cloud computing users work with data and applications that are often located off-premise. In the banking sector, this data includes customer requests for instance cheque book requests, account balances requests, funds transfers, PIN change requests among other sensitive requests.

IBM (2012), asserts in their Global Risk Survey that cloud computing has brought about serious concerns involving the access to, use and control of data. In this survey, IBM found out that 77% of respondents deem that adopting cloud computing is tantamount to breaching privacy and makes it more difficult to exist; 50% of the respondents are worried about a data breach and loss whereas 23% are concerned about deteriorating of the corporate network security.

This research's gosl is to create a model that includes a Third Party Auditor to elucidate the impact that cloud computing has on the integrity and confidentiality of data preserved on behalf of banking institutions. Therefore it will look at:

- How data integrity of the cloud data can be improved through a Third Party Auditor.
- How data integrity relates to the security controls required in order to safeguard the data confidentiality for the banks customers.
- Developing a model to enhance security controls for the customers through having a Third Party Auditor with a digital signature.

1.3.2 Main Problem

To create a new a model that would ensure secure transactions through implementation of a Third Party auditor (TPA) with a digital signature apart from the cloud service provider and the client (Financial Institutions).

1.4 OBJECTIVES AND AIMS

1.4.1 Overall Objective

To develop a model that would ensure secure transactions through having a Third Party auditor (TPA) with a digital signature apart from the cloud service provider and the client.

1.4.2 Specific Aims

- **Identifying** the various cloud security models that are currently available that can enhance the integrity and security of Banks' customers' data on the cloud.
- **To design the TPA model that will be employed** by the banks in improving data integrity and security of the clients who will be transacting through cloud computing.
- **To develop a model** to involve a Third Party Auditor (TPA) for Cloud Computing for Banking in order to improve the data security and integrity.
- **Demonstrating how the model will be implemented through the use of OPNET IT Guru.**

- **Testing and validating** the Third Party Model for banking through the cloud computing.

1.5 RESEARCH QUESTIONS

1. What do the existing Cloud Security Models comprise of?
2. What data integrity risks are the banking cloud services experiencing? How will the data integrity of the cloud data be improved by the Third Party Auditor with a digital signature?

1.6 SIGNIFICANCE OF STUDY

This study is important since;

a) It will demonstrate a security model introducing a Third Party Auditor for banks when outsourcing banking resources for its clients using smart or mobile devices.
b) Provide confidence to the banking industry on the data integrity of the customers' data.
c) Identify the data integrity risks associated with cloud computing in Banks

1.7 DEFINITION OF TERMS

- **Cloud Computing:** This is the use of resources for computing such as hardware and software that are delivered as a service over a network. The service maybe inform of hardware software, development platform among others that are on a pay-as-you-use basis (NIST, 2009).

- **Cloud Service Provider (CSP):** This is an individual who or company which makes available to customers hardware, server, storage and also applications and software services accessible via a private or public network (cloud). This therefore means these resources are available for access through the Internet.

- **Cloud Server (CS):** This is a server that provides remote services and Web hosting, to customers via a network of connected servers that comprise a cloud. It provides customers, unlike standalone servers and virtual servers, vast scalability options and the minimal potential for service interruption. It is also called a cloud host and provides customers with in other words seamless scalability, increased accessibility options, superior reliability and it is potentially cost saving.

- **Third Party Auditor (TPA):** This is an independent individual, entity or organization that audits the data of the cloud client on its behalf to ensure integrity of the data on the cloud server is upheld.

2.0 LITERATURE REVIEW

The migration to the cloud still remains a luring trend from a financial point of view but several major factors need to be considered by companies as they prepare to embrace this technology. Security is one of the major aspects. Inspite of the fact that some cloud computing security concerns are hereditary from other solutions adopted in order for the services to be created, quite a number of novel security questions that are specific to these solutions also come up, such include also the ones that are linked to how the services are structured and also the kind of service or data can be placed in the cloud (Gonzalez N. *et al.,* 2012).

2.1 Cloud adoption and banking sector

The appliance of cloud computing afford the financial industry with a cutting edge with aspects such as a strengthened data security, resources sharing, service quality improvement and significant reduction in operating costs. Cloud computing will therefore play a starring role in providing solutions to these problems (JingjingJiang *et al*, 2011).

Cloud computing is being embraced currently by many organizations and banks are now taking advantage of this but are still cautious since they need to be assured of the security aspect.

Online Banking Services (2010), a provider for solutions for revenue generating and cash management solutions, notes that Cloud computing will increase the customer base of the banks since customers will easily serve customers from the comfort of their locations. More so, Cloud computing facilitates financial hubs to meet the burden of thousands of customers for business banking who have diverse transaction volumes through many channels.

It is now correct to assert that Cloud-based contributions will influence social and mobile media to convert the banking occurrence and relationships for customers (Accenture, 2012). This notion from Accenture gives us a clue that cloud computing is there to revolutionalise the banking sector.

2.2 State-Of-Art in Cloud Security

2.2.1 Cloud Security

The analysis of security concerns in the context of cloud computing solutions shows that each issue brings different impacts on distinct assets. Therefore, the Cloud Security Alliance (CSA) puts emphasis on the Cloud Security Alliance categories indicated in figure 2;

Figure 2: Cloud computing security taxonomy (Cloud Security Alliance, 2009).

The above anatomy from Cloud Security Alliance shows a top level overview of the security taxonomy proposed, highlighting the three main categories: security related to privacy, architecture, and compliance.

From the above CSA taxonomy diagram, it can be deduced that security in a cloud is no different than security measures undertaken in any other IT environment. The security of the cloud majorly relies on both the Client and the Cloud provider who must all do their part in ensuring the security of the files and data being transferred.

As the cloud client goes about its business on the cloud maybe using the software, platform, infrastructure or any other services that exist on the cloud, there is need to

ensure that it guarantees value for the stakeholders. This can be achieved by ensuring that all the risks are scoped to ensure security of the cloud is maintained. According to ISACA (2010), in the guidelines to establish and ensure solvency, it provides that management must select response strategies in a cloud environment. This strategy should be all the specified risks that have been identified and analyzed. These therefore might include the below options:

- Avoidance: This will involve stopping any activities that may give rise to the risk
- Reduction: This involves setting up measures to reduce the possibility of occurrence or impact thereof of the related risk.
- Share or Insure: It majorly involves sharing or transferring the financing of the risk.
- Accept the risk: In this case no action is taken since cost/benefit decision has been made.

2.2.2 Cloud Security Models

This study looks at four existing Cloud Security Models explained below:

- The Microsoft Private Cloud Model
- NIST Cloud Security Model
- The Cloud Cube Model and
- The Data Security Model

2.2.2.1 The Microsoft Private Cloud Model

In the implementation of both the private and hybrid cloud, the information Technology (IT) decision-makers have raised substantial concerns with regards to the areas of data protection, legality, compliance and personally identifiable information (PII). These requirements are predominantly important in hybrid implementations, which require you

or the business units within your organization who are in the position of the customer to a public cloud supplier (Microsoft TechNet, 2012).
Some of the key issues highlighted under this are:

- **Governance** - Organizations looking to implement a private cloud infrastructure are likely to need to make certain that effectual governance of the new environment is taken into account. The management protocol of the private cloud architecture should enable administration to view security aspects of the environment and illustrate the current threat levels to the organization.

- **Compliance**: There is a possibility that by moving to a private cloud environment there may result in users in one country with a specified set of regulations accessing data in another country with a totally different or even contradictory set of requirements.

- **Data Protection and PII (Personally Identifiable Information): -** Personally identifiable information (PII) is data that allows a living person to be identified. The United States (US) Office of Management and Budget identifies the following information as PII.
    - Full name (unless a very common name)
    - National identification number
    - Vehicle registration plate number
    - Driver's license number
    - Date of birth
    - Birthplace

2.2.2.2 NIST Cloud Security Model

According to NIST (2011), the key security and privacy issues include:

- Governance

- Compliance
- Data Location
- Trust
- Architecture
- Identity and Access Management
- Software Isolation
- Data Protection
- Availability
- Incident Response

These NIST recommendations can be summarized as below:

- **Governance: -** What is required is to extend organizational practices pertaining to the standards, procedures, and policies used for application development and provisioning of services in the cloud, and also includes the design, implementation, testing, use, and scrutinizing of any deployed services or any services that have been engaged. Putting in place audit mechanisms and tools that will ensure organizational practices are adhered to throughout the system lifecycle.

- **Compliance:-** NIST advices that this level demands one to internalize the various types of laws and regulations that impose security and privacy obligations on the organization and that could potentially impact cloud computing initiatives, especially those involving data location, privacy and also security controls, management of records, and electronic discovery requirements. Constant reviews and assessing of the cloud provider's offerings with respect to the organizational requirements to be met to ensure that the contract terms adequately meet the requirements. Lastly measures need to be taken to ensure that the cloud provider's capability to discover electronic devices and processes do not compromise the privacy or security of data and applications.

- **Trust: -** Financial institutions need to ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. They also need to establish clear, exclusive ownership rights over data. More so, instituting a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system will instill trust. Finally, there also needs to be continuously monitoring the security state of the information system to support on-going risk management decisions.

- **Architecture: -** It is important to have a clear understanding of the technologies underlying technologies of the cloud provider in use in the course of service provisioning and taking into account the implications that the technical controls involved have on the privacy and security of the system.

- **Identity and Access Management:-** This require the cloud client to ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

- **Software Isolation:-** It is important to understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

- **Data Protection:-** Evaluation of the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data is also very important. Businesses or any organization need consider the risk of collating organizational data with that of other organizations and businesses whose threat profiles are high or whose data collectively is quite sensitive. It is important to also fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

- **Availability: -** It is key to understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. It is very important also to make sure that during an intermediate or prolonged disruption or a serious disaster, operations that are critical can be immediately resumed, and that all operations can be eventually recovered in a timely and organized manner.

- **Incident Response: -** Contract provisions need to be understood while making sure those procedures for incident response meets the requirements of the organization. Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. A matter of priority is to guarantee that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

2.2.2.3 The Cloud cube model

The cloud cube model tends towards identifying four different dimensions for providing security to the clouds. These dimensions can be categorized into two important types like the internal and external and these dimensions define the physical location of the data across the cloud. Organizational boundaries are considered as the internal and external dimensions for the cloud and it will be based on the cloud usage like from outside the organization or within the organization.

The second dimension is the propriety or open and this defines the ownership of the cloud when there is a security concern. The level of interoperability and data transportability is estimated across this aspect. The typical constraints on the data usage are estimated across this dimension. Propriety indicates the organization ownership and the control over the cloud remains with the cloud client, but the open indicates the public

nature of the cloud. These parameters are now used to impose the required security constraints.

The third dimension represents the Parameterized or De-Parameterized nature of the cloud. Parameterized indicates the architecture being followed across the cloud within the IT limits of the organization and the De-Parameterized indicates that the IT architecture is external to the organization. The internal network firewalls act across the Parameterized architecture, whereas the external firewalls acts across the De-Parameterized architecture.

The fourth dimension describes the Insourced or Outsourced nature of the cloud. In general Insourced dimension is maintained by own staff and the internal security Policies act on the cloud. Outsourced dimension deals with the security policies provided by the third parties.

2.2.2.4 Data Security model

Protecting the data is the main concern across cloud computing and this model describes a famous model to have the data protected. There is a three level defense system that is used across in providing security to the cloud data. Authentication of the User can be considered as the first layer and on this layer all the users who are trying to access the cloud data need to be authenticated against their login credentials.

Second layer is responsible for data encryption process. The user's data is protected using the typical data encryption models once the users are authenticated at the first layer. This can be considered as the important layer as encryption is always required to hide the actual data from the attacker. The third layer deals with the fast recovery of the data. In case the data is lost the recovery mechanism is implemented across this layer to enable all data is restored.

The user authentication layer is tasked with protecting the data from unauthorized access and to make sure that the data is not tampered with. Failure of the authentication layer in some cases, encryption is done by the second layer prevent the data from misusage and this provides an upper layer of data protection. The third layer has the key role to recover the data in a faster manner If the attacker can access the encryption keys and gain the data.

2.2.3 Cloud Audit

Currently, most of the cloud audit is done through the users doing their own audit. That is the clients perform the scrutinizing of documents, audit trails among other checks. These checks can be snap checks done daily, weekly, monthly, quarterly, yearly among other checks. According to Balaji (2012), almost all the cloud users and clients do auditing internally either by their IT or Business Teams. He proceeds to advice that the following must be considered by the users in the course of cloud auditing.

a) *Regulatory Compliance Audit:* It lists the regulations that will affect your data and applications, and will check if each of those regulations is met in your cloud setup.
b) *Disaster Recovery/Business Continuity (DR/BC) audit*: Ensure that the IT infrastructure continues to operate, even though partial, despite the disaster. Also, the mean time to recover the systems and amount of data recovered are important metrics when performing this audit.
c) *Security Audit:* It must uncover the various vulnerabilities in the cloud solution applied. Some of the security issues include Denial of Service (DoS), unauthorized access and intentionally destroying data that still has disposal hold. The audit should make sure the

setup is sufficiently protected against the common type of attacks and has the necessary level of security that satisfies the requirements of the enterprise. Therefore, considerable attention must be paid to data security issues to protect against any information leakage.

d) *Performance and Reliability Audit:* Reliability audit must make sure that your data is available to the employees and customers always. Downtimes can be very expensive, in terms of lost employee productivity and loss of goodwill from the customers. The audit should also spell out the Service Level Agreement (SLA) requirements and find out if all the providers satisfy those requirements. It is important to have performance audits must identify the various metrics (for instance time to save a document and time to load the website landing page) and verify if the cloud setup satisfies the metrics. Stress tests can be incorporated in the reliability and performance audits to make sure the stack used is robust under severe load conditions.

e) *ROI (Return on Investment) and business Audit:* Migration to cloud computing has to make proper business sense and this audit computes the ROI for the cloud infrastructure. The audit should be implemented at the total cost of the solution (including the costs for retraining staff) and also find out if it is cheaper to implement than the alternatives. A comprehensive business audit must spell out various business metrics and goals against which the cloud services have to be tested.

Over the past five years the world has been grappling with the economic crisis and banks among other institutions have been hit the most. The competition among banks has been breath taking in the quest to increase customer base and profits while reducing operational costs.

In a competitive scene that favors the fastest and the smartest; success for the future- thinking bank lies in information-led transformations. Banks need therefore to build sophisticated insight and predictive analytics so they can act on new insights ahead of the competition.

According to Accenture (2012) in its annual paper, Accenture's banking 2015-20, it looks at three unique business models emerging among smart banks as shown in Figure 3;
1. The "analytical multichannel" bank

2. The “socially engaging” bank

3. The “digital ecosystem” bank

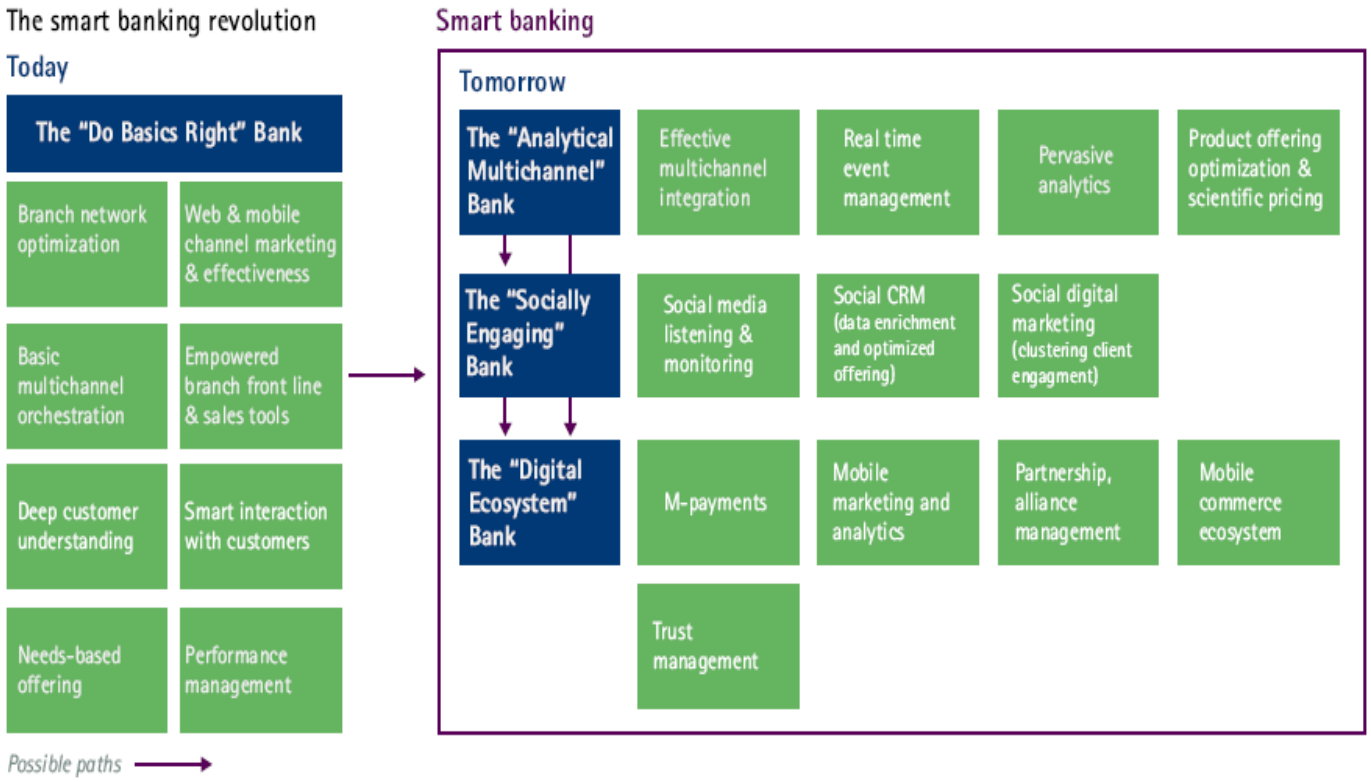


Figure 3: The smart banking revolution and emerging business models (Accenture, 2012)

Most consumers are now moving to the cloud and it is only wise for the banks and other enterprises to follow suit and be where their consumers are. Online transactions are now like a way of life. Ordering goods and services over the Internet and paying in the same way is now a norm.

The Cloud offers a lot in terms of energy optimization, reduction of operating costs and metered use (where you pay-as-you-use) among other services like Infrastucture (Iaas), Software(Saas), Platforms(Paas) and even of late Security-as-a-service.

2.2.4 Third Party Auditor

The Third Party Auditor (TPA) is skilled and capable than the cloud users and is trusted to judge the cloud storage service for the sake of the user upon request. Users depend on the Cloud Server (CS) for the storage and maintenance of their cloud data. They may also dynamically communicate with the CS to manage their stored data for different application purposes. The users may turn to TPA in assuring the integrity of their outsourced data, while believing to maintain the privacy of their data from TPA. We consider the presence of a semi-trusted CS as does. However, for their personal benefits the CS might ignore to Maintain or knowingly delete the data files of cloud users that are rarely accessed.

Furthermore, the CS may decide to conceal the data corruptions caused by any security breaches of the server to retain reputation (Andreas, 2010).

We consider the TPA to be reliable and have no motivation to conspire with either the CS or the users during the auditing process.

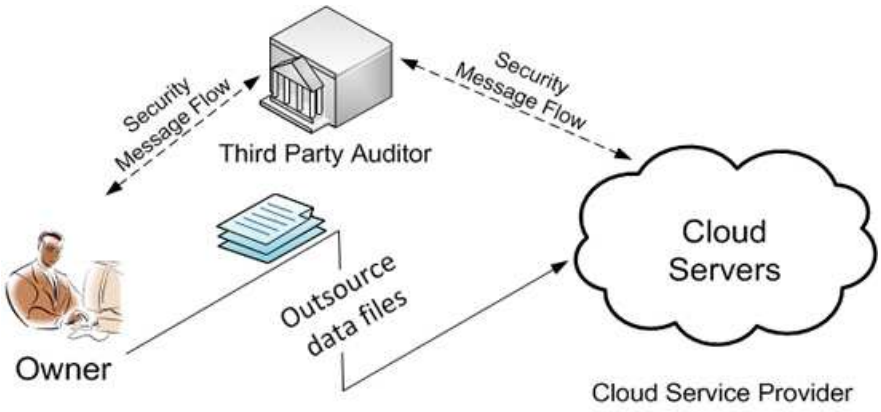


Figure 4: Cloud Data Flow Model (Wang *et al*., 2009)

The Cloud Data Flow model is a distributed application structure that segregates tasks or workloads between the suppliers of a service, called Cloud servers, and service seekers, called clients. Generally clients and servers communicate over a computer network on distinct hardware, but both may reside in one system. A server is a host machine that executes one or more server programs which share their resources with clients. A client machine never shares

any of its resources, but requests for services of the server. Therefore clients start communication sessions with servers that are waiting for incoming requests.

Despite many benefits cloud computing is still being met with resistance from the banking or financial industries with fear about security breaches (Pomares, 2011). Maintaining the integrity of data plays a vital role in the establishment of trust between data subject and service provider. As with any data storage and processing medium, data integrity problems exist within the Cloud computing paradigm (NEC, 2010).

Making the decision to outsource particular data, consumers – at either the individual or enterprise level – must be able to evaluate the risk of that data being corrupted or otherwise deleted to use. Thus, as a supplementary architectural component for Cloud computing, an auditor to whom the consumers could entrust the task of verifying data integrity is introduced. This auditor would be periodically checking the integrity of all data stored with Cloud Service Providers (CSPs) and release, for example, monthly audit reports.

From these reports, Cloud consumers could evaluate the risks related with any particular CSP before they decide to rely on its service. The audit report may also be useful to the Cloud service provider: in addition to assisting as a promotional means, a good audit report from a third party may help the service provider in getting a favourable insurance rate, in accordance with the measured stability of their prime valuable resource such as data.

To introduce an efficient third party auditor (TPA) for privacy (Wang et al., 2010) and security, the following basic requirements have to be satisfied: TPA should be in a position to effectively audit the cloud storage without requiring the local copy of data, and bring in no new extra on-line burden to the cloud user. This kind of auditing process should not introduce additional vulnerabilities against the privacy of user's data.

Wang et al., 2009 proposes a software application as an auditor that has used and uniquely combined the public key based homomorphic authenticator with random masking to attain the privacy-preserving cloud storage auditing system. Homomorphic authenticators are defined as

unforgeable verification metadata produced from individual data blocks, which can be securely combined in such a manner to ensure an auditor that a linear combination of data blocks is accurately calculated by checking just the aggregated authenticator.

Ateniese et al., 2007 defined a “provable data possession” (PDP) model for assuring possession of data files on untrusted storages. They describe techniques based on homomorphic tags for auditing this file. Even though their scheme is demonstrably strong, their technique requires sufficient computation that it can be expensive for a complete file. In a subsequent report (Ateniese et al., 2007) they described a PDP scheme that makes use of symmetric-key encryption. It relies on symmetric-key encryption and MACs to verify integrity of stored data.

2.2.5 State of Practice: Cloud Applications

Cloud has been applied to different sections already and is beginning to be a key part of our society.

Such include;

a) Google Docs: Different types of documents including normal word documents, PDF documents, and presentations can be uploaded and downloaded into and from the Google server from remote areas. Users are also given the provision of editing the document and uploading back to the server.
b) Mobile and Internet Banking: This can also be considered a major example of Cloud usage where customers transact over the web to the bank servers checking their balances, performing funds transfers, paying bills among other banking tasks thus the data is downloaded from the banks servers amended and uploaded back with amendments as per the customers’ request.
c) Emailing Servers: Use of different Emailing Servers like Google Mail, Yahoo and hotmail among others provide privileged mail access to users across the globe. Therefore mails and corresponding attachments are stored in these remote servers.

d) YouTube is also an example of the cloud application and is now widely used in video storage. The users upload videos and can easily be downloaded by anyone, anywhere and at anytime.
e) Picasa application: Users can upload photos and download them through picasa URLs. The corresponding photos are stored in the picasa server.
f) There are also some storage sites for instance www.4shared.com and also www.sendspacce.com which provide remote storage space for the users who are registered.

3.0 METHODOLOGY

3.1 RESEARCH STUDY:

This study will be conducted through an experiment. Thus the experimental methodology is adopted.

3.2 RESEARCH DESIGN

3.2.1 CONCEPTUAL MODEL

The model proposed in this work involves a Third Party Auditor who is an independent Company. It does not restrict it to a software auditor as Wang et al., 2009 and Ateniese et al., 2008 does.

The model will include the Third Party Auditor who ensures the data integrity is maintained but since this is more or less a software, there is a 24hour standby administrator to ensure the software works well and any exceptions raised thereof are handled immediately.

The model will appear in figure 5 below.

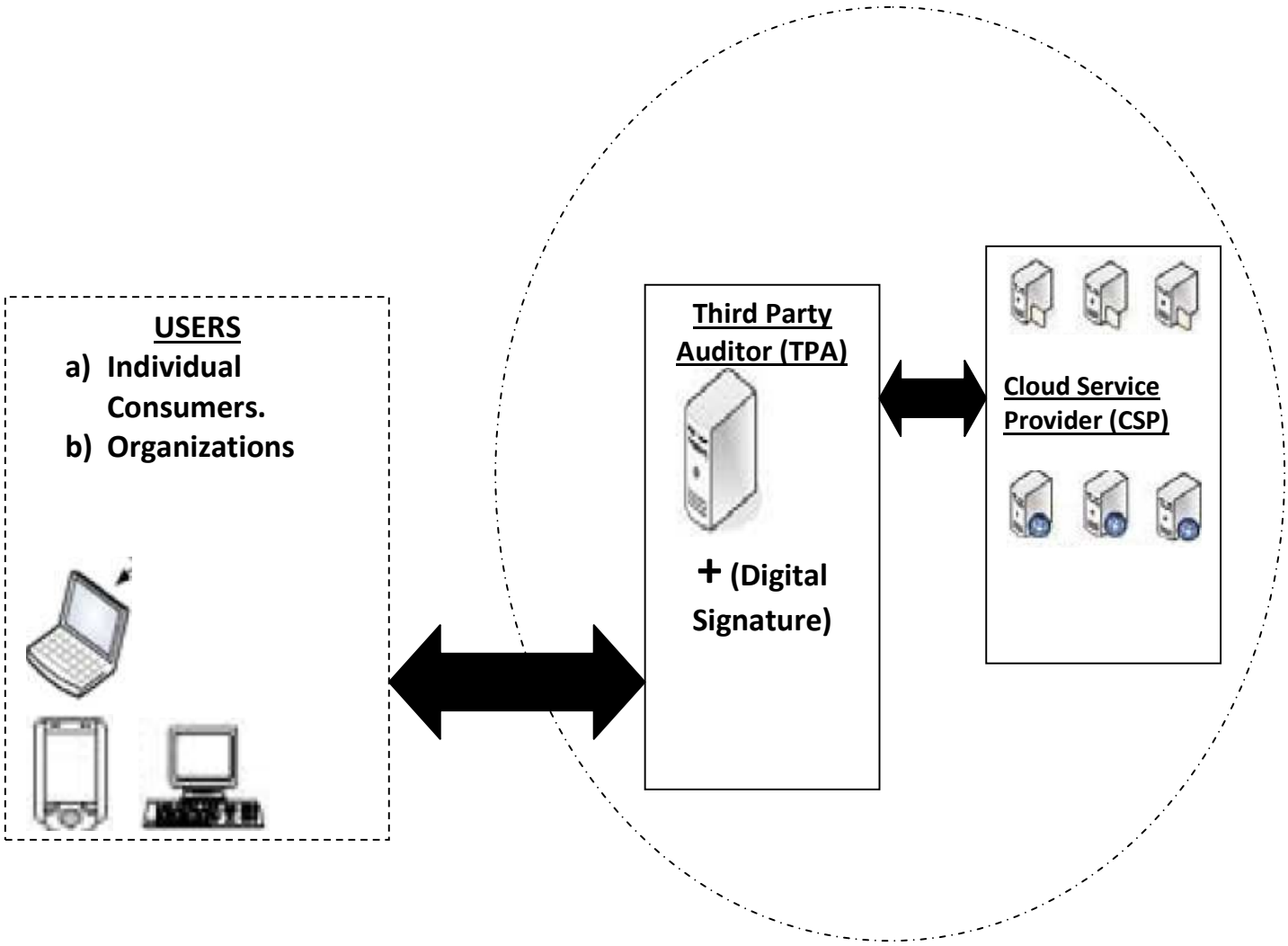


Figure 5: TPA Conceptual Model (TPA including digital signature)

3.2.2 DATA COLLECTION METHODS:

Data collection in this study will be obtained through running several simulations through OPNET IT Guru and analyzing the results as required.

3.3 SAMPLE AND POPULATION

Sampling Frame

The sampling frames used will be OPNET IT Guru network traffic data

3.4 DATA ANALYSIS TECHNIQUES:

Data analysis is the process of analyzing all the information and evaluating the relevant information that can be helpful in better decision making (Sivia & Skilling, 2006). The Analysis of data can be done through the use of various tools and methods. Data analysis is important in helping to derive the conclusion out of the gathered information.

3.4.1 Descriptive Analysis Methods:

According to Lindloff and Taylor (2010), collected data are organized in such a way that it will describe the nature and type of data collected. Diagrams, graphs and or Tables can be used to demonstrate this. This method is helpful in making better decisions. It is also very easy to understand and analyze the data through the diagrams.

3.4.2 Comparative Analysys:

This method of analysis is through comparison of results obtained from the experiments using different variables and parameters. In this study, we compare several scenarios to come up with a knowledgeable conclusion as to how security in the cloud will be improved.

3.5 IMPLEMENTATION OF CLOUD SECURITY MODEL

3.5.1 Implementation Model:

The implementation model includes the presence of a Third Party Auditor (TPA) as a middle-man between the Cloud Client (Banks) and the Cloud Service Provider (CSP). To ensure every

access by the user to the Cloud storage is in control, this model proposes a model where Cloud Bank Client utilizes the cloud storage through an auditor with digital signatures.

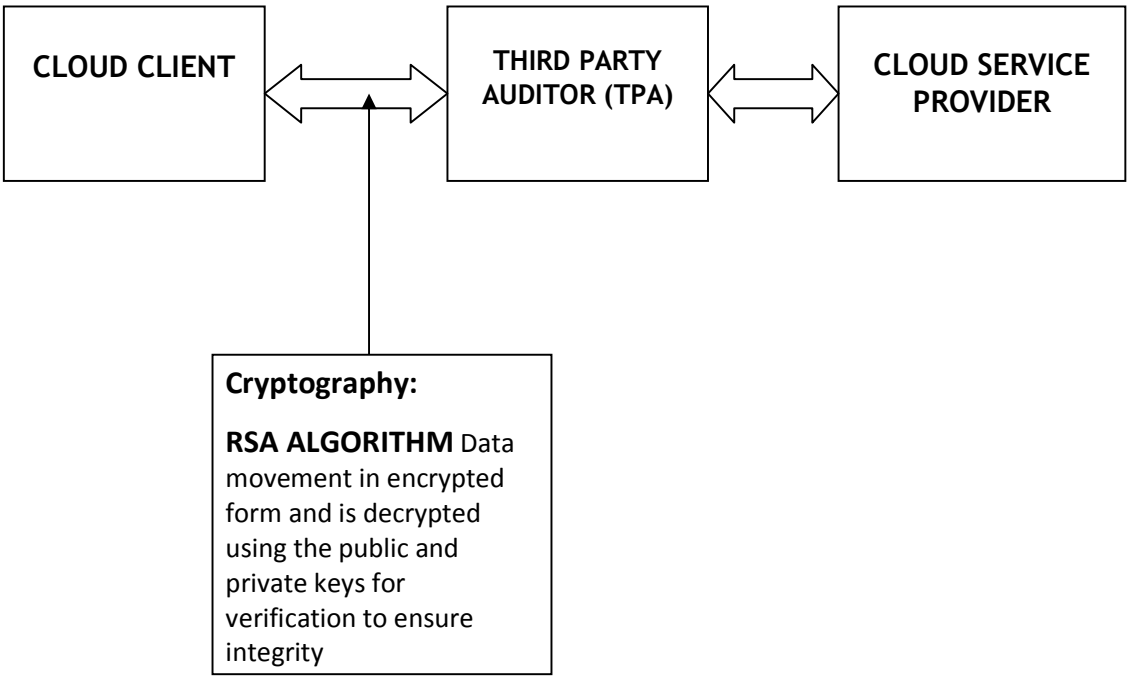


Figure 7: Implementation Model incorporating a TPA and RSA in the Cloud Security Model

3.5.2 Implementation Tools

The implementation tools will include the OPNET IT Guru that will be used as a simulation tool.

3.5.3 Implementation Procedure

a) No TPA Scenario

OPNET IT guru is a simulation tool that helps in demonstrating scenarios. This scenario tends to show in the network that there is no TPA with digital signature. The IP based cloud tool on OPNET tool is implemented and it doubles up as the internet cloud provides a connection between two or more subnets that represent the cloud service provider. A set of a pair of routers is setup transversely on the network and one of them is used as the firewall router. A database application and a web application are used as the main applications to generate traffic. The necessary traffic for the application is generated by having to configure at the profile level of the application. An extreme database access application is used in this case to force more queries by the database over the database server. A crucial setup is performed at the profile together with the application levels and the cloud response against the web and the database is thoroughly analyzed.

Figure 8 below demonstrates the basic workspace of OPNET It guru.

Figure 8: OPNET IT Guru Main screen

A new project is created from the file menu. The corresponding process is then described in the paragraphs below.

The cloud simulated in this project is performed with 150 hosts with the simulations being done in such a way that the 150 hosts do access the database and the web applications. In this scenario, no security was provided and the way the cloud performs normally is estimated. To do an evaluation of the clouds' performance, several performance metrics are used. Such include response time of the HTTP page for the web application, Database query and response times and the statistics of the Nodes can also be used to evaluate the performance of the cloud.

The level and utilization of the link are also estimated for the purposes of cloud performance evaluation.

b) TPA with RSA scenario

This scenario duplicates the scenario in 3.6.4.1 and introduces a TPA and RSA cryptography in order to ensure that the files are checked and prevent an unauthorized access and also make sure only data sent is the data that is received at the other end.

c) OPNET IT Guru - Simulation Tool

OPNET IT Guru offers a strong edge that can be used to fashion the required model of the network. The two main simulations for the cloud are performed in this project. The simulation will capture a scenario with the TPA and the digital signature and another without the TPA.

All the required components of the network are found from the OPNET IT Guru Object palette. It provides a platform that can be used to deduce comparisons among the different scenarios which can then be utilized in recreation of the scenario as required accordingly. What is required to be changed is done on the scenarios that are duplicated and once the desired number is arrived at, an evaluation of the performance is done by selecting the individual statistics at different levels that is the Global, node and link levels. The detailed procedures for the scenarios run in this project are as below.

4.0 DATA COLLECTION (SIMULATION)

4.1 Simulation of No TPA with RSA scenario procedure

To simulate a basic network, a new project is created as shown below and the scenario name provided as No TPA.

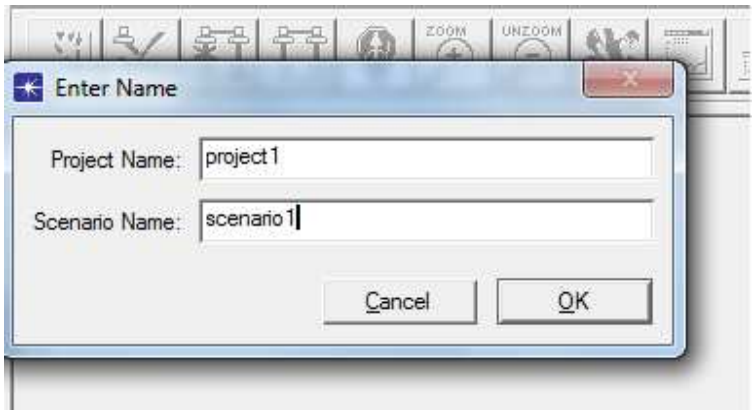


Figure 9: Creation of new project and scenario.

The below steps are then followed to create the basic network.

- The initial topology option is chosen as Create Empty scenario then click next.
- The required network scale is chosen as the world then click next.
- None is selected in the maps and click next.
- Click next twice and once this is complete,
- The workspace and the object palette appear as shown below.

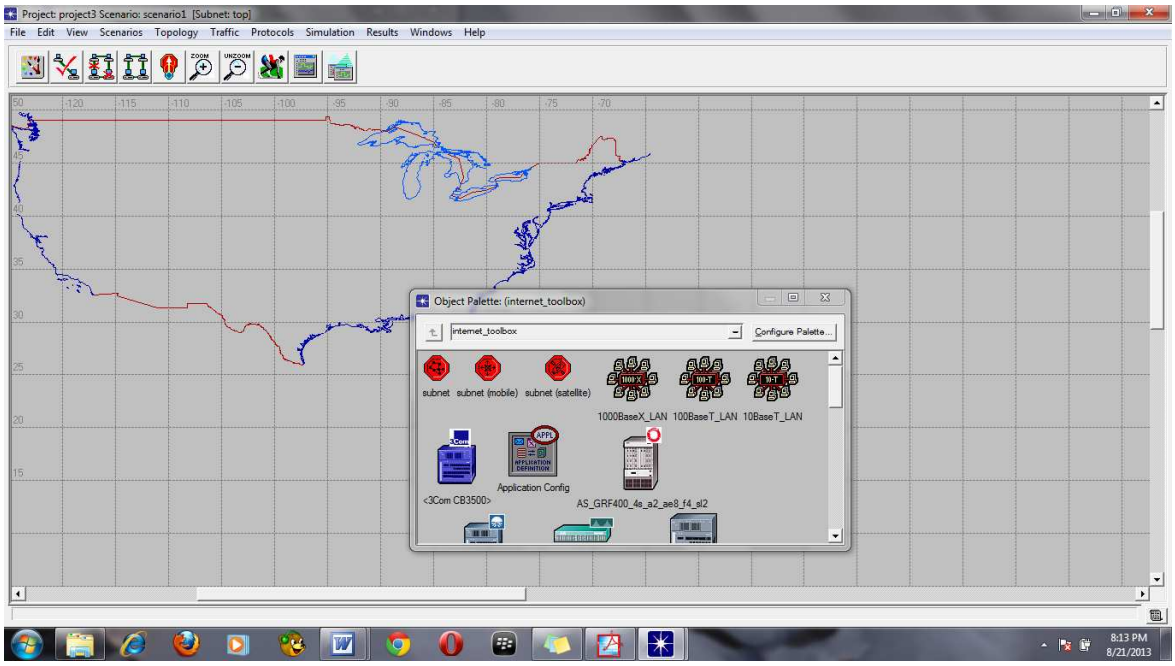


Figure 10: Workspace for the network on OPNET IT Guru

The next step involves dragging the from the object palette to the workspace the following listed objects.

a) Application Configuration object – In this case the database and web applications will be used.
b) Profile configuration object – This will be used for the definition of the application profiles.
c) The Ip32_Cloud – Used as the cloud (Internet).
d) 2 ethernet4_slip8_gtwy's.
e) A 10BaseT_LAN object is also used – To act as a workplace to support 150 workstations.
f) Two ppp_server objects are also dragged to the workspace – They will act as the database and web server.

The configuration on the workspace will be rearranged and configured as below:

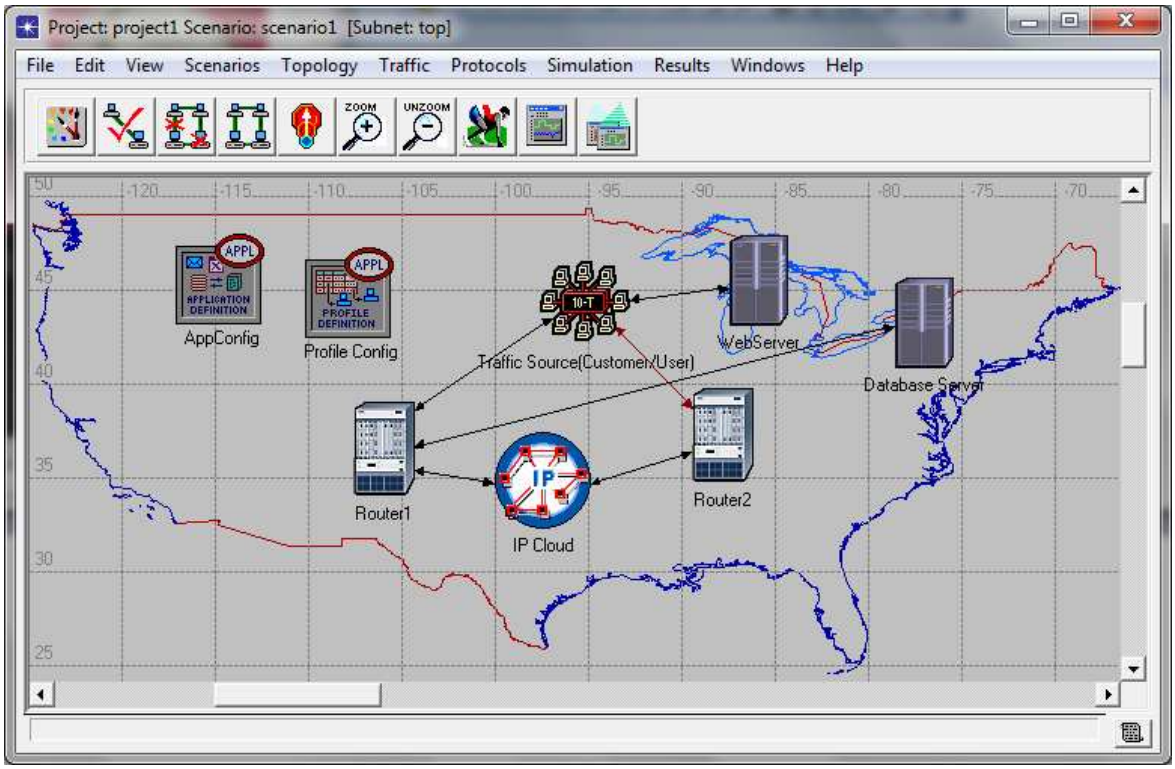


Figure 11: The basic network setup on the workspace.

4.1.1 Application and Database Configuration

The application configurations are configured as below for both the database and web applications.

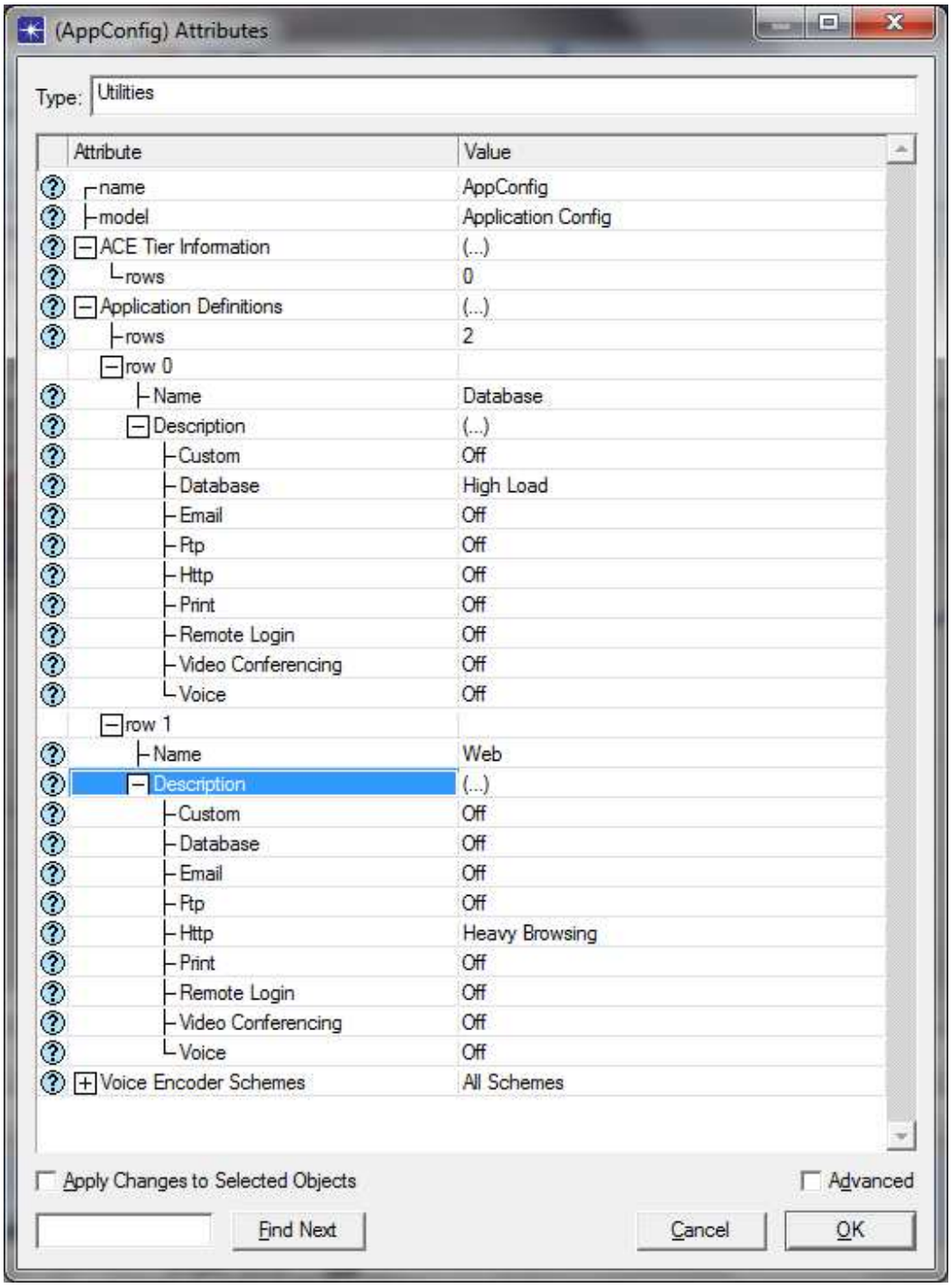


Figure 12: The Application Configurations for both the database and the http traffic

The profile configurations are as below.

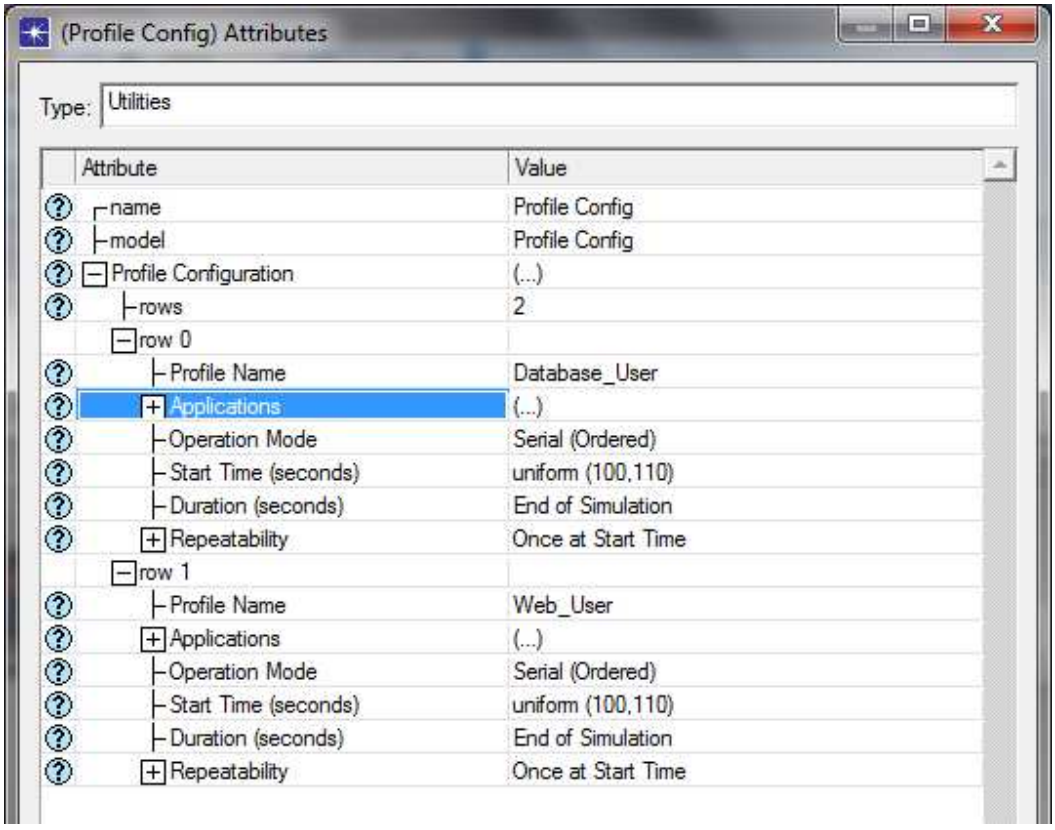


Figure 13: Profile configuration for both the database and web user profiles

The profiles creation signifies means that the applications have the ability to generate traffic and therefore the configuration of the cloud can be done.

4.1.2 Cloud Configuration

The next step involves the configuration of the cloud from the OPNET IT Guru IP32_cloud object on the workspace. In this research, the cloud has been used to provide support to the web/http application and the database.

The cloud configuration will appear as below in figure 14:

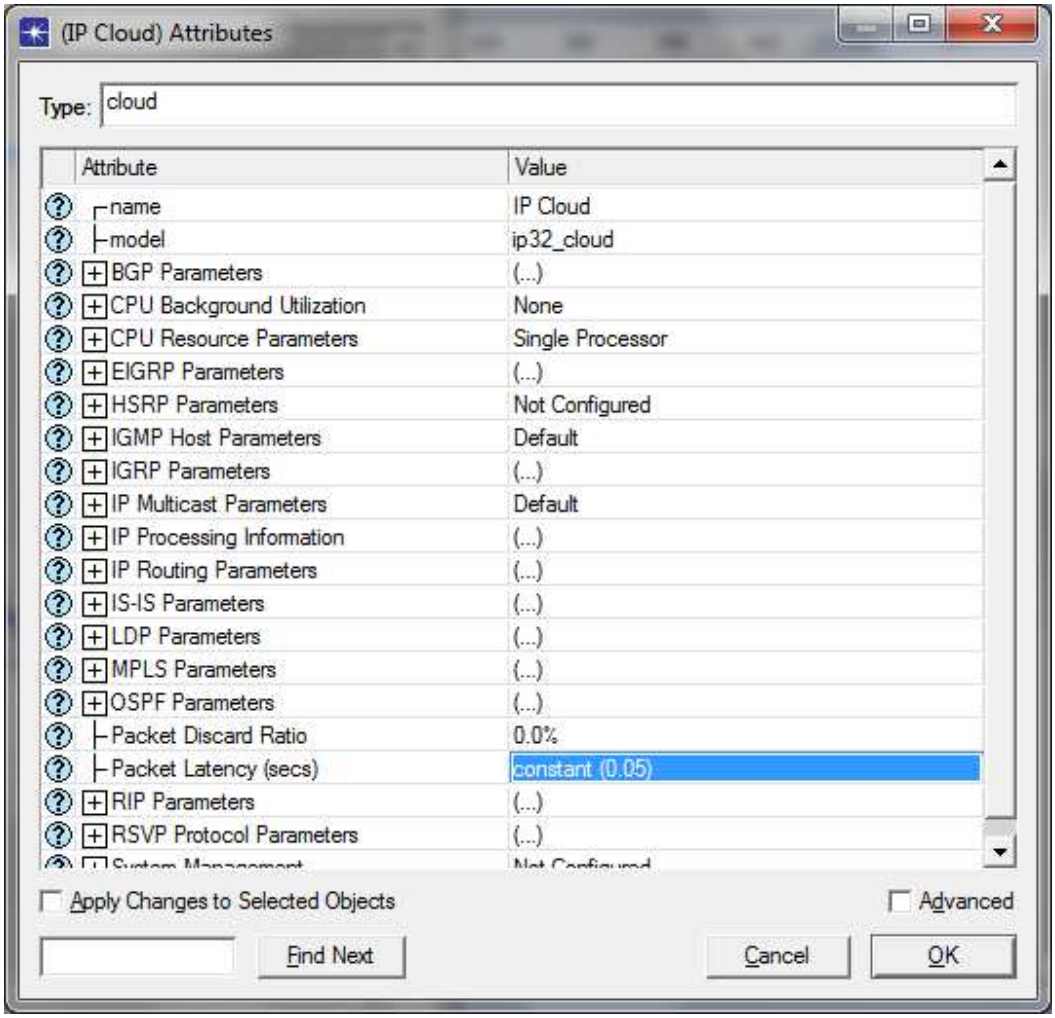


Figure 14: Cloud Configuration

Configuration has been made to have the packet latency as 0.05 seconds to enable maximum packet delay, due to the web and the database applications, across the cloud to be limited to just 50ms. As a result, all packets in the cloud are progressed with this delay that is limited.

4.1.3 Router Configuration

The routers configuration will now follow with both router 1 and router 2 connected to the cloud via the PPP_DS1 links as shown below:

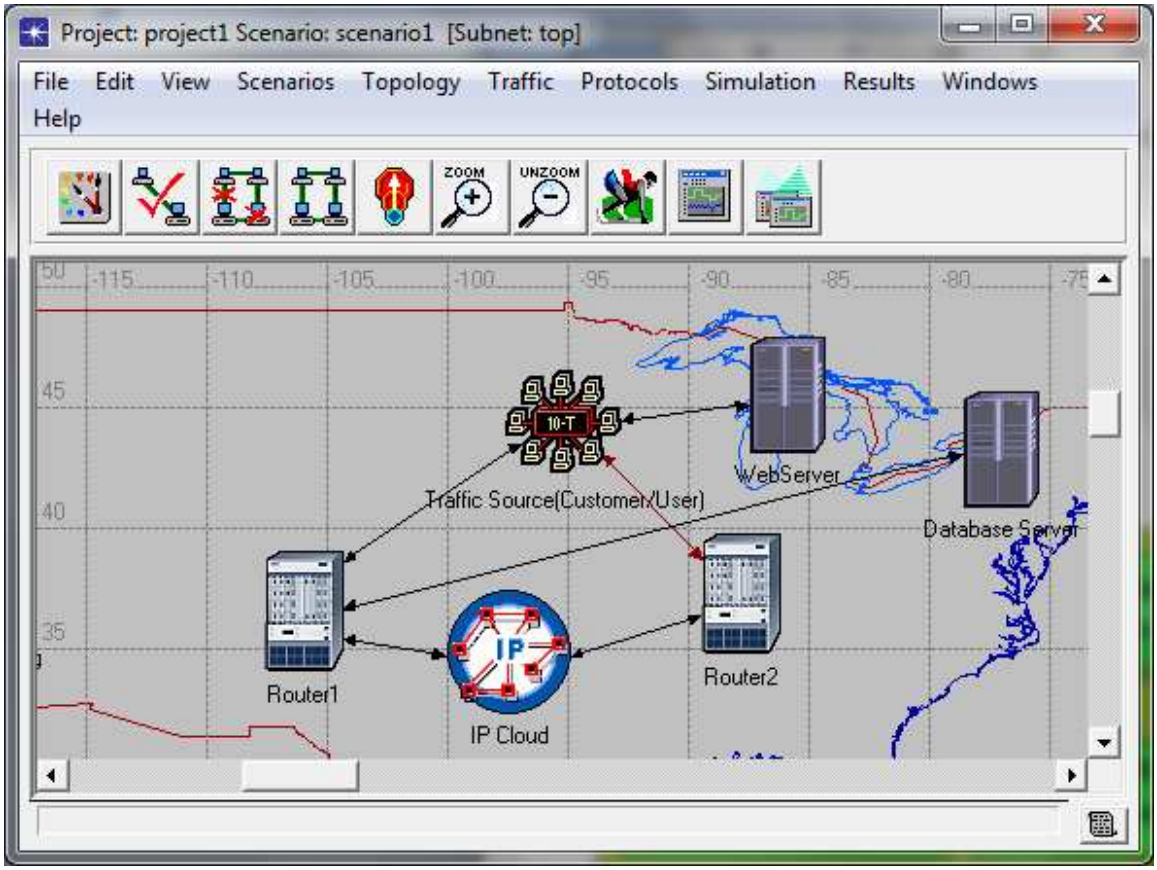


Figure 15: Router Connection

4.1.4 Client Configuration

The number of users in this setup will be depicted by the number of workstations which is 150 in number. Both web and database profiles are configured to support up to 100 and 50 respectively. The client is configured as shown below.

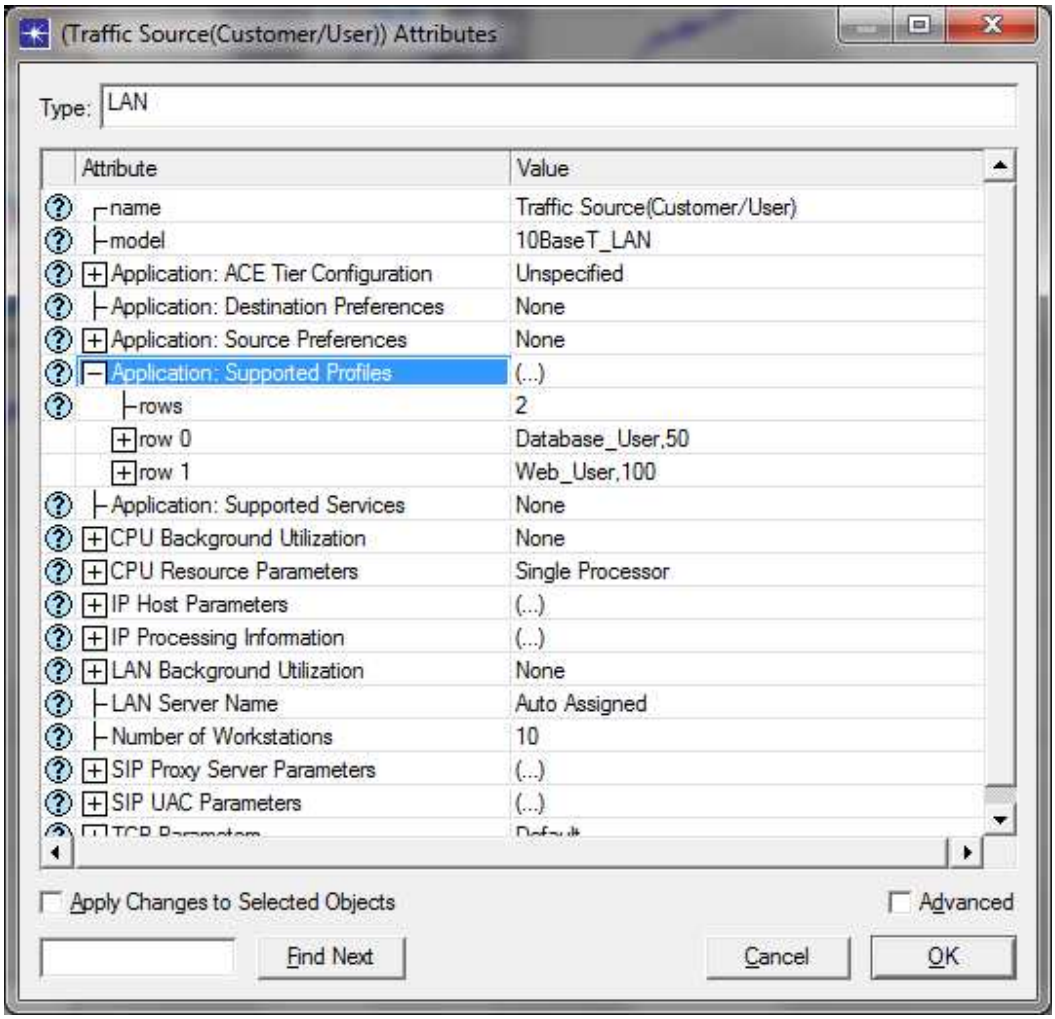


Figure 16: Client Configuration

4.1.5 Server Configuration

The servers were then configured on the OPNET IT Guru to show the nature the application it supports as shown below:

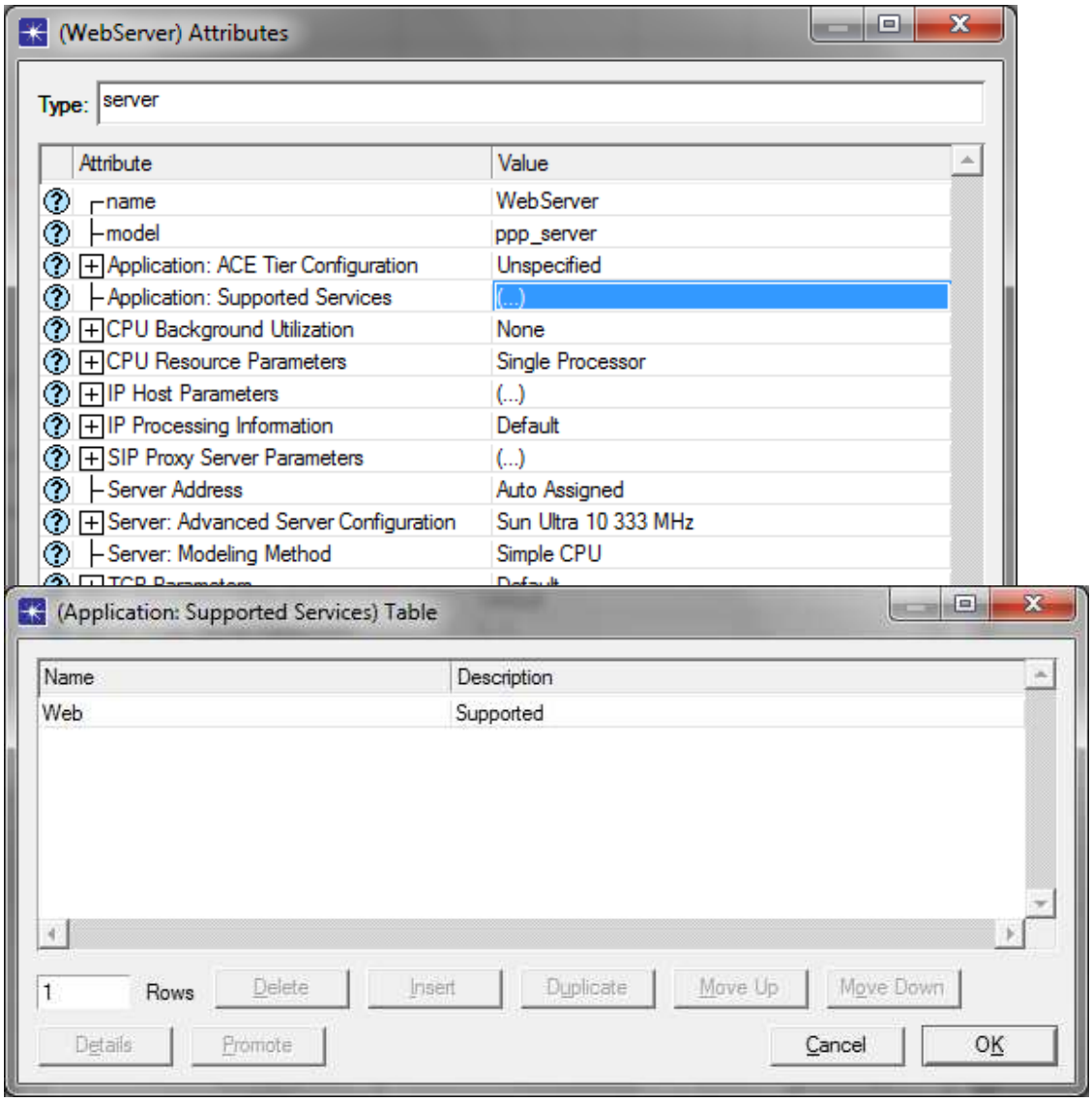


Figure 17: Web Server Configuration on the OPNET Workspace

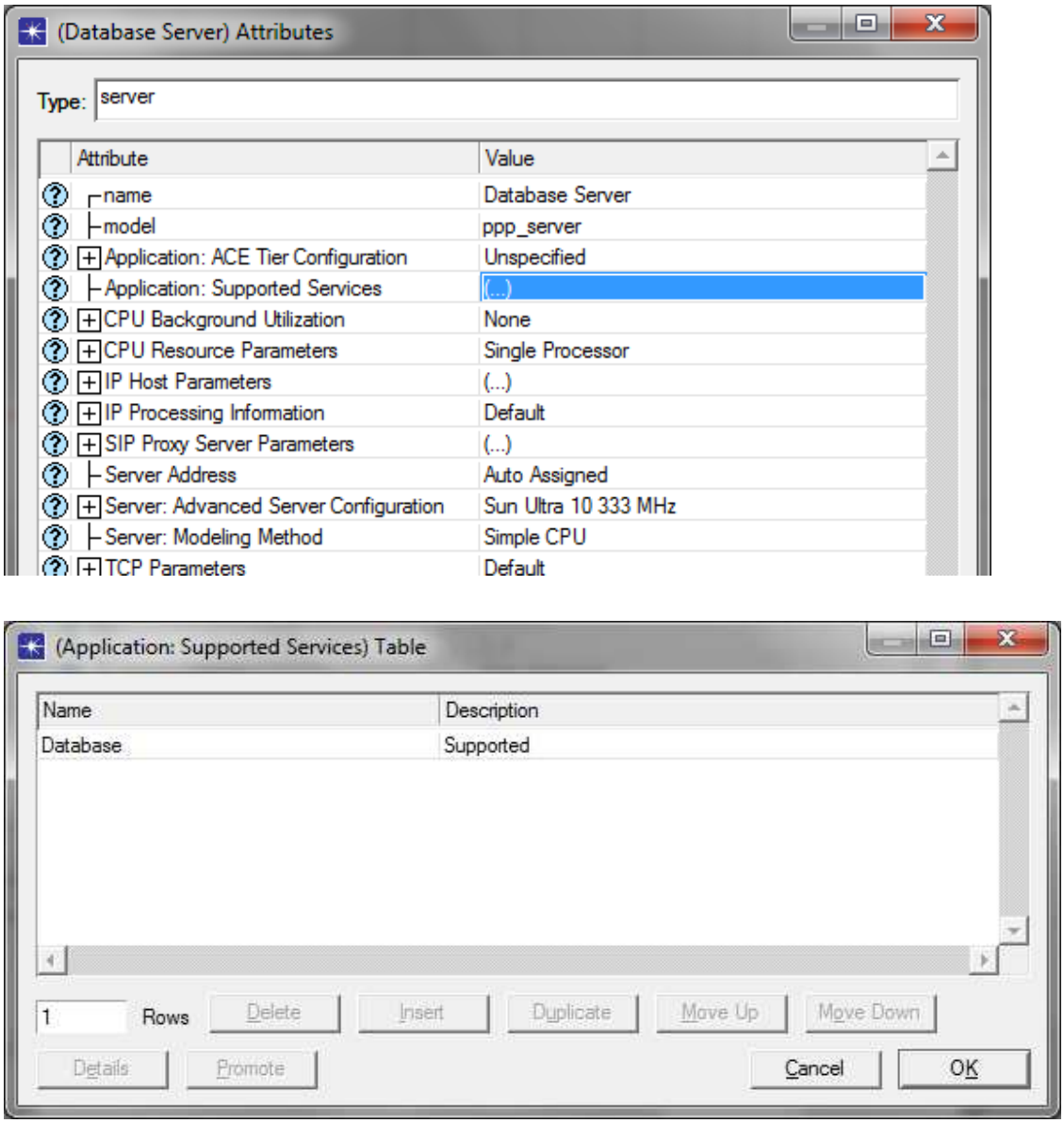


Figure 18: Database Server Configurations on the OPNET Workspace

4.1.6 Cloud Performance Metrics

The configuration of the network is complete. The cloud performance against the database and web applications needs to be evaluated and therefore a few configurations need to be done at the global, node and link levels.

The work space interface showing the levels of performance metrics is shown below:

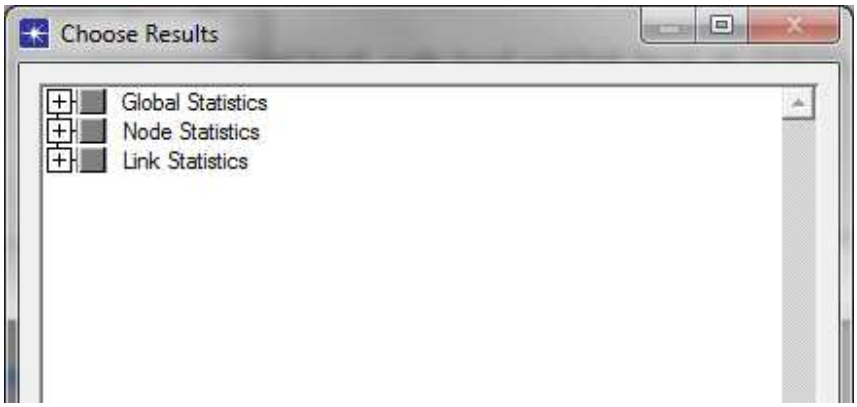


Figure 19: The levels of performance metrics

At the global level, the response time and the page response time of a DB Query and http request respectively are configured where as at the node level, the performance will be measured from the load (requests/second) of both the server DB query and http server request.

At the link level, the point to point link utilization is measured.

The configurations of all the three levels of performance metrics as done on the OPNET network is shown below.

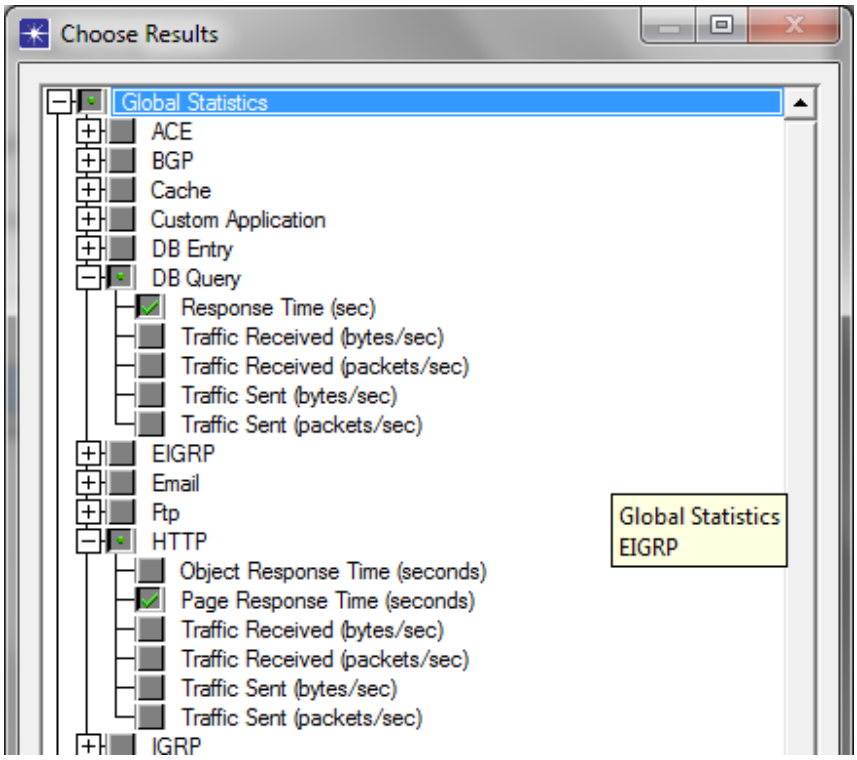


Figure 20: Global Configuration level metrics

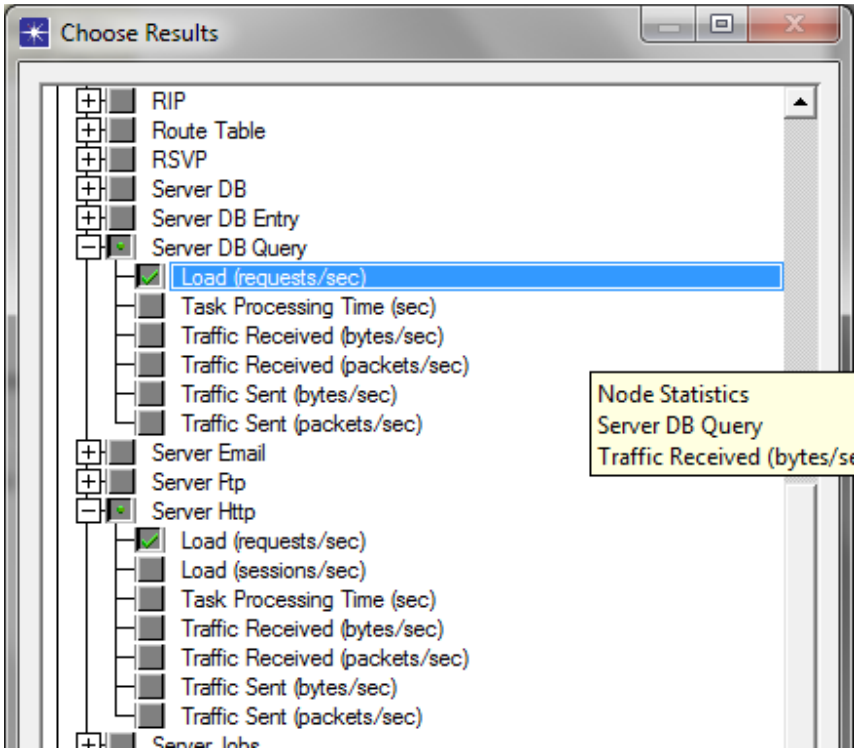


Figure 21: Node configuration level Metrics

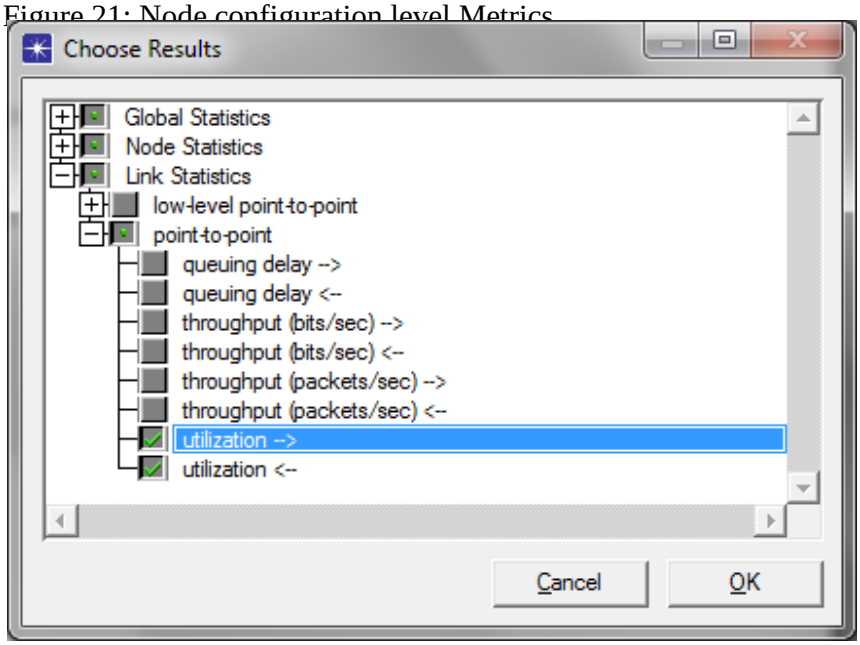


Figure 22: Link configuration level metrics.

This simulation is now completed and the tests proceed after this.

4.2 Simulation of TPA with RSA scenario procedure

This scenario of the TPA with RSA is created by copying the earlier scenario. Its major objective is to enforce the Third Party Auditor policies with a digital signature over the cloud and introduce a digital signature. Packet filtering is done and therefore what is allowed in the network is just the required traffic. The copied scenario option is chosen from the scenarios menu and is shown in figure 23 below:

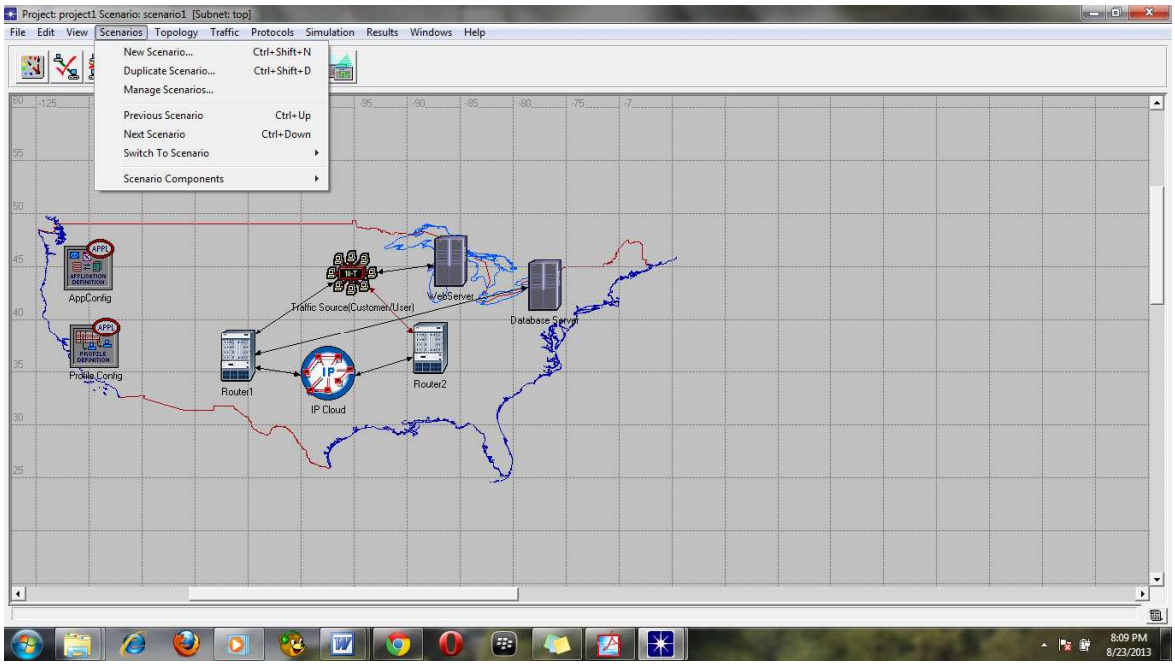


Figure 23: Duplication of a Scenario

The TPA is configured to offer constant latency of 0.05s for both the database and web applications as shown below.

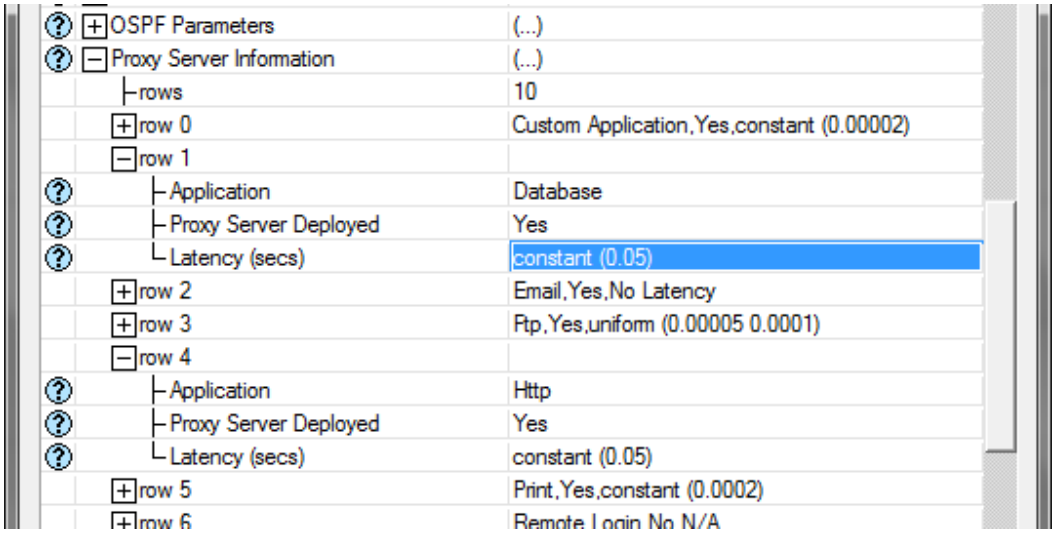


Figure 24: TPA configuration

The TPA will be introduced which in this case to monitor and validate all the network traffic from the Cloud Client.

The TPA will replace Router 2 and the resultant the configurations will appear as below:

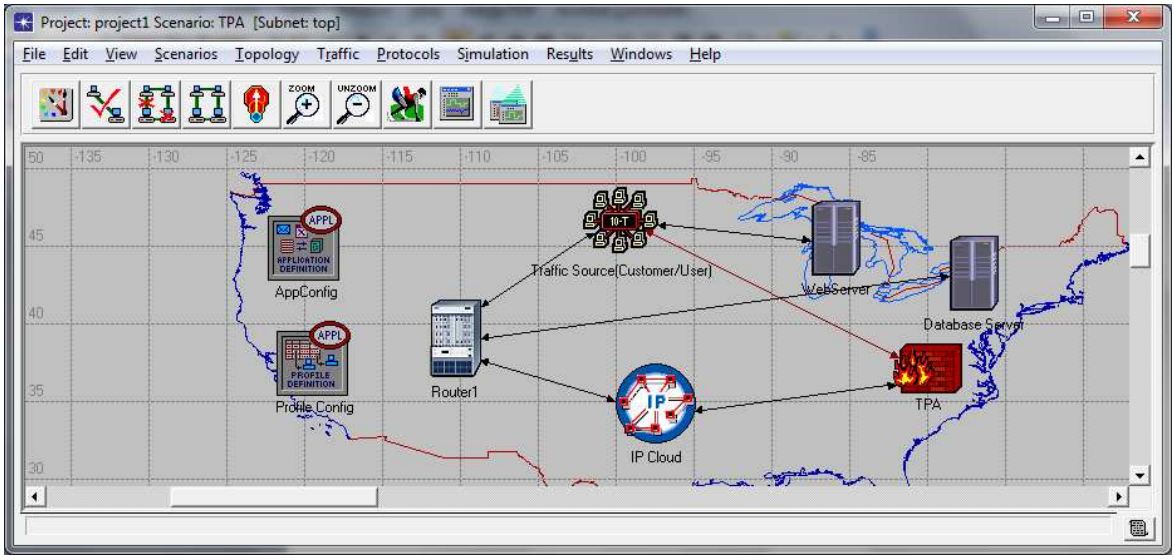


Figure 25: TPA Scenario Setup

4.3 Executing the Simulation

Once the scenarios are setup as described above, the simulation is executed for 60 minutes by choosing the manage scenarios option on the OPNET Tool.

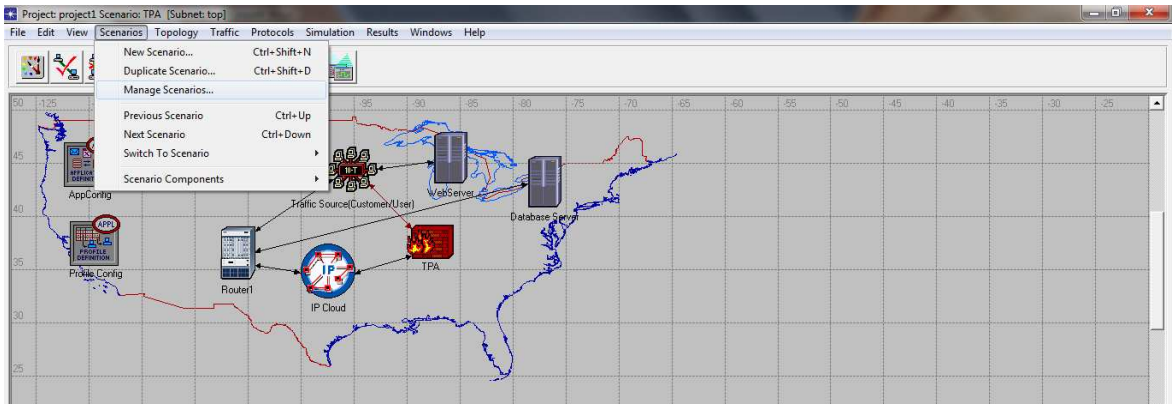
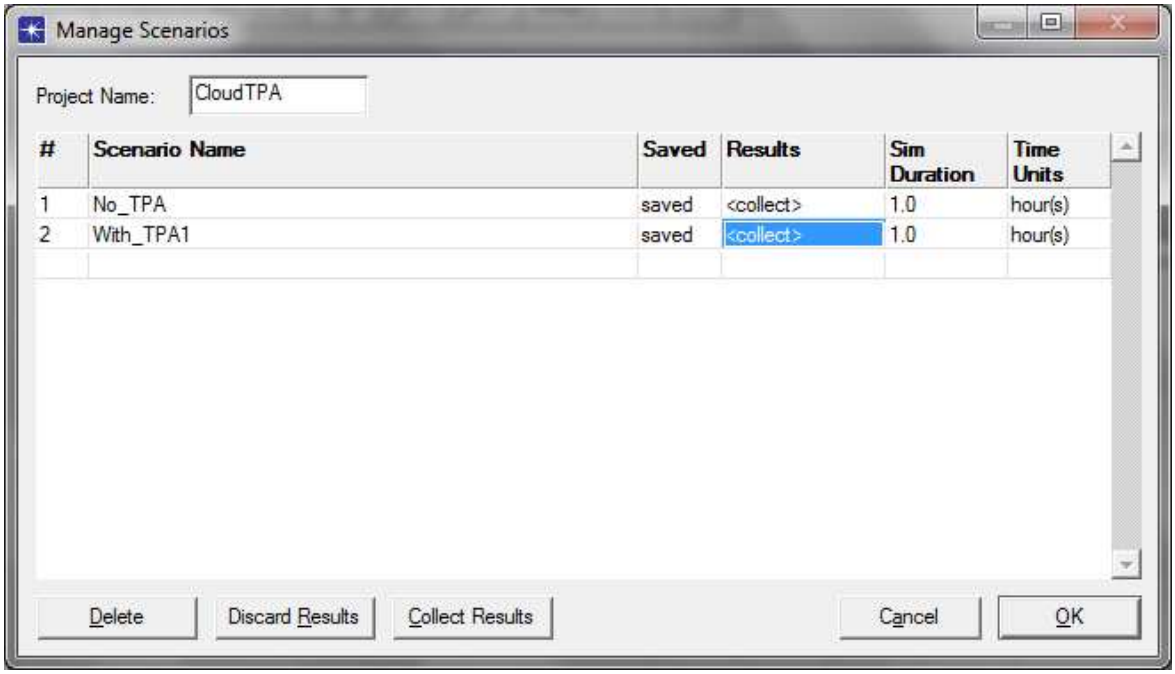


Figure 26: Manage Scenarios screenshots.

The option for the results is marked as collect as shown in the diagram below.



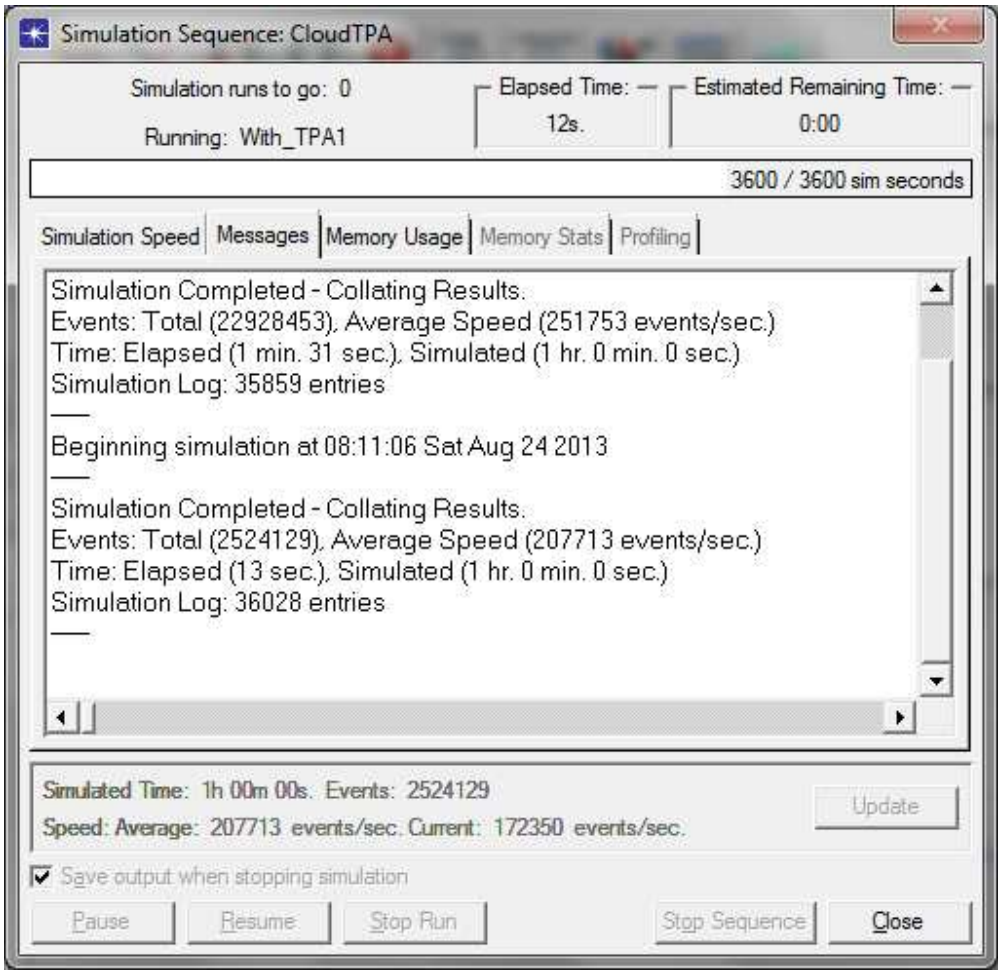


Figure 27: Simulation run for an hour successfully

After one hour the screen is updated as shown in the figure 28 below:

Figure 28: Simulation completed after 60 minutes (one hour).

The evaluation of results is now progressed and is discussed in depth in the next chapter. The scenarios discussed above are then matched up to each other alongside the metrics of performance selected and configured above.

5.0 DATA ANALYSIS AND FINDINGS

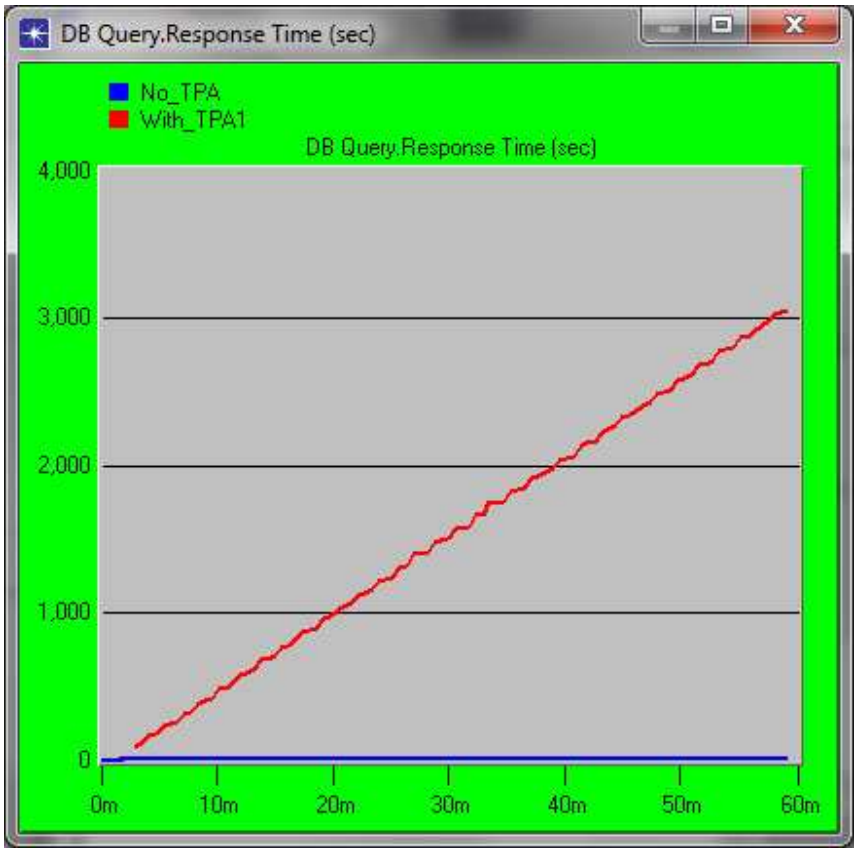
The chapter covers the evaluation of the results once the simulation completes to execute. As stated, a set of two scenarios have been simulated like the one with a TPA and one with no TPA. The performances of the web and database are analysed in this chapter based on the metrics of performance selected at the global level, node level and the link level. The graphs generated are matched up to alongside the metrics and an elaborate evaluation is as provided in the below documentation.

5.1 Database application Results

This part covers the evaluation of the performance of the database application under the two scenarios. First scenario without the TPA and then secondly the scenario where there is a TPA configured for use. The general performance of the database alongside these test scenarios is predicted as per the metrics that were selected and the ensuing graphical representations are given below.

5.1.1 Response Times of the Database query

The response time of a Query for a database process suggests the overall performance of the database. If there are no executions of any security policies or any hurdle to the application traffic across the network, the query response time would be less and definite graph from the project Scenario is as below.


DB Query.Response Time (sec)
No_TPA
With_TPA1
DB Query.Response Time (sec)
4,000
3,000
2,000
1,000
0
0m
10m
20m
30m
40m
50m
60m

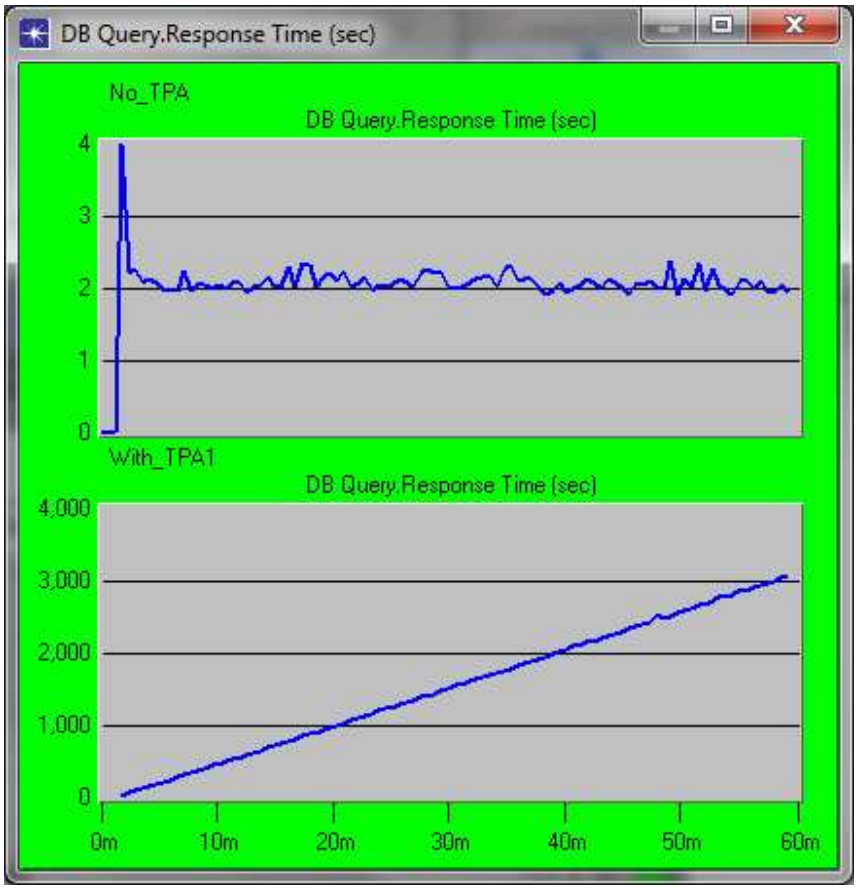


Figure 29: Database response time

The above graphical representation guides us to conclude that the response time is high when the TPA is connected. This is as a result of the constant packet latency that is configured across the TPA network. Since the TPA includes a firewall with a Firewall Service Module (FWSM), there is both filtering, encryption and decryption at this point including packet filtering.

5.1.2 Query Load of the Server DB

The general database server load is estimated in this part. See graph below that deduces the behavior of the database.

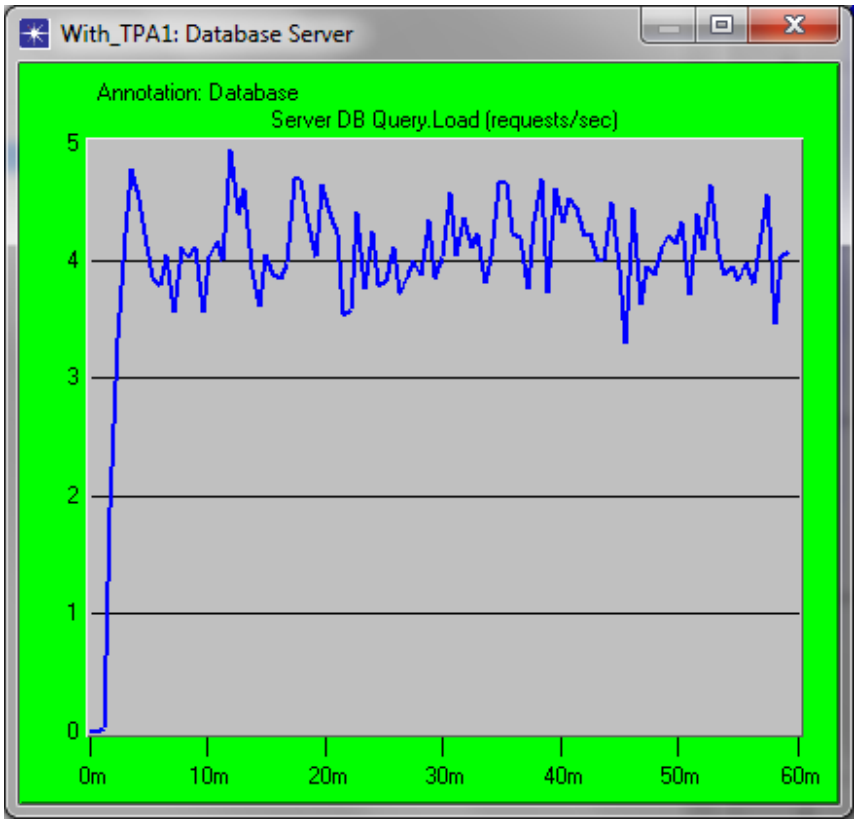


Figure 30: Load on the database server

It can be deduced therefore that when there is no TPA the load is less and hence the low values between the first two or so minutes. The introduction of the TPA increases the network load almost immediately. The database load shown above is the same across the set of two test scenarios. As shown above, this point to the fact that as a result of the extra TPA security policies, some packet delay could be caused as a result of being they are scrutinized and filtered, but this does not in any way affect the overall burden of the server.

5.1.3 Database Server point to point utilization

The general use of the database server across the router points to the application performance against major security issues. The result of the two sets of scenarios is a linear graphical representation as shown in figure 31 below.

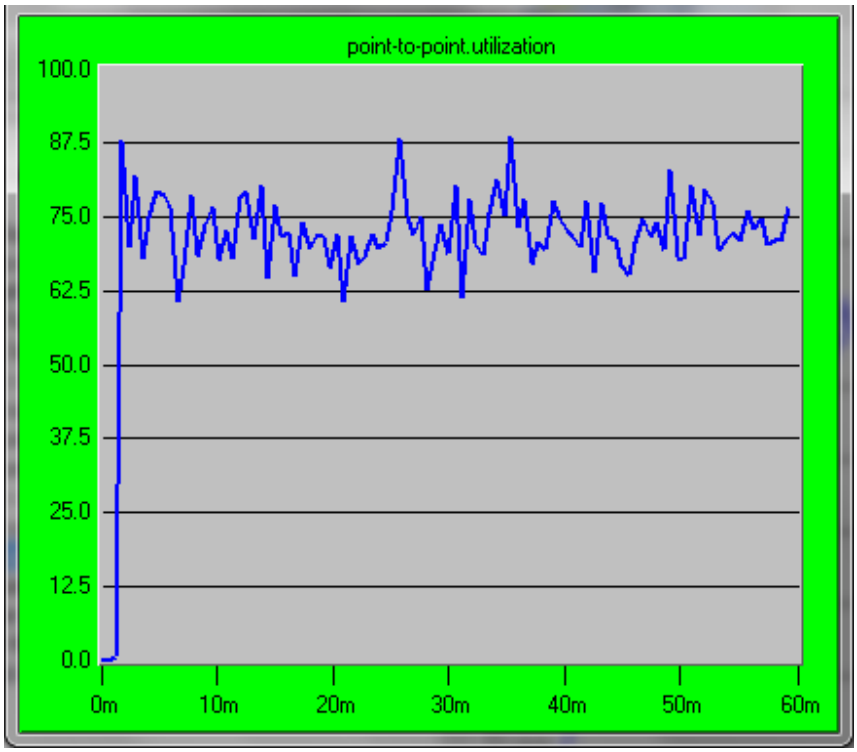


Figure 31: Database point to point utilization.

From the above linear graphical representation, we do anticipate the general usage of the database server is high when the TPA is installed across the cloud. Our deduction from this is that the utilization of point to point is the same when there is no TPA installed.

Theoretically, it should be observed that with no TPA installed, there should be a low point to point utilization to point out that, when there is no filtering and scrutiny of the packets or application of any security policies, the general usage of the server is low.

Therefore it is important to note that the utilization of the point to point of the database server will be higher when the TPA is configured across the cloud.

5.2 The Web Application Results

Simulation of the web application was also executed in this research. The web application's performance was estimated alongside the response time of the web page. Similarly like in the databases' case, a set of two test scenarios were simulated to enable this and an explanation in detail is provided below.

5.2.1 No TPA Scenario - Page Response time

The general response time of the web page when there is no TPA is given below.

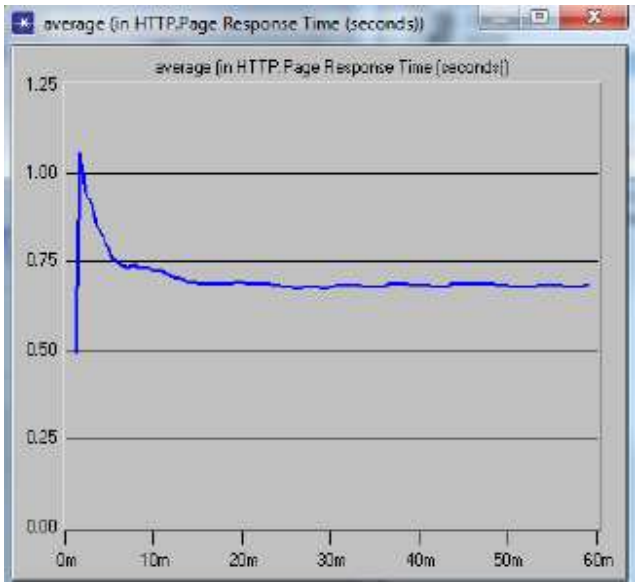


Figure 32: No TPA – web Response time

The linear graphical representation shown above clearly indicates that there is a steady response time when there is no TPA. This can be attributed to the fact that there are no known restrictions of the flow of packets.

5.2.2 Network With TPA - Page response time

When a TPA has been introduced in the setup, the web page response time is described in the linear graph below.

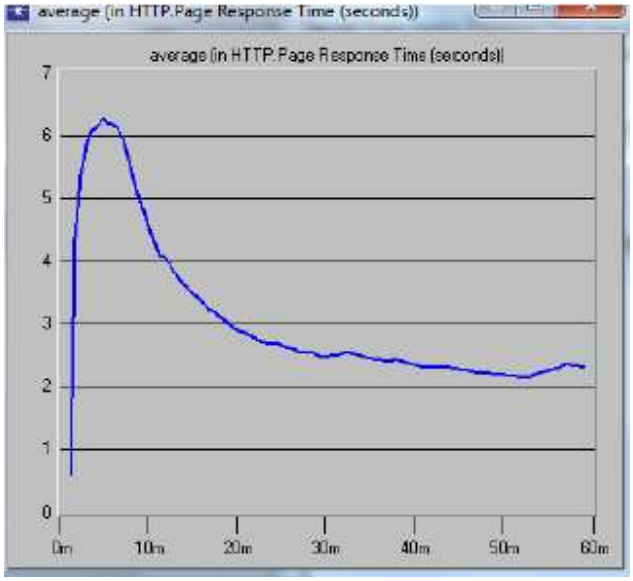


Figure 33: Set up with TPA - Response time

It is clearly depicted from the linear graph that the web page response time is more than that without the TPA. It can also be depicted that it is not constant due to the scrutinizes, restrictions and security policies that have been implemented through the TPA that consequently increase the packet latency. Therefore the page response time increases as the web traffic is being filtered.

5.3 The Cloud Performance

Evaluation based on the above scenarios is done to investigate the performance of the web and the database and a discussion is pursued in the below area of discussion.

5.3.1 Cloud point to point utilization across Router_2/TPA

The general cloud point to point utilization across router_2 and also the TPA is given below:

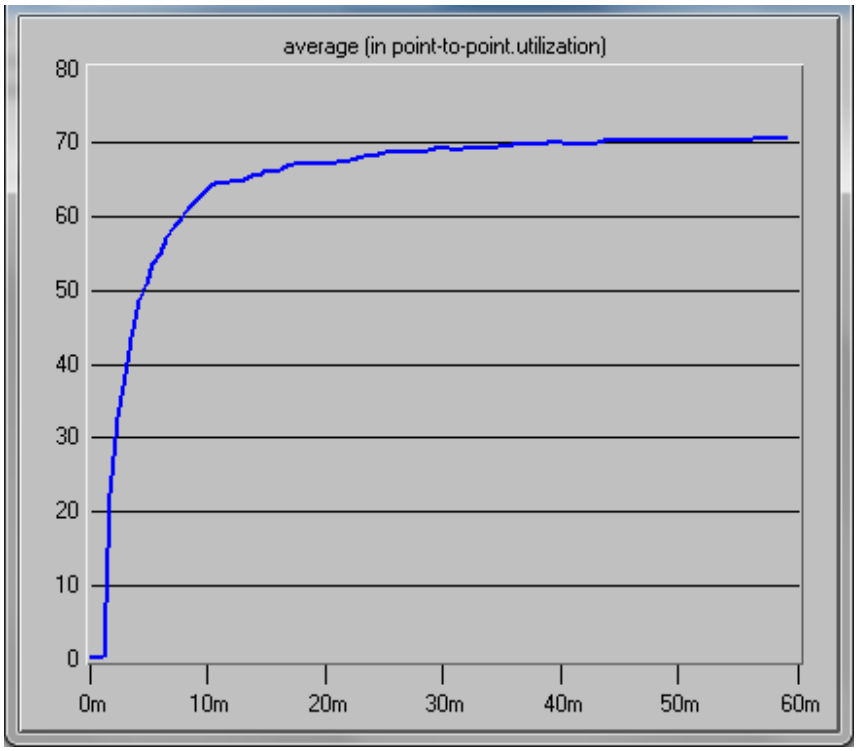


Figure 34: point to point utilization – No TPA

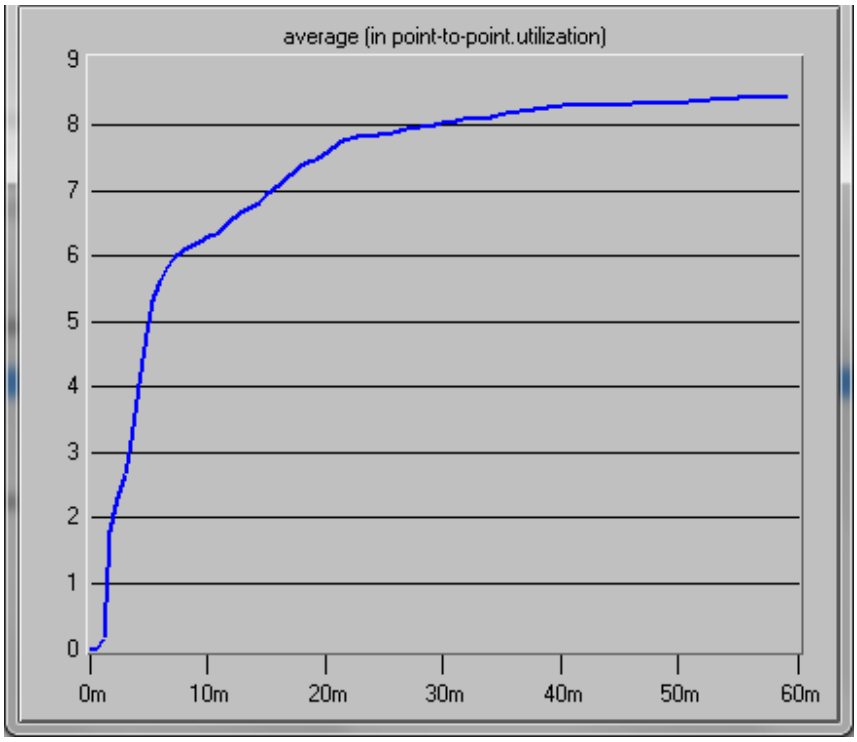


Figure 35: Point to Point Utilization – With TPA

It can be clearly observed from the above linear graphical representations that the general utilization of the cloud point to point is higher with a TPA across the network. The TPA enforces security policies resulting in filtering of the packets and thus results in delays to filtering and consequently, an increment in the cloud utilization.

Similarly, with no TPA, the utilization is also high because the http and database are continuously processed by the cloud. From the general analysis, it can be estimated that the overall utilization of the cloud is able to be increased when the TPA is imposed across the traffic of the web.

We can now deduce that the database and web applications have been improved by the proposed TPA model with security policies including the cryptographic properties. When the TPA security policies are imposed, there is a great deal of improvement of the utilization of the cloud in response to the users and customer queries and requests.

As mentioned 150 users or customers (in this case configured as workstations for simulation purposes) are used. The database application is supported by 50 users and the general utilization of the point to point improves with the introduction of the TPA. The main aim of the research was to improve the overall performance of cloud under the TPA. Heavy browsing across the clouds increases the utilization but a resultant reduction of the performance. This TPA model is designed to limit the traffic of the web and consequently enhance the response of the database querying by the users.

6.0 TESTING

To prove the above results, to the proposed model the number of workstations and the packet latency is changed to test. Two cases are used to prove the results, in the first case the number of workstations is changed to 300 and in the second case packet latency is changed to 0.10.

In this case, the number of workstations is changed to 300 and the latency is increased to 0.10seconds unlike the earlier 0.05. By increasing the number of workstations, the numbers of users in the cloud are also increased. By right clicking on the users and customers icon on the setup in OPNET, the attributes of workstations is changed from 150 to 300. After changing the number of workstations in each scenario, the simulation runs for an hour. The following results are observed:

6.1 Database query response time:

Response time indicates the overall performance of the database application. When there are no TPA the page response time would be very less when compared with the TPA scenario.

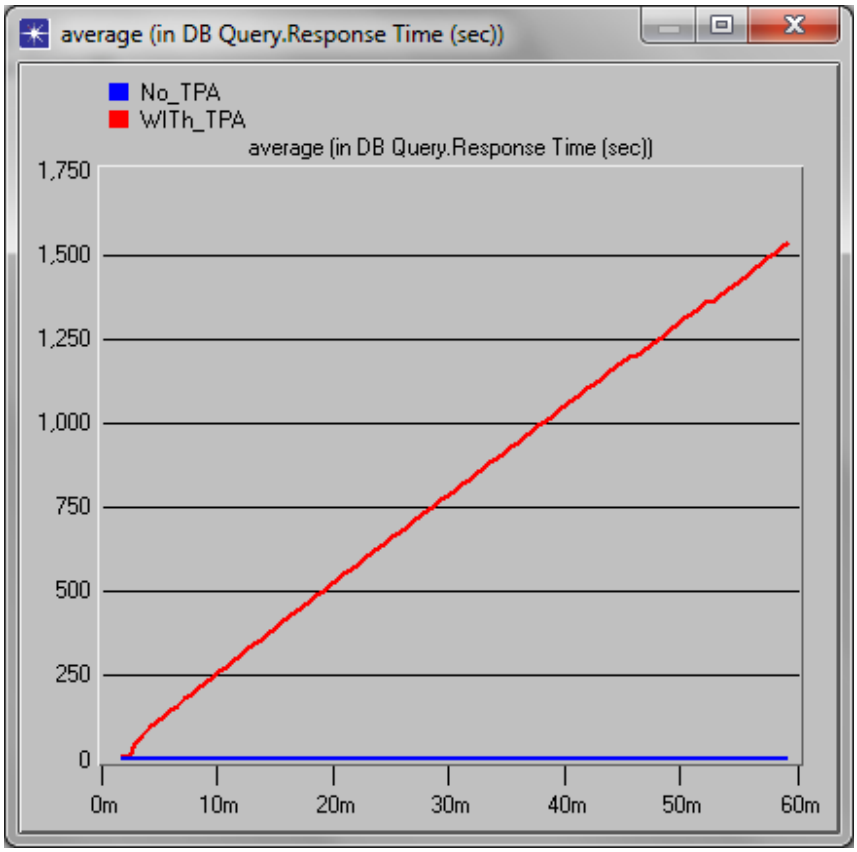


Figure 36: Response time

The above graph indicates that when TPA is imposed, the average response time is very less when compared with other scenarios. As the response time is indirectly proportional to performance, thus it can be stated that there is enhanced cloud performance.

6.2 Query load of the Server DB:

The general server database load can be estimated here. Load on database server at each scenario, when there are 300 workstations can be known from below graph.

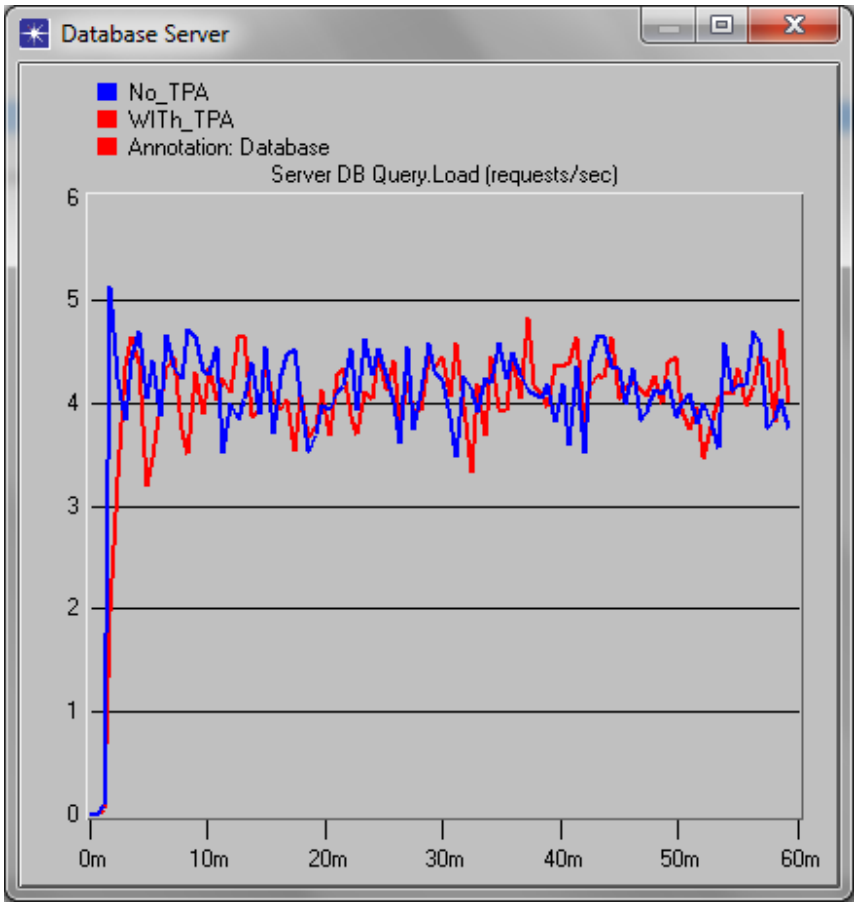


Figure 37: Database server load

Analysis can be done from the linear graph above that with no TPA the load is low as compared to other diagram. The database server load is almost the same in the two sets of test scenarios. Though, with the introduction of the TPA implementation, the situation is different. TPA policies make packets to delay as they keep being filtered. The load on the server is not so much affected.

In general, even if the number of workstations is increased, the same result is observed that is there will be no extra traffic on the database server when the TPA is configured across the cloud.

6.3The Database Server utilization at the Point to point nodes

Utilization of the database server across router_1 indicates performance against key security issues. The graph representing this is as below.

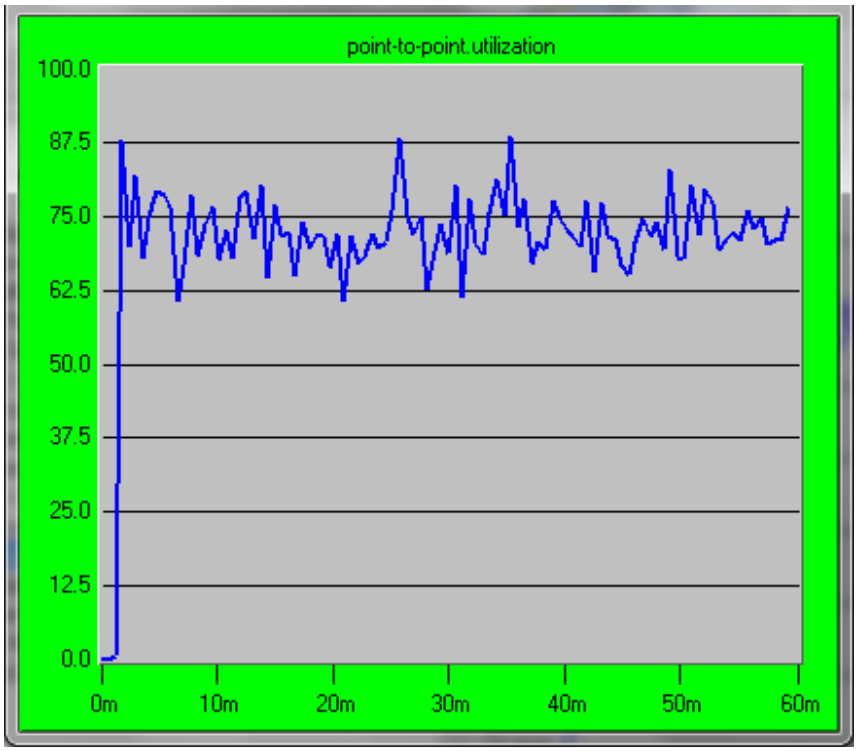


Figure 38: A database server across router point to point utilization

When the number of workstations in this case users or customers is increased and the latency increased, the utilization of the database server is same in all the two scenarios. From the graph, we can deduce the fact database server point to point utilization is enhanced once there is a TPA across the cloud.

6.4 Cloud Point to point utilization across the TPA and Router2

In general the cloud utilization at the point to point node across the router no configuration of TPA is done and when there is a TPA enforced is deduced in the graph below.

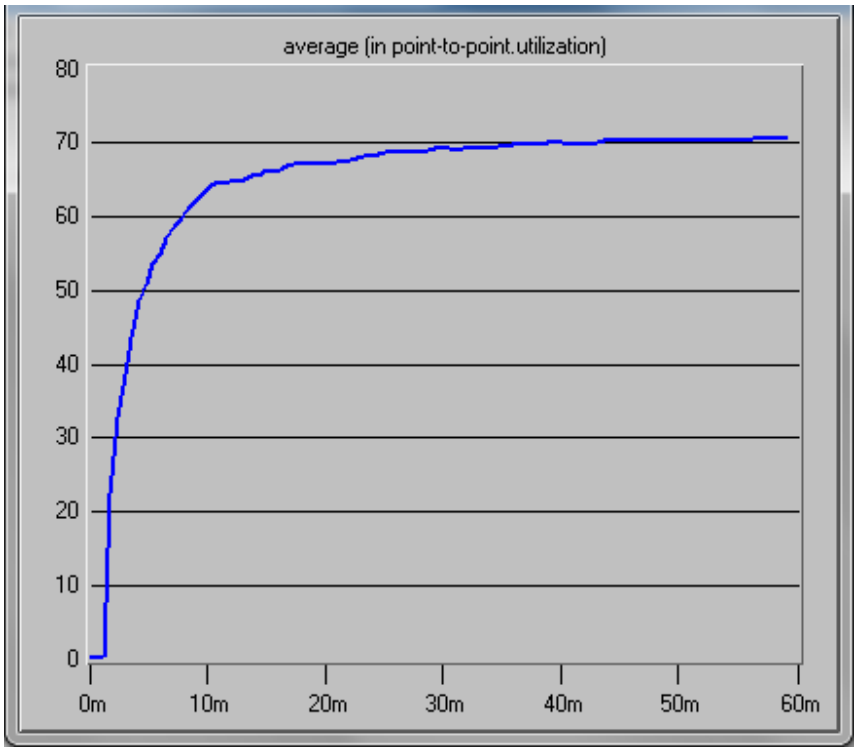


Figure 39: Cloud Utilization (Point to point across the router and TPA)

Even if the packet latency is changed the cloud point to point usage is high when there is TPA across the network. Lack of TPA being configured also leads to a high usage across the cloud as the cloud needs to route the database and the web packets endlessly.

Apart from the above cases, this network is been tested by changing the number of workstations and the packet latency.

7.0 CONCLUSION AND FUTURE WORK

7.1 Conclusion

As we conclude it is important to note that the usage of the web and its components is high and will continue to increase. This will consequently increase the demand for cloud implementation significantly and many banks and financial institutions have now embraced this service for core operations. A huge number of cloud providers are now in the market and have lured many customers to provide this service to them. Kenya's major player in the cloud industry is Safaricom. Most banks are already using their platform to offer various services to their customers. A wide range of services is being offered by the cloud service providers and the major services include database and other services which include software. One key significance of the cloud is that the risk and cost of infrastructure purchase is reduced for the cloud clients and becomes a shared risk. The main advantage with cloud computing is that, the risk of infrastructure maintenance is reduced to the direct parties. The general expenditure and operations cost is also reduced as a result of cloud maintenance costs being low. The advantages are more however, we have several limitations to implementation of the cloud but the main one is the security issue. The data being in a remote site controlled by the cloud service provider, the user has little or no control of what happens to the data at the site. There are several models of security that have been proposed to reduce the workload of the user of having to provide the security of the cloud resources that include the database and web. Some survey literature sources we can deduce the fact that there is no clear model of cloud security that vividly describe the database application performance due to the security rules being enforced over the cloud.

This research provides an evaluation of the database performance with the enforcement of TPA in the cloud. Generally, a TPA being configured to a network leads to the degradation of any application against the sent and received traffic. As a result, we require a substitute model that provides security in order to ensure that applications performances are not affected due to the

unnecessary traffic of the http packets or filtering of packets performed due to the security rules subjected by the TPA.

This research proposes a security model that has been discussed in the earlier sections of this research. From the general investigation of the results the proposed TPA model is well suited for improving the performance of the database application and ensuring only what is required goes through the network. The policies encountered due to the TPA will enable authentication, scrutiny, encryption, and decryption of data. The simulation here describes the behavior of two applications (database and web) under the TPA scenario and one where there is no TPA. About 150 users are used in this case and of this only 50 are used to test the database application. The database performance is in the end improved with the implementation of the TPA setup that enforce the policies and security rules. The objective of the research to enhance the overall performance of the cloud under TPA is achieved. With heavy internet access experienced, the general cloud utilization is realized and increased.

7.2 Future work

This work could be comprehensively done to improve security of data flowing in the cloud domain. Separately, there is still room for other future enhancement and this is highlighted below.

- There is room for other applications that could be put into service to help in the evaluation of the proposed security model.

- The Private and other types of clouds could be implemented in the evaluation of the security model with the aim of improving the security in the cloud significantly.

8.0 REFERENCES

C. Wang, et. Al. “Privacy-preserving public auditing for data storage security in cloud computing,” in *INFOCOM, 2010 Proceedings IEEE*, pp. 1 –9.

JingjingJiang, Dehua Yang, “A Research on Commercial Bank Information Systems Based on Cloud Computing” IEEE Proc. 3rd International Conference Communication Software and Networks (ICCSN), 2011, pp. 1-4.

Avantika Sharma, “Cloud Computing in Banking and Financial Services”, http://www.collabera.com/documents/Cloud_Computing_Banking_and_Financial_Services_PositionPaper.pdf

Zhixiong, John Yoon, “IT Auditing to Assure a Secure Cloud Computing”, IEEE 6th World Congress on Services, 5-10 July, 2010.

G. Ateniese, R. et. Al. “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

G. Ateniese, R.D. et. Al., “ Scalable and Efficient Provable Data Possession,” Proc. Fourth Int’l Conf. Security and Privacy in Communication Networks, pp. 1-10, 2008.

NIST Definition of Cloud Computing v15, accessed on 22/11/2012, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

Auditing the Cloud, accessed on 22/11/2012, http://www.isacaatlanta. org/events/GeekWeek/presentations/DavidBarton-AuditingtheCloud.pdf

Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www.cloudsecurityalliance.org.

Wang C., et. Al. “Ensuring Data Storage Security in Cloud Computing,” July 2009.

Andreas H., “A Case for the Accountable Cloud”, ACM SIGOPS Operating Systems Review, 02, April 2010.

Shah M. A, et. Al “Auditing to keep online storage services honest,” Berkeley, CA, USA: USENIX Association, 2007, pp.1–6.

Gartner: “Seven cloud-computing security risks” http://www.infoworld.com Accessed 22/11/2012.

Pearson S., “Taking Account of Privacy when Designing Cloud Computing Services”, May 23, 2009, Vancouver, Canada.

Kaliski and Wayne, “Toward Risk Assessment as a Service in Cloud Environments”, HotCloud'10 Proceedings of the 2nd USENIX conference on Hot topics in cloud computing, 22-25 June, 2010.
Peter M. et al., “Effectively and Securely Using the Cloud Computing Paradigm”, NIST IT Laboratory, 2009, http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf
Zhu Y. et al., “Efficient provable data possession for hybrid clouds,” in Proceedings of the 17th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2010, pp. 756–758.
http://www.bankinfosecurity.com/avoiding-evil-securing-mobile-devices-a-5251 last accessed 22/11/2012
http://www.bankinfosecurity.com/2-more-banks-are-ddos-victims-a-5298 last accessed 22/11/2012
http://www.bankinfosecurity.com/interviews/top-4-cyberthreats-2013-i-1720 last accessed 22/11/2012
http://docs.bankinfosecurity.com/files/whitepapers/pdf/487_WhitePaper_WeatheringtheStorm_Considerations for Organizations Wanting to Move Services to the Cloud.pdf last accessed 22/11/2012
http://www.bankinfosecurity.com/webinars/perfect-storm-managing-identity-access-in-cloud-w-303 last accessed 22/11/2012
http://www.bankinfosecurity.com/blogs/do-chinese-cloud-mobile-providers-pose-threat-p-1354 last accessed 22/11/2012
Goundar, Sam, “Cloud computing: Opportunities and issues for developing countries” http://archive1.diplomacy.edu/poolbin.asp?IDPool=1335 last accessed 23/11/2012
Bristow R *et al*., (2010) Cloud computing and the power to choose. EDUCAUSE Review 45(3), pp.14–31. [accessed 23 Nov 2012]
Swaminathan K. S. (2008) Computing in the Clouds. The journal of high-performance business AMCIS 2010 Proceedings. Paper 574 [accessed 23 Nov 12].
Gonzalez *et al*. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11 [accessed 23 Nov 2012].

Mell P. and Grance G., “The NIST Definition of Cloud Computing (Draft),” *in Proceedings of the National Institute of Standards and Technology*, Gaithersburg, pp. 6, 2011.

Chandran S. and Angepat M., “Cloud Computing: Analyzing the risks involved in cloud computing environments,” *in Proceedings of Natural Sciences and Engineering*, Sweden, pp. 2-4, 2010.

Pfleeger C. and Pfleeger S., *Security in Computing*, 2nd ed, Prentice Hall, New Jersey, 1997.

Metri P. and Sarote G., “Privacy Issues and Challenges in Cloud computing,” *International Journal of Advanced Engineering Sciences and Technologies,* vol. 5, no. 1, pp. 5-6, 2011.

Shah M., *et al*., “Auditing to keep online storage services honest” *in Proceedings of HotOS’07*, Berkeley, CA, USA, pp. 1-5, 2007.

Kaufman C., Perlman R., and Speciner M., *Network Security: Private Communication in a Public World*, 2nd ed, Prentice Hall PTR, New Jersey, 2002.

Ateniese G., *et al*., “Provable data possession at untrusted stores,” *in Proceedings of CCS’07*, New York, USA, pp. 598-603, 2007.

NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).

P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2009.

Spatarella, J, “Bank Systems & Technology Article: Three Ways to Deter Cyber Crime”: Online Banking Solutions (OBS), 2010

Accenture 2012, The smart banking revolution and emerging business models

Balaji, V. (2012), Cloud Auditing – Making Sure That Your Cloud Works Per Your Expectations

Dawson C., (2002) Practical Research Methods:A user-friendly guide to mastering research techniques and projects, Oxford, United Kingdom.

Harlow, Pearson Education.Govinder, K. INTERNATIONAL JOURNAL OF ADVANCED SCIENTIFIC AND TECHNICAL RESEARCH (ISSUE 2, VOLUME 4-August 2012) ISSN 2249-9954

Lindlof, T.R., & Taylor, B.C. (2010). Qualitative Communication Research Methods (3rd ed.). California: SAGE.

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

TechNet (2012). http://technet.microsoft.com/en-us/video/technet-radio-inside-microsoft-it-how-cios-can-benefit-from-cloud-computing-part-2.aspx , [last accessed 22nd November 2012].

IBM (2010). Building a smatter planet. Http://www.ibm.com/smaterplanet, last accessed on 22nd November 2012.

Pomares W.M.(2011). Explaining the SOA/Rest Impedance Mismatch: SOA Cloud Symposium, Avantica Technologies.

NEC (2010)¸"A Privacy by Design Approach" in *Modelling Cloud Computing Architecture without Compromising Security*

OBS (2010), http://www.reuters.com/article/2010/05/04/idUS140101+04-May-2010+BW20100504 , [accessed 23 Nov 2012].