



# The Impact of Security Configuration on Public Cloud Connectivity

## Citation

Tseng, ChunChao. 2023. The Impact of Security Configuration on Public Cloud Connectivity. Master's thesis, Harvard University Division of Continuing Education.

## Link

<https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374018>

## Terms of use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at

<https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFIOWI2M2EwYTg>

## Accessibility

<https://accessibility.huit.harvard.edu/digital-accessibility-policy>

## Share Your Story

The Harvard community has made this article openly available. Please share how this access benefits you. [Submit a story](#)

# The Impact of Security Configuration on Public Cloud Connectivity

ChunChao Tseng

A Thesis in the Field of Software Engineering  
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

March 2023



## Abstract

Cloud computing technology has brought enormous changes to how the IT industry works over the past few years. As the many cloud service providers (CSPs) are deploying more indispensable and complicated applications, cloud security has also become of paramount importance. However, with more complex and advanced security measures in place, connectivity has also become an increasingly important issue. In this project, we examine cloud technology and security and evaluate how public cloud performance is affected by different security configurations that are often deployed in the cloud environment in a real-life scenario.

## Dedication

To my incredible parents, ChingKun, YuYing, my sister Elsa, and all the friends who supported and encouraged me during this journey.

## Acknowledgments

I am fortunate to study and work with members at Harvard; it has been an incredible and wonderful journey in my life. I am grateful to my thesis director Jose Ramirez and research advisor Dr. Hongming Wang, who provide thoughtful advice and guidance, and have always been patient and passionate during my research.

I would also like to thank and recognize my loving parents and my dear sister. This journey is meaningful because of their company. Without my family and their steadfast support, nothing would be possible.

Finally, I want to thank and acknowledge all the friends who have supported and encouraged me, this unbelievable journey is complete because of their support.

## Table of Contents

Abstract .....	iii
Dedication .....	iv
Acknowledgements .....	v
Table of Contents .....	vi
List of Tables .....	viii
List of Figures .....	ix
Chapter I. Introduction .....	1
Chapter II. Background .....	2
2.1 Cloud Computing .....	2
2.2 Cloud Security .....	7
2.3 Security Configuration .....	9
2.4 Research Problem .....	13
2.5 Related Work .....	14
Chapter III. Methods .....	18
3.1 Computation and Specifications .....	18
3.2 Experiments .....	27
Chapter IV. Results and Discussions .....	36
4.1 Data Analysis .....	36
4.2 Comparison and Discussion .....	49

Chapter V. Conclusion .....	54
References .....	57
Appendix 1. Glossary .....	68

## List of Tables

Table 4.1 Test Results of Condition 1 .....	37
Table 4.2 Test Results of Condition 1a .....	38
Table 4.3 Test Results of Condition 1b .....	39
Table 4.4 Test Results of Condition 1c .....	40
Table 4.5 Test Results of Condition 2 .....	41
Table 4.6 Test Results of Condition 2a .....	42
Table 4.7 Test Results of Condition 3 .....	43
Table 4.8 Test Results of Condition 4 .....	45
Table 4.9 Test Conditions Comparison .....	46
Table 4.10 Test Results of All Conditions .....	47

## List of Figures

Figure 2.1 Cloud Firewall .....	11
Figure 2.2 Cloud Load Balancing .....	12
Figure 3.1 Instance Group Configuration1 .....	20
Figure 3.2 Instance Template Configuration1 .....	21
Figure 3.3 Instance Template Configuration2 .....	22
Figure 3.4 Instance Group Configuration2 .....	24
Figure 3.5 Autoscaling Configuration .....	25
Figure 3.6 Virtual Machine Configuration1 .....	26
Figure 3.7 Virtual Machine Configuration2 .....	27
Figure 3.8 Architecture Diagram of the Cloud Environment .....	29
Figure 4.1 Comparison of Test Results under Different Test Conditions .....	48
Figure 4.2 The Mechanism of Cloud Load Balancer .....	49

## Chapter I.

### Introduction

Cloud computing represents the realization of the concept that by sharing the infrastructure, platform, and software in the cloud environment, users can utilize the resources, including computing, storage, and other advanced products, with optimal configuration and cost. Cloud computing technology also enables the user to concentrate on the application and minimize the cost of managing and maintaining the infrastructure or platform on which the application deploys.

In this thesis, we provide the background on cloud computing needed to help anyone understand general concepts, and also include the models, characteristics, and different aspects of cloud security and the concepts of identity and access management (IAM), generally used to control the security in the cloud environment. We also review the literature to give readers an overview of why cloud computing and security are critical issues. How does cloud security work to protect the cloud environment, and how might it affect connectivity on the public cloud?

Our experiments are designed to test how various security configurations and specifications might impact connectivity and performance. We discuss the results of these computational experiments, how they might affect the use of the cloud environment and how this might be related to applications in actual practice. We also discuss the implications for future research.

## Chapter II.

### Background

#### 2.1 Cloud Computing

Cloud computing has changed the way people access information as well as the way the IT industry works. Instead of accessing on-premises hardware and resources, by sharing the resources on public infrastructure and platforms, cloud computing enables users to share the resource on different types of clouds and applications, thus creating new ways of utilizing the cloud computing resource. The main characteristics, service models, and deployment models of cloud computing are listed below (Mell & Grance, 2011) (Ali et al., 2015).

The following characteristics can describe cloud computing:

i. On-demand service

Users are capable of unilaterally accessing available cloud services, such as server time and network storage, on an as-needed basis and without intervention from the Cloud Service Providers (CSPs).

ii. Broad network access

The capabilities and environments deployed on the cloud must be broadly accessible to the end-users from different or heterogeneous environments. (e.g., laptops, mobile devices, and workstations, etc.)

iii. Resource pooling

CSPs provide provisional or scalable cloud resources to serve multiple independent users by sharing/pooling the resources in a multi-tenant model. Thus the physical or virtual resources such as computing, storage, memory, and network bandwidth can be dynamically assigned or reassigned according to user demand.

iv. Rapid elasticity

Cloud capabilities can be elastically or automatically provisioned and released; users are also able to scale up/down the applications deployed on the cloud automatically based on the demand. Cloud resources often appear unlimited and can be appropriated in any quantity at any time. Elasticity is also one of the main features of cloud computing which can dynamically adjust the amount of allocated resources to the changing workload (Al-Dhuraibi et al., 2017).

v. Measured service

The cloud services (e.g., computing, storage, network bandwidth) can be dynamically measured or optimized based on the cloud metering configurations. Resources usage can also be monitored, controlled, reported, or monetized for both users and service providers.

Cloud computing can generally be categorized into three different service models. Different models construct the correspondent management responsibility called Shared Responsibility Model, and various service level agreements (SLAs) are defined and provided by the CSPs (Birje et al., 2017) (Sun, 2018).

i. Infrastructure-as-a-Service, IaaS

Cloud service providers provide public infrastructure for users who pay for the infrastructure resources and develop their own platforms or software.

The user controls the application, storage, network, operating system, and other fundamental computing resources. The IaaS model provides the user the more adaptability than the other models, including PaaS and SaaS. In contrast, the user also takes more responsibility for maintaining, managing, and operating the user's own cloud computing environment.

ii. Platform-as-a-Service, PaaS

Cloud service providers provide a public platform where users can develop their own software and pay for the platform resources. The users do not oversee or control the underlying cloud framework, including network, servers, storage, and operating system, yet have control over the application facilitating environment arrangement and management.

iii. Software-as-a-Service, SaaS

Cloud service providers provide public software that users can directly use and do not need to configure the underlying framework, including system, servers, network, operating system, and storage. Cloud service providers or other third parties develop the software on the cloud.

Deployment models refer to the form the cloud computing environment is defined, arranged, operated, and regulated. The models can usually be categorized into

four models. Each model provides different scalability, reliability, security, and cost (Etro, 2015); the following are the four models and their features:

i. Private cloud

The infrastructure of the cloud is provisioned exclusively by a single organization, and may be owned, managed, and operated by the organization, a third-party, or a combination thereof.

ii. Public cloud

The infrastructure of the cloud is provisioned for open use by the general public, it may be owned, managed and operated by a business, academic, or a governmental organization.

iii. Community cloud

The infrastructure of the cloud is provisioned by a specific community of users from organizations with shared concerns.

iv. Hybrid cloud

The infrastructure of the cloud combines two or more of the distinct deployment models above, which remain unique entities but are bound together by standardized or proprietary technologies.

In general, cloud computing represents the concept of a parallel and distributed system of a series of virtual machines that can dynamically allocate resources (Namasudra, 2017) (Basu, 2018). Over the years various technologies are developed to support the realization of the concept, such as virtualization, grid computing, and service-oriented architecture (Puthal et al., 2015) (Ibrahim et al., 2016). These technologies bring enormous advantages to the cloud computing such as agility, availability, flexibility, and

cost efficiency. Meanwhile, different issues also emerge and become of concern to the users, along with the fast growth of cloud computing. The main issues include

(Namasudra, 2017) (Parikh et al., 2019):

i. Security and privacy

Various threats, such as social engineering, hacker attack, and unauthorized or malicious access to the cloud environment or the data on the cloud.

ii. Transferability

The data stored on one cloud might not be easily transferrable to another one due to technical or business restrictions, which can also be used as a way of lock-in to prevent user transfers under normal conditions.

iii. Downtime

The resources of the cloud might still encounter certain situations in which the CSPs cannot provide full service of the cloud, even under the predefined SLAs.

iv. Limited Control:

Users might have limited control over the resources on the cloud, which is usually not limited to the CSPs, but also from the 3<sup>rd</sup> party service or solution providers.

Among the main issues, those most discussed and concerned are regarding security and privacy, and can be further listed below (Namasudra, 2017):

i. Confidentiality

Confidentiality refers to the status that the data stored or transferred in the

cloud can be kept secure and secret. Different levels of sensitive data should be secured by different levels of security measures such as cryptography (Almorsy, 2016).

ii. Access control

Access control that ensures only authorized and authenticated users or parties can access the corresponding information in the cloud by setting the configuration such as Identity and Access Management (IAM) (Gupta et al., 2020) (Hussein & Khalid, 2016).

iii. Data and storage-related issues

The integrity and availability of the data stored, transferred, and computed in the cloud must be kept secure and complete. Related measures include data segregation, data loss prevention, and data recovery is the standard way to protect the data and secure storage (Hashizume et al., 2013).

In this thesis, we concentrate on the issue of cloud security, including the background, type of cloud security, and typical configuration to maintain the cloud security.

## 2.2 Cloud Security

The transition from local computing to cloud computing has brought numerous advantages to users and cloud service providers. However, due to the expanding scale of the global cloud network environment, cloud security has also become a significant issue in the cloud computing environment for both consumers and providers (Singh & Chatterjee, 2017). Despite the convenience and flexibility of cloud computing, various

implementations derived from the cloud still encounter security concerns from different aspects (Zhe et al., 2017). In the description below, cloud security is categorized into three dimensions and discussed accordingly: computer security, network security, and information security (Sun, 2018).

Computer security refers to a broad concept of the computer system's protection and security system in the cloud environment. Many aspects must be considered such as trusted authentication, appropriate authorization, data security, and privacy (Arora et al., 2017). Cloud security also covers almost all the layers in the cloud system. Typical attack types include Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS), clickjacking, eavesdropping, spoofing, social engineering, tampering, privilege escalation, and back doors attacks are familiar to computer security (Srinivasan et al., 2012).

Network security represents the main issues of all network-oriented attack types that overlap with computer security. Common network-oriented attacks include a virus, eavesdropping, DoS attack, spoofing, Smurf attack, man-in-the-middle attack, ARP poisoning, buffer overflow, heap overflow, SQL injection, phishing, and cross-site scripting (Schneider, 2012).

Information security concentrates on the issues in which information is stored, transferred, managed, and operated in a cloud environment. The main aspects of information security are identity management and privacy protection (Radwan & Abdelbaki, 2017).

The cloud environment is a complex virtual environment of infrastructure, with a huge amount of traffic flowing inside the physical hardware, the complexity in the virtual

environment also increases (Zhang et al., 2011) (Indu et al., 2018). From the three cloud security dimensions and the corresponding large amount of services and data in the cloud environment, as a result, security risks in the cloud environment are created, and the real challenge comes from adapting the proper and pre-emptive protection (Khan, 2016) (Zeng & Germanos, 2019).

Cloud security is a dynamic, complex, and complicated issue at the core of cloud technology, therefore various countermeasures are proposed and applied to the corresponding type of threat (Almulla & Yeun, 2010). In the following section, we discuss the typical security configuration usually used as the fundamental protection to cloud resources (Kandukuri & Rakshit, 2009).

## 2.3 Security Configuration

### 2.3.1 Identity and Access Management

Among the security methods, access control or Identity and Access Management (IAM) can be defined as the method which provides an adequate level of protection for organization resources and data through rules and policies (Riti, 2018). IAM provides fine-grained access control over all of a specific cloud environment and prevents access to other non-authorized resources (Tabrizchi & Kuchaki, 2020). With IAM, users can specify “who can access which services and resources, and under which conditions” (AWS, 2021). The configuration of IAM is also not restricted to the organization’s resources and provides protection to users’ information and actions. It also provides access control based on the role of the user, which is generally categorized as role-based access control (RBAC) (Zhou et al., 2015). IAM can be considered as a set from three aspects (Almulla & Yeun, 2010):

First, authentication in cloud computing controls the process of verifying the identities of the users and the systems (Rana et al., 2017). Despite normal single-factor authentication (SFA), to increase the security level and decrease the possibility of the system being compromised, multi-factor authentication (MFA) is also a common procedure nowadays in applications with which the user must provide more than one authentication source to be authenticated (Mohammed, 2019).

Second, authorization represents the process in which the users or systems are authenticated, and this process determines the privilege of accessing resources granted to legitimate parties (Naik & Jenkins, 2016).

Third, auditing is the process to monitor and track the record of users or systems that are granted access to the resources in the cloud environment. The process of auditing is activated in order to review, record and check whether compliances with the predefined security configurations and policies (Moura & Hutchison, 2016).

### 2.3.2 Firewall

A firewall is generally a set of network restrictions or rules to restrict the traffic to the cloud resources, which offers limited access to the cloud environment (Yu et al., 2013). Based on the firewall rules, the traffic or packets that can access the cloud from the local network is restricted to either pass or drop, which constructs one of the fundamental protections to the cloud environment (Khakpour & Liu, 2012). A typical firewall operates on the protocol of the network, such as TCP or IP, however these firewall rules can nowadays be too simple to protect the cloud environment from

complex threats, therefore different firewall rules and frameworks are developed and applied in the current cloud environments (Bhushan & Gupta, 2017).

The firewall also works as an architecture to offer different cloud on-demand services, this includes the risk of network access control, service type, and security level (Chen et al., 2017). Different list-based filters are also developed to block malicious attacks or service requests (Sqalli et al., 2011). In addition, more types of firewall products protect the cloud environments in different frameworks (Bhadauria et al., 2011) (Subashini, 2011).

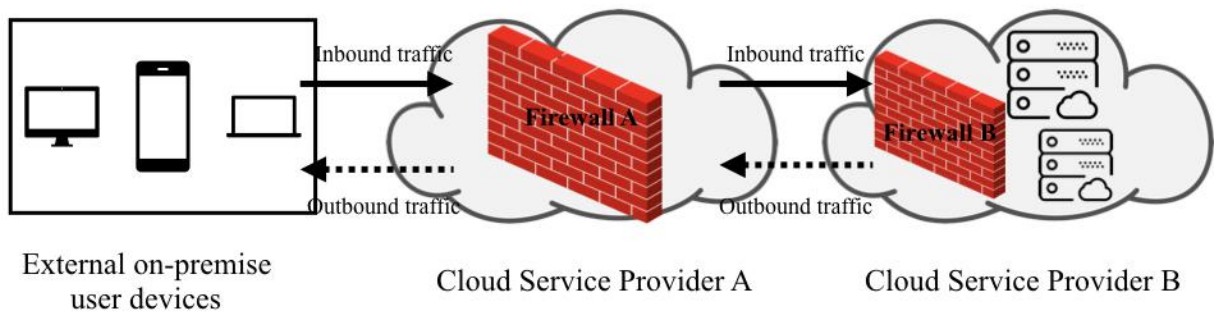


Fig 2.1 Cloud Firewall

*In the cloud environment configured and protected with a firewall, the inbound traffic from external on-premises devices has to be checked and allowed when the inbound firewall rules are met. The same mechanism exists between different cloud service providers that operates different application and stores different data. The outbound traffic from servers of the cloud service provider also has to meet the outbound traffic rules to allow the egress traffic (Sheng et al., 2016).*

### 2.3.3 Load Balancing

Load balancing is the technology of dividing the workload that an instance in the cloud has to process between more instances. Therefore the workload can be separated, while increasing the process speed and efficiency as well as optimizing the utilization of the cloud resources (Coutinho et al., 2015) (Kanakala et al., 2015).

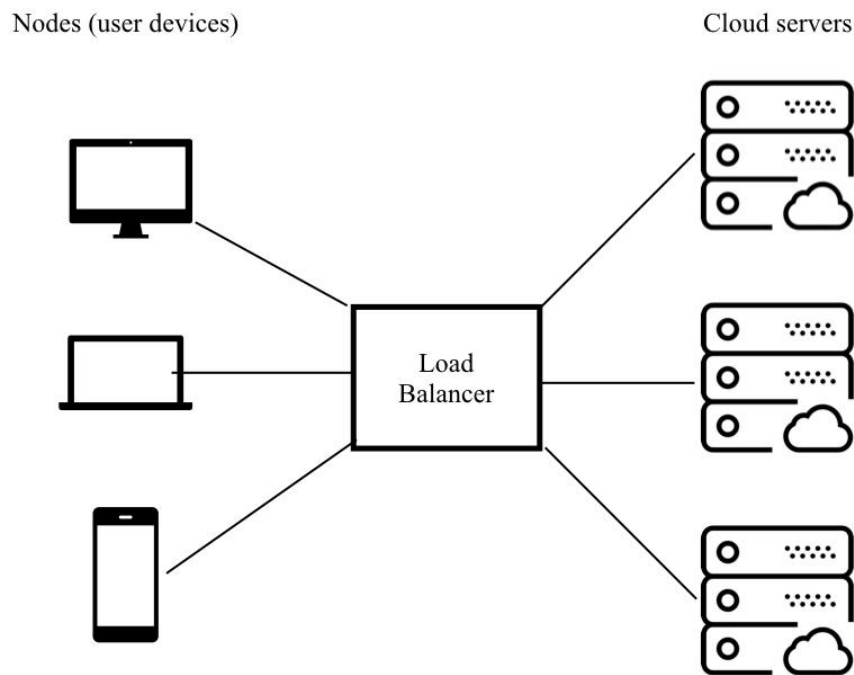


Fig 2.2 Cloud Load Balancing

*Load balancing in the cloud environment is performed by a load balancer in the cloud. The cloud load balancer receives the requests and traffic from the nodes (end user devices), then distributes the workload to the instances or servers in the cloud. In this process the goal of load balancing is to optimize resource utilization, increase throughput and user satisfaction.*

The purpose of load balancing is to evenly distribute the instant or massive amount of workload to different instances or nodes (end user devices). The main characteristics of load balancing include: equal division of workload across nodes, achieving higher user satisfaction, reducing response time, and improving the overall performance of the cloud system (Aslam & Shah, 2015) (Khare & Deen, 2022). On one hand, for a cloud environment, load balancing increases cloud resource utilization, improves throughput, and also avoids resource overload. On the other hand, for the nodes or end-user devices, load balancing improves response time and user satisfaction (Kumar et al., 2018) (Kumar & Kumar, 2019).

The metrics of load balancing comprise of several parameters such as resource utilization, performance, scalability, throughput, response time, and associated overhead (Deepa & Cheelu, 2017). Due to the purpose of optimizing the massive workload in the process, we take this characteristic as one of the countermeasures against DDoS, which is also one of the most critical and standard security configurations in a cloud environment in real practice (Jia et al., 2014).

## 2.4 Research Problem

Cloud computing has become a critical technology and indispensable resource in various industries and research fields. It represents a new business model and computing paradigm (Xiao & Xiao, 2012). Offering dynamically scalable resources on public infrastructure and platforms, cloud computing enables users to share the resource on different types of clouds and applications, also reducing capital expenditure (CapEx) and operational expenditure (OpEx) (Jensen et al., 2009). While ever-increasing applications

are developed, operated, and managed on the cloud, cloud computing has brought many security issues and challenges for both consumers and providers (Singh & Chatterjee, 2017).

To maintain the security of assets on public clouds, many technological methods contributed to better security performances in the cloud, but there are still no perfect solutions (Sun et al., 2018). This project will focus on security and its impact on the connectivity of public clouds. By measuring the connectivity under different security configurations, we attempt to find the optimal security configuration that can provide necessary protection to the assets on the cloud while not affecting the connectivity.

In order to keep the digital assets on the public cloud secure and accessible only to authenticated users, different security configurations are applied to the cloud environment. We further develop a cloud testing environment to measure the connectivity in the cloud in response to the different levels of security configurations and the time needed to connect to the cloud.

## 2.5 Related Work

The questions on cloud computing and its security have been studied by many researchers from different levels and perspectives, and more derivative questions are also being studied along with the rapid growth in the demand for cloud computing and applications thereon (Joshi & Wornell, 2017).

### 2.5.1 Cloud computing

Cloud computing can be traced back to the concepts of Remote Job Entry (RJE) in the 1960s, and it has been a fast-evolving field for academics and business in recent years (White, 1971) (Armbrust, 2010). The concept of cloud computing has been studied from a wide variety of aspects, including academic, technical, commercial, and even legal or regulatory ones (Kumar & Goyal, 2019). From a technical point of view, the unprecedented and innovative way to manage the resources in the shared infrastructure and platform, cloud computing can generally refer to the applications delivered as services over the internet and the hardware and systems software in the data centers that provide those services (Armbrust, 2010).

Technically deconstructing the components of cloud computing, it is essentially a combination of existing technologies of multiprocessor, visualization technology, network based distributed data storage and networking (Behl, 2011). Among these technologies, state-of-the-art artificial intelligence and machine learning technologies are also being integrated into cloud native technologies as a trend in various applications (Surya, 2018). The process of accessing the cloud computing resources is a consequent and intertwined series of information transmission from a network, computing resources, data storage, to visualization, to authorize and authenticate the information to the corresponding counterpart for processing. Security configuration is hence designed to control and manage data transmission (Ren, 2012).

### 2.5.2 Cloud security

Cloud security is an essential issue in the distributed system of cloud computing, it represents the threat from a range of technical, social, and legal challenges; thus careful

consideration must be taken before entering into cloud systems (Wood, 2010) (Sadiku et al., 2014) (Sen, 2015). To identify the technical challenges among the cloud security threats, an aggressive attack model can be constructed, analyzed and used to evaluate any security mechanism (Huang, 2015). In the attack model, the cloud security properties must first to be defined as the target, such as confidentiality, integrity, availability, and contractual security. These properties are the general target of an attack on a cloud environment, and the source who attacks can generally be categorized into malicious CSP and malicious cloud user (Mushtaq et al., 2017). In the attack, the techniques include storage manipulation, storage monitoring, VM image sharing, compromised hypervisor, storage dishonesty, and location dishonesty (Huang, 2015) (Chang et al., 2016).

To protect the properties and secure the resources in the cloud environment from the above-mentioned techniques, users must take security measures and set up security configurations for the cloud environment (Samarati et al., 2016). The common ways and mechanisms to protect the assets include encryption mechanisms, system mechanisms, and access control mechanisms (Huang, 2015) (Coppolino et al., 2017).

Encryption is a complicated research topic, which will not be discussed in this research. This research focuses on the security configuration and how it protects the cloud environment against the attack targeting the corresponding system mechanism and access control mechanism. System mechanisms comprise security implemented in the cloud, such as hypervisors, firewalls, operational procedures, dedicated VMs, and corporate segregation (Popović & Hocenski, 2010). Access control mechanisms comprise authentication, user creation and access control (Huang, 2015).

Although the mechanisms are discussed in the previous research, their relevant impact on connectivity is not clear and not discussed. This study is designed to measure the connectivity and the impact when different security configurations are implemented to protect these mechanisms. The load balancing procedure and firewall rules are designed for system mechanisms, including hypervisors, firewalls, operation procedures, dedicated VMs, and corporate segregation. The role-based access control and the IAM rules are designed for access control mechanisms, including authentication, user creation and access control.

## Chapter III.

### Methods

In this chapter, we discuss the requirements and specifications of the public cloud environment to be utilized in the project, including the cloud architecture, the designated region/zone, and the network, which could maximize the difference between cloud configurations while minimizing the effect of the external environment. In the second part of the chapter, we describe the experiments designed for the study to test the connectivity under different levels of security configuration.

### 3.1 Computation and Specifications

#### 3.1.1 Computation

A cloud testing environment is the first requirement in this project. A public cloud is selected to be utilized as both the infrastructure and the platform. Generally, a public cloud platform can provide access points through which physical devices can connect to the cloud in a secure and private way (Pierleoni et al., 2020). Google Cloud Platform (GCP) will be chosen as the platform to deploy the cloud computing environment in this project due to the following reasons:

- i. Global network
- ii. Latency

Google Cloud has developed its global network to connect the data centers across the globe and provided a wide range of services for computing, storage, security, and data analysis (Gupta, 2021) (Bisong, 2019). By deploying its own undersea cables to connect the regions and available zones in different continents, Google Cloud is able to reduce the latency between networks and maintain the reliability in its cloud environment.

In order to minimize the latency affected by data communication between different oversea networks, we further deploy the whole cloud test environment in the region in the local Google Cloud data center, as it is the only public cloud that has a data center and region during the time this work is conducted.

### 3.1.2 Specifications

- i. Virtual private cloud environment

The virtual private cloud environment is an isolated environment deployed in the public cloud with the concept of multi-tenant, which could access the shared resources in the public cloud but not be affected by other users' cloud environment. To minimize the latency between overseas networks, the virtual private cloud environment is designed to be deployed in the local data center where we are located. The destination is Region “asia-east1 (Taiwan)”, with Zone “asia-east1-c” in Google Cloud. (Fig 3.1)

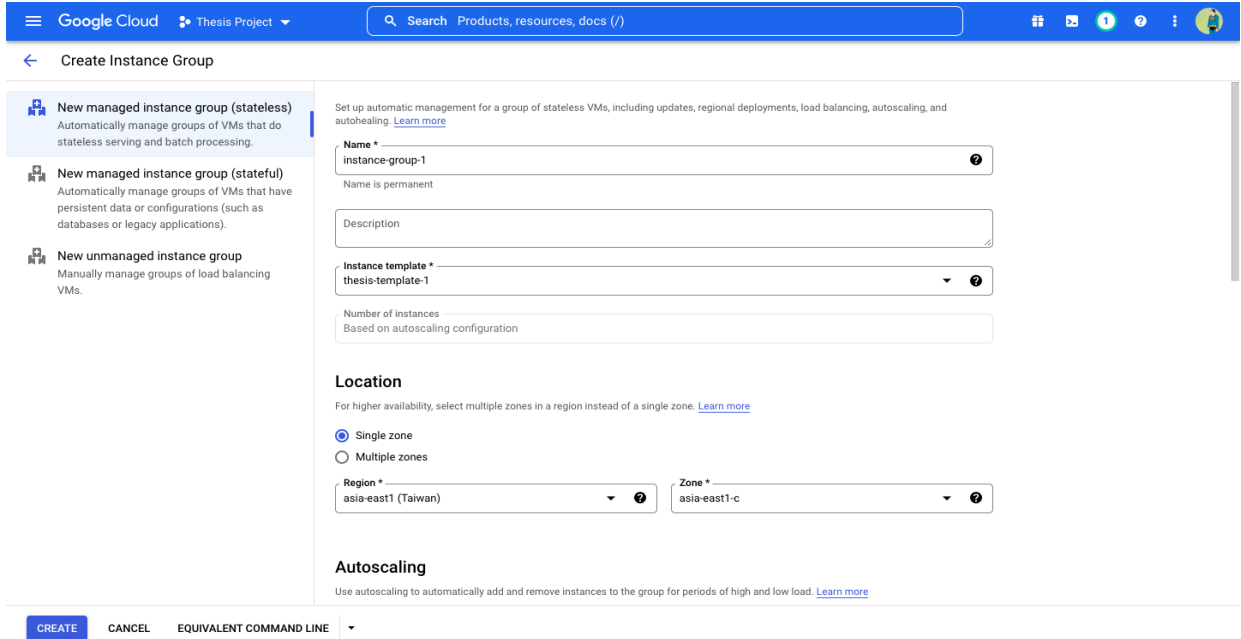


Fig 3.1. Instance Group Configuration1

*The instance group configuration specifies the parameters for the instance group. The instances will be created based on the instance template which is designed to create multiple instances more efficiently. Here the location of the instances is set to be using region of asia-east-1 and zone of asia-east1-c.*

ii. Instance templates

The instance template is designed to be used as the blueprint to efficiently create multiple instances in the cloud environment, it is also the necessary step to create the instance group in the cloud. By specifying the specifications in the template, the individual virtual machines and environment will be created identically once the comment of creating instances is sent.

In the instance template, virtual machine type “e2-micro” is selected. The startup script below used to create the page for connectivity test is also specified in the template. (Fig 3.2, 3.3)

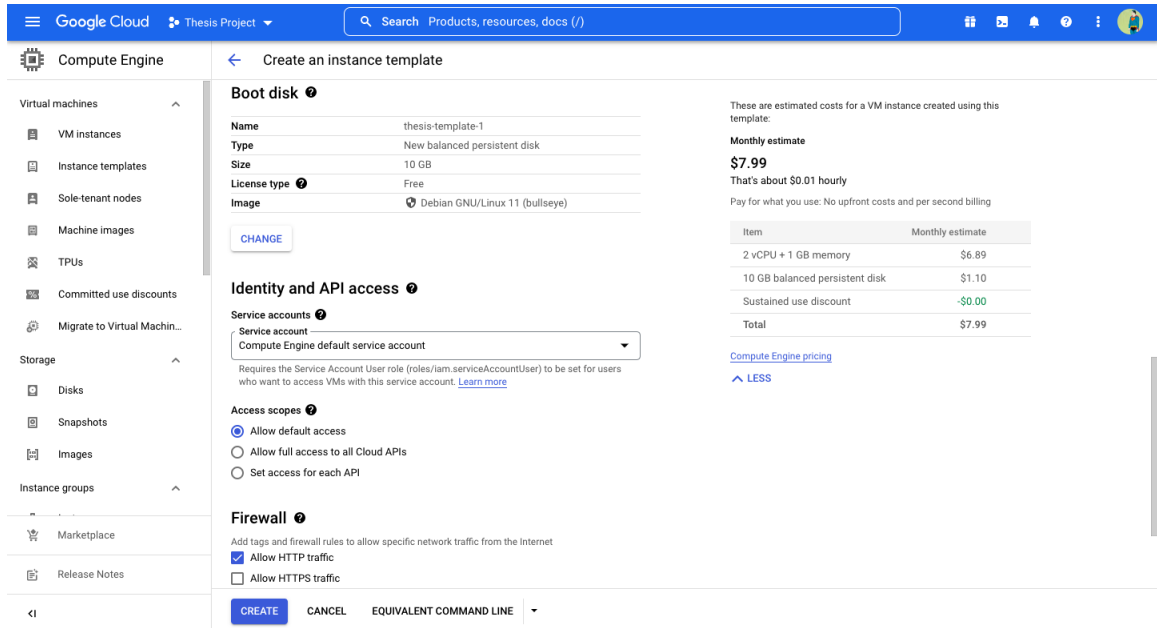


Fig 3.2. Instance Template Configuration1

*The parameters of the instance are specified in the instance template. In this template, the name, type, size, image of the boot disk, as well as the identity and API access of the instance, are set up as the parameters for the default test environment.*

**Security**  
Shielded VM and SSH keys

**Management**  
Description, deletion protection, reservations, automation, and availability policies

**Description**  
The script is used to set up test page for the connectivity.

**Reservations**  
Automatically use created reservation

**Automation**  
Startup script  

```
#!/bin/bash
apt-get update
apt-get install -y apache2
cat <<EOF > /var/www/html/index.html
<html><body><h1>Thesis connectivity test page.</h1>
<p>This page was created for the connectivity test.</p>
</body></html>
EOF
```

These are estimated costs for a VM instance created using this template:  
**Monthly estimate**  
**\$7.99**  
That's about \$0.01 hourly  
Pay for what you use: No upfront costs and per second billing

Item	Monthly estimate
2 vCPU + 1 GB memory	\$6.89
10 GB balanced persistent disk	\$1.10
Sustained use discount	-\$0.00
<b>Total</b>	<b>\$7.99</b>

Compute Engine pricing  
[^ LESS](#)

CREATE CANCEL EQUIVALENT COMMAND LINE

Fig 3.3. Instance Template Configuration2

*The parameters of the instance are specified in the instance template. In this template, we continue to set up the default security and management parameters. The set-up description and automation were created with the code below.*

```
#!/bin/bash

apt-get update

apt-get install -y apache2

cat <<EOF > /var/www/html/index.html

<html><body><h1>Thesis connectivity test page.</h1>

<p>This page was created for the connectivity test.</p>

</body></html>

EOF
```

iii. Instance group

The instance is created based on the instance template. The location is set as “Single Zone”, with Region “asia-east1” and Zone “asia-east1-c”. The instance group is also set to be auto-scalable to meet the demand of increasing workload. When the CPU utilization exceeds 60% in one instance, the instances will automatically set to auto scale to up to five instances to deal with the workload. (Fig 3.4, 3.5)

Google Cloud Thesis Project Search Products, resources, docs (/)

### Create Instance Group

- New managed instance group (stateless)**  
Automatically manage groups of VMs that do stateless serving and batch processing.
- New managed instance group (stateful)**  
Automatically manage groups of VMs that have persistent data or configurations (such as databases or legacy applications).
- New unmanaged instance group**  
Manually manage groups of load balancing VMs.

Set up automatic management for a group of stateless VMs, including updates, regional deployments, load balancing, autoscaling, and autohealing. [Learn more](#)

**Name \***  
instance-group-1  
Name is permanent

**Description**

**Instance template \***  
thesis-template-1

**Number of instances**  
Based on autoscaling configuration

**Location**  
For higher availability, select multiple zones in a region instead of a single zone. [Learn more](#)

Single zone  
 Multiple zones

**Region \*** asia-east1 (Taiwan)    **Zone \*** asia-east1-c

**Autoscaling**  
Use autoscaling to automatically add and remove instances to the group for periods of high and low load. [Learn more](#)

CREATE CANCEL EQUIVALENT COMMAND LINE

Fig 3.4. Instance Group Configuration2

*The parameters of autoscaling are also specified in the instance group configuration for automatic instance creation when the workload exceeds the specification.*

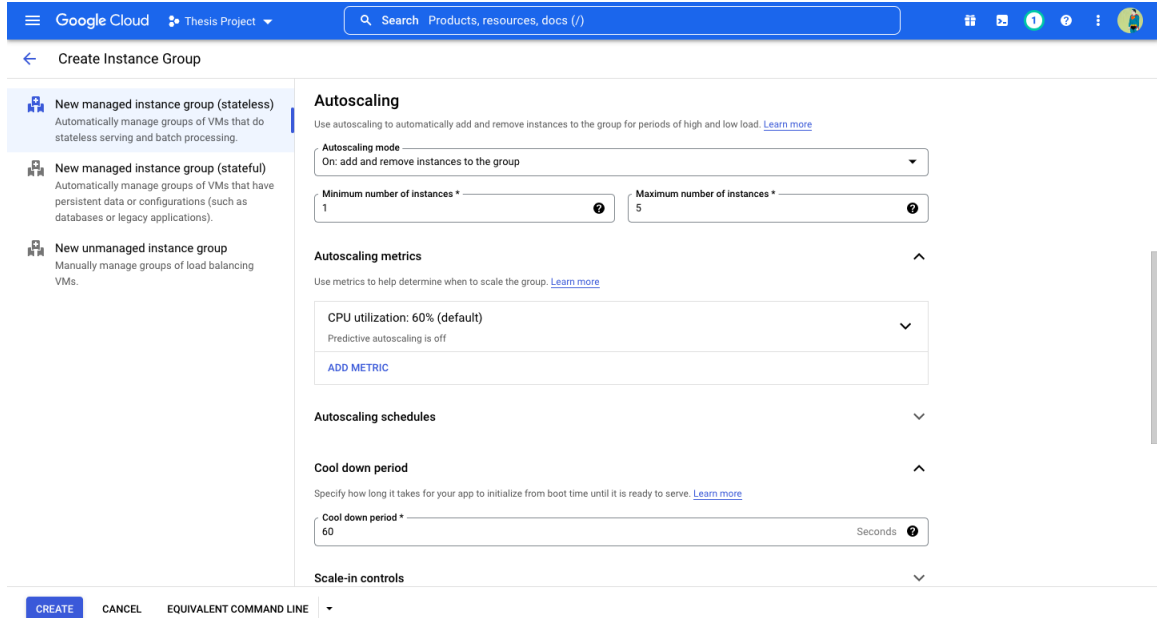


Fig 3.5 Autoscaling Configuration

*The parameters of autoscaling are specified in the instance group. When specific conditions are met, the instance will automatically be added to or removed from the group. The condition we specified is that when the CPU utilization rate exceeds 60%, the instance will be added to the instance group with a minimum of one instance to maximum of five instances.*

iv. Virtual machines

The virtual machines, or instances, are selected with the default “e2-micro” type to host the test page. In this machine, a default boot disk with Debian GNU/Linux 11 and 10 GB disk is selected for the test page. The Identity and API access is set “Allow default access” for the project owner of the cloud environment. (Fig 3.6)

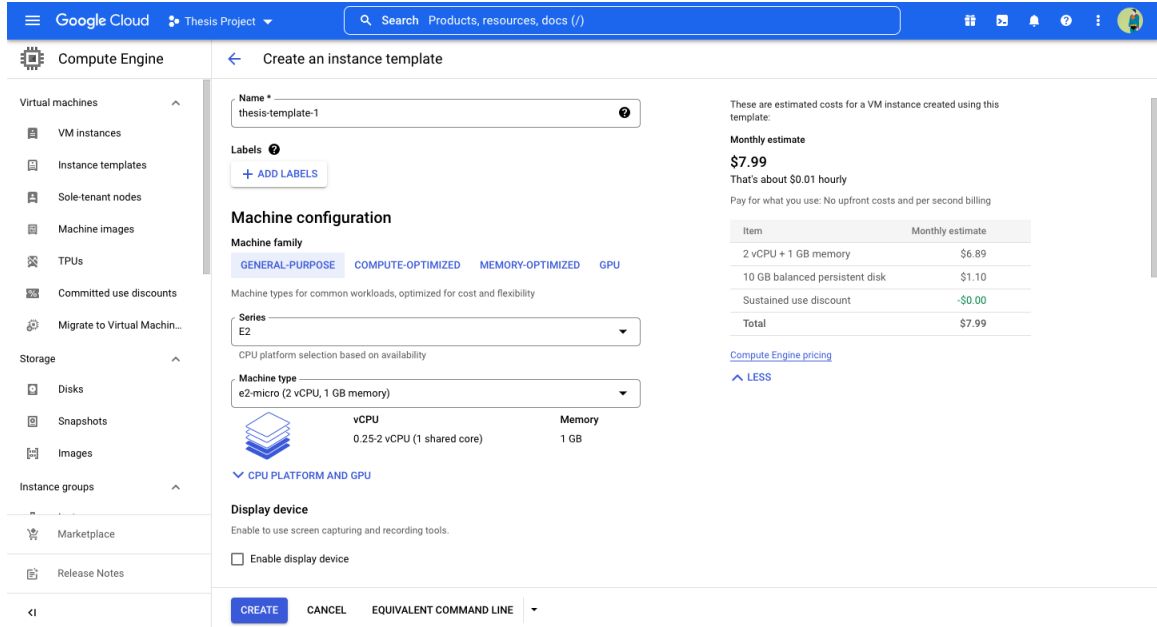


Fig 3.6 Virtual Machine Configuration1

*In the instance template, the specifications of the virtual machine are specified with Series as E2, machine type as e2-micro (2 vCPU, 1GB memory, 10GB balanced persistent disk).*

v. Virtual private cloud network and firewall

The cloud network and firewall configuration are set with default settings in the beginning and will be changed later as described in the research methods, in which HTTP and HTTPS traffic are allowed with specific ports. (Fig 3.7)

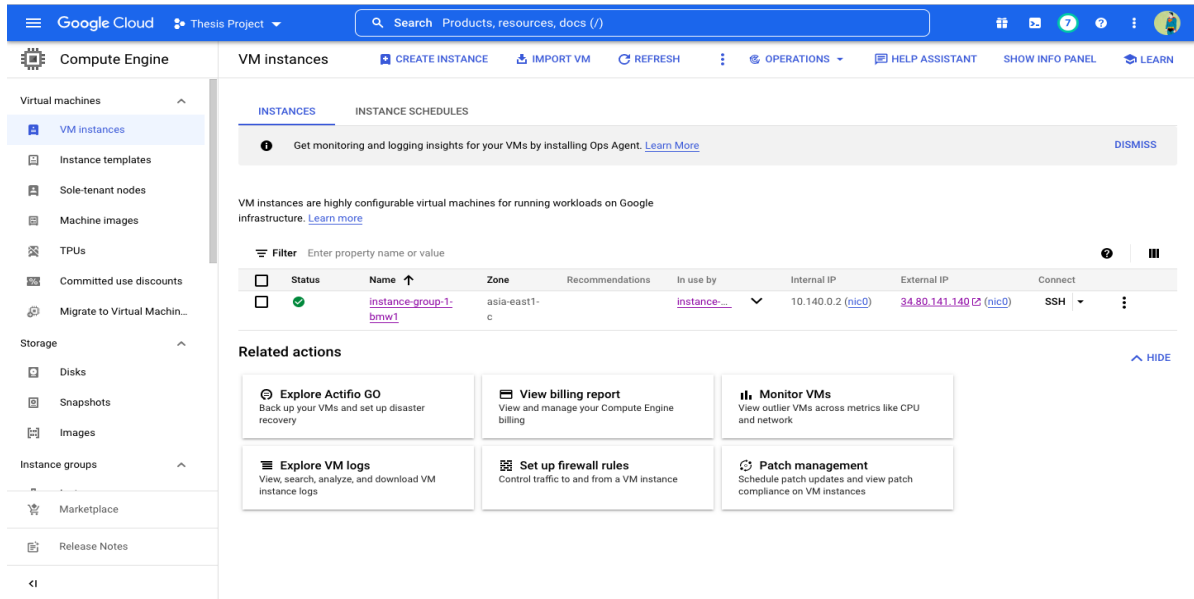


Fig 3.7 Virtual Machine Configuration2

*With all the parameters of the configurations above, the VM instances will be created based on the conditions. An internal IP and an external IP are created and designated in the environment. Users from on-premises devices can connect to the cloud environment via SSH and corresponding keys. This will also be the main method in this research to access the cloud environment.*

### 3.2 Experiments

The experiments to understand the relationship between security and performance in this research start by setting the security configurations in an independent cloud environment deployed on a public cloud.

In the deployed environment, we are excluding the latency variation caused by normal network connection and configuration, measuring the overall access speed to the computing resource under different security configuration levels and complexity. The selected security configurations as variables in this research are the most common, necessary and widely-used configurations in practice. More advanced or cutting-edge cloud security products and configurations only available on one of the public clouds are not adopted in this research.

A typical three-tier structure, including frontend/backend/database, will be deployed on a virtual private cloud on the local GCP region. The overview of the structure is shown in the Figure below: (Fig 3.8)

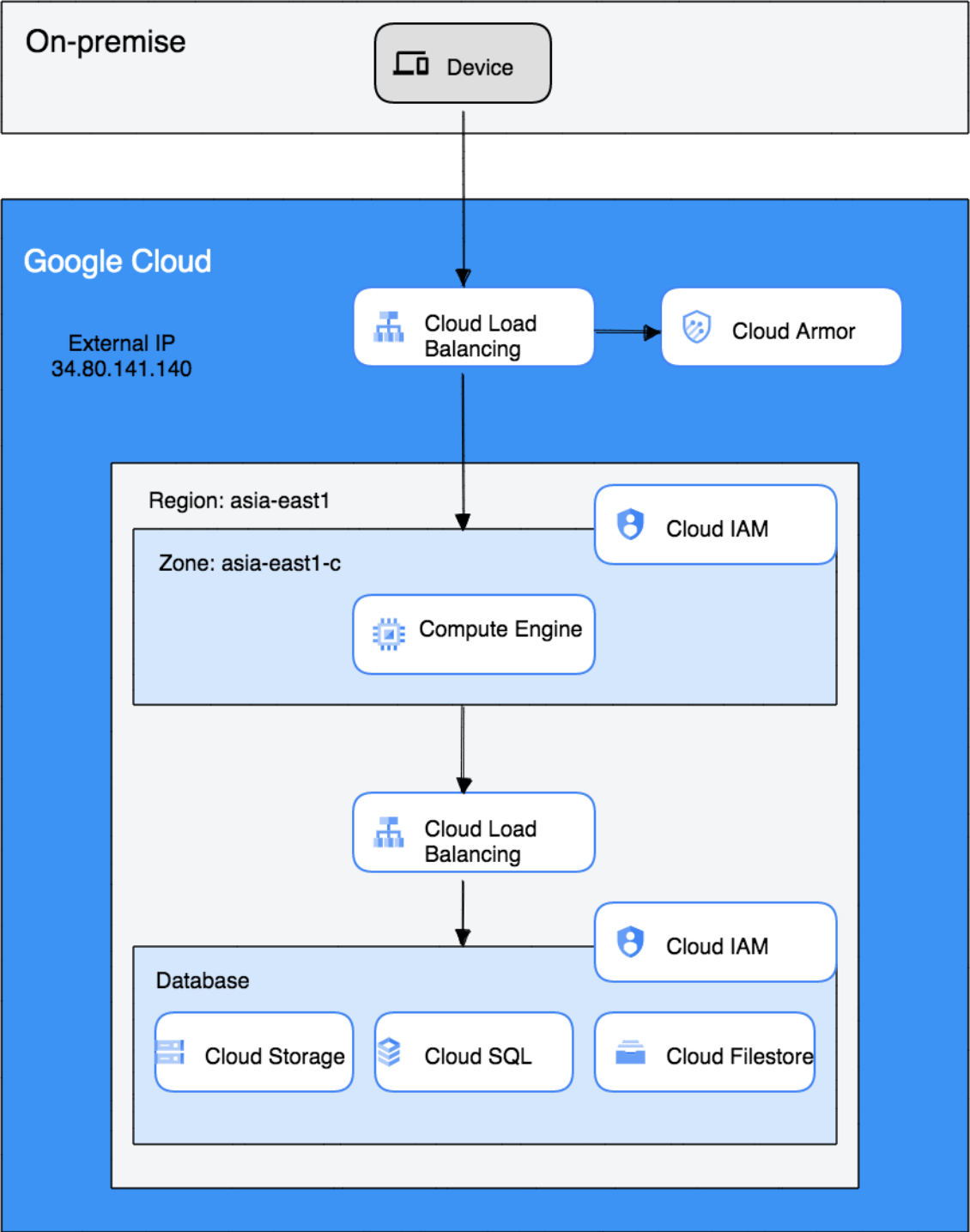


Fig 3.8 Architecture Diagram of the Cloud Environment

*The architecture diagram illustrates the configuration in the cloud environment. Users access the cloud environment from on-premises devices such as laptops. When the users connect to the cloud environment from the external IP, different security configurations help the cloud to identify whether the users are correctly authorized and authenticated to access the cloud. The configurations include a load balancer, firewall (such as Cloud Armor), and IAM. In this research, the region is specified as asia-east1, and the zone is specified as asia-east1-c. The goal is to be correctly authorized to access the compute engine through the load balancer, firewall, and IAM rules. In a more advanced test environment, an internal cloud load balancer and IAM rules can further protect the database, such as Cloud Storage, Cloud SQL, or Cloud Filestore, in a GCP environment.*

In the testing environment, the structure contains a frontend/backend/database. The security configuration in each section includes a Web Application Firewall (WAF) for the frontend, Identity and Access Management (IAM) for the frontend/backend/database, and Data Loss Prevention (DLP) for the database. Different types and levels of configuration will be applied to the testing environment. The goal of the measurement is to measure the latency from the local environment to the resources hosted in the GCP cloud environment and analyze connectivity data versus the corresponding security configuration.

When accessing a database that is hosted in a specific public cloud region, the following methods will be used to measure latency (Google, 2021):

- i. Ping

ICMP ping is a common way to measure server reachability.

ii. Curl

Curl measures Time To First Byte (TTFB). In the measurement, the curl command will be issued repeatedly to the database server.

The test will be performed under different conditions below respectively. Each test will be conducted via local server SSH command to connect to the cloud instance. In each test, the latency will be measured 300 times with an interval of 20ms. The latency will be recorded by round trip time(rtt), with minimum(min), average(avg), maximum(max), and standard deviation(mdev).

### 3.2.1 Condition 1: Measuring latency with default security configuration

Under condition 1, the latency is measured with the default security configuration, in which no load balancer is deployed, and therefore all the traffic goes to the same instance in the virtual private cloud environment. There are no specific firewall settings for the cloud instance, all HTTP requests are allowed via default ports.

While connecting to the cloud instance via SSH, the IAM of the user is set as the default user: project owner. With this identity, the user has the overall ownership of the project in the cloud environment. The virtual cloud environment is constructed in the project.

### 3.2.1.1 Condition 1a: Measuring latency with default setting and the firewall

Under condition 1a, the latency is measured with the default security configuration, in which no load balancer is deployed, and therefore all the traffic goes to the same instance in the virtual private cloud environment. We also set up the specific firewall settings for the cloud instance, the user can only connect the cloud instance via the allowed source IP.

While connecting to the cloud instance via SSH, the IAM of the user is set as the default user: project owner. With this identity, the user has the overall ownership of the project in the cloud environment. The virtual cloud environment is constructed in the project.

### 3.2.1.2 Condition 1b: Measuring latency with default setting and the IAM rules

Under condition 1b, the latency is measured with the default security configuration, in which no load balancer is deployed, and therefore all the traffic goes to the same instance in the virtual private cloud environment. There are no specific firewall settings for the cloud instance, all HTTP requests are allowed via default ports.

While connecting to the cloud instance via SSH, firstly the IAM of the user is set as the default user: project owner. With this identity, the user has the overall ownership of the project in the cloud environment. The virtual cloud environment is constructed in the project. Then we change the role of user to project editor and viewer, to test the latency with different IAM respectively.

### 3.2.1.3 Condition 1c: Measuring latency with default setting, firewall, and the IAM rules

Under condition 1c, the latency is measured with the default security configuration, in which no load balancer is deployed, and therefore all the traffic goes to the same instance in the virtual private cloud environment. We also set up the specific firewall settings for the cloud instance, the user can only connect the cloud instance via the allowed source IP.

While connecting to the cloud instance via SSH, the role of user will be tested with project owner, editor and viewer, and test the latency with different IAM respectively.

### 3.2.2 Condition 2: Measuring latency with a load balancer

In condition 2, on top of condition 1, the load balancer is further deployed as the first additional security configuration. The load balancer is set to balance the traffic to the virtual cloud environment under certain conditions. The latency will be measured in the situation while the load balancer constantly detects the traffic and balances the traffic to different instances. The firewall rules and the IAM of the user remain the same as condition 1.

#### 3.2.2.1 Condition 2a: Measuring latency with a load balancer and IAM

In condition 2a, we also test the latency with the configuration of the load balancer and IAM, the firewall rules remain the same as condition 1. The latency will be measured in the situation where IAM is set as project owner, editor, and viewer.

### 3.2.3 Condition 3: Measuring latency with a load balancer (condition 2) and with the firewall

In condition 3, the variable is the firewall rule to the cloud. On the basis of condition 2, a stricter firewall rule is applied to the virtual cloud environment. In this test, two conditions will be tested: first, the advanced firewall rule to restrict the source IP, and second, the advanced firewall rule to restrict the access with the source/target tag.

### 3.2.4 Condition 4: Measuring latency with a load balancer, firewall (condition 3), and IAM

In condition 4, the test target will be how IAM impacts the connectivity in the cloud environment. On top of condition 3, different IAM settings are applied to the virtual cloud environment to increase the level of the security configuration. In the beginning of the test, the user has the authorization of the project owner as the default setting, a series of tests will be performed under the scenario of role-based access control (RBAC)

- i. Basic role of viewer, user who is authorized as viewer only has permission for the read-only actions which do not affect state and can only view but not modify the existing resources.

- ii. Basic role of editor, user who is authorized as editor has all the permissions of viewer, and also has permission for actions that modify state, such as changing existing resources.
- iii. Basic role of owner, user who is authorized as owner can access all the resources in the project, to create, read, update, and delete the resources in the cloud. The owner can also manage the roles and permissions for a project and all the resources within the project. Owner also has all the permissions which viewers and editors have.

In condition 4, users will be granted different role-based access and test latency under the corresponding level of IAM.

## Chapter IV.

### Results

In chapter 4, on the basis of deploying the cloud environments and methods described in chapter 3, the data of security configuration and connectivity collected in different stages will be visualized in diagrams and analyzed.

#### 4.1 Data Analysis

Based on the research methods and different test conditions set in chapter 3, the test results are described and illustrated in the following tables and diagrams.

##### 4.1.1 Test result with condition 1: Latency with default security configuration

In the test with condition 1, the cloud environment is protected by default security settings as below.

- i. No load balancer is deployed.
- ii. All HTTP requests are allowed via default ports, the IP allowed to access the cloud is set as 0.0.0.0/0, source IP is not restricted, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the role of the cloud project owner.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times of measurements with 20ms interval. The latency result is denoted as L1, which indicates the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L1</b>	0.020	0.048	0.068	0.012

Table 4.1. Test Result of Condition 1

*Table 4.1 describes L1, the test result of condition 1, in which the security configuration is by default setting. The result shows a minimum 0.020ms, average 0.048ms, maximum 0.068ms, and standard deviation 0.012ms.*

#### 4.1.1.1 Test result with condition 1a: Latency with default setting and the firewall

In the test with condition 1a, the cloud environment is protected by default security settings and the firewall as below.

- i. No load balancer is deployed.
- ii. Restrict HTTP requests via allowed ports and the allowed source IP from on-premises device, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the role of the cloud project owner.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times of measurements with 20ms interval. The latency

result is denoted as L1a, which indicates the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L1a</b>	0.022	0.048	0.069	0.012

Table 4.2. Test Result of Condition 1a

*Table 4.2 describes L1a, the test result of condition 1a, in which the security configuration is by default setting and firewall. The result shows a minimum 0.022ms, average 0.048ms, maximum 0.069ms, and standard deviation 0.012ms.*

#### 4.1.1.2 Test result with condition 1b: Latency with default setting and the IAM rules

In the test with condition 1b, the cloud environment is protected by default security settings and the firewall as below.

- i. No load balancer is deployed.
- ii. All HTTP requests are allowed via default ports, the IP allowed to access the cloud is set as 0.0.0.0/0, the source IP is not restricted, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the different roles of the cloud project owner, editor, and viewer.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times of measurements with 20ms interval. The latency

result is denoted as L1b, which indicates the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L1b</b>	0.021	0.047	0.068	0.013

Table 4.3. Test Result of Condition 1b

*Table 4.3 describes L1b, the test result of condition 1b, in which the security configuration is by default setting and IAM. The result shows a minimum 0.021ms, average 0.047ms, maximum 0.068ms, and standard deviation 0.013ms*

#### 4.1.1.3 Test result with condition 1c: Latency with default setting, firewall, and the IAM rules

In the test with condition 1c, the cloud environment is protected by default security settings and the firewall as below.

- i. No load balancer is deployed.
- ii. Restrict HTTP requests via allowed ports and the allowed source IP from on-premises device, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the different roles of the cloud project owner, editor, and viewer.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times of measurements with 20ms interval. The latency

result is denoted as L1c, which indicates the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L1c</b>	0.022	0.049	0.069	0.013

Table 4.4. Test Result of Condition 1c

*Table 4.4 describes L1c, the test result of condition 1c, in which the security configuration is by default setting, firewall, and IAM. The result shows a minimum 0.022ms, average 0.049ms, maximum 0.069ms, and standard deviation 0.013ms*

#### 4.1.2 Test result with condition 2: Latency with a load balancer

In the test with condition 2, the cloud environment is protected by condition 1 configuration and load balancer.

- i. A load balancer is deployed with triggering conditions when the CPU utilization exceeds 60% in one instance, the instances will automatically set to auto-scale to up to five instances to deal with the workload.
- ii. All HTTP requests are allowed via default ports, the IP allowed to access the cloud is set as 0.0.0.0/0, the source IP is not restricted, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the role of the cloud project owner.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times measurements with 20ms intervals. The latency

result is denoted as L2, which includes the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L2</b>	0.022	0.046	0.065	0.014

Table 4.5. Test Result of Condition 2

*Table 4.2 describes L2, the test result of condition 2, in which the security configuration is by default setting with the load balancer is deployed. The result shows a minimum 0.022ms, average 0.046ms, maximum 0.065ms, and standard deviation 0.014ms.*

#### 4.1.2.1 Test result with condition 2a: Latency with a load balancer and IAM

In the test with condition 2a, the cloud environment is protected by condition 1 configuration, load balancer, and IAM.

- i. A load balancer is deployed with triggering conditions when the CPU utilization exceeds 60% in one instance, the instances will automatically set to auto-scale to up to five instances to deal with the workload.
- ii. All HTTP requests are allowed via default ports, the IP allowed to access the cloud is set as 0.0.0.0/0, the source IP is not restricted, no source/target tag is checked.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the different roles of the cloud project owner, editor, and viewer.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times measurements with 20ms intervals. The latency result is denoted as L2a, which includes the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L2a</b>	0.023	0.049	0.070	0.013

Table 4.6. Test Result of Condition 2a

*Table 4.6 describes L2a, the test result of condition 2a, in which the security configuration is by default setting with the load balancer and IAM. The result shows a minimum 0.023ms, average 0.049ms, maximum 0.070ms, and standard deviation 0.013ms.*

#### 4.1.3 Test result with condition 3: Latency with a load balancer and firewalls

In the test with condition 3, the cloud environment is protected by security configurations in both condition 1 and condition 2. Meanwhile the two firewall rules are set and deployed.

- i. A load balancer is deployed with triggering conditions when the CPU utilization exceeds 60% in one instance, the instances will automatically set to auto scale to up to five instances to deal with the workload.
- ii. Restrict HTTP requests via allowed ports and the allowed source IP from on-premises device, and source/target tag is checked as an additional

condition of the firewall.

The condition with allowed ports and source IP is denoted as condition 3a, and the condition where source/target tags are also configured is denoted as condition 3b.

- iii. The user accesses the cloud environment from the on-premises device with authorization of the role of the cloud project owner.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times of measurements with 20ms interval. The latency result is denoted as L3a and L3b, representing the latency of condition 3a and 3b, respectively, which includes the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L3a</b>	0.023	0.050	0.070	0.011
<b>L3b</b>	0.024	0.050	0.071	0.011

Table 4.7. Test Result of Condition 3

*Table 4.7 describes L3a and L3b, the test result of condition 3a and 3b, in which the security configuration is by default setting with the load balancer and firewall rules are deployed. The L3a result shows a minimum 0.023ms, average 0.050ms, maximum 0.070ms, and standard deviation 0.011ms. The L3b result shows a minimum 0.024ms, average 0.050ms, maximum 0.071ms, and standard deviation 0.011ms.*

#### 4.1.4 Test result with condition 4: Latency with a load balancer, firewalls, and different IAM rules

In the test with condition 4, the cloud environment is protected by the security configurations in all of conditions 1, 2, and 3. Also the three different IAM rules are set and deployed.

- i. A load balancer is deployed with triggering conditions when the CPU utilization exceeds 60% in one instance, the instances will automatically set to auto scale to up to five instances to deal with the workload
- ii. Restrict HTTP requests via allowed ports and the allowed source IP from the on-premises device, and target tag is checked as an additional condition of the firewall.
- iii. The user accesses the cloud environment from the on-premises device with authorization of the different roles of the cloud project owner, editor, and viewer. The condition 4 with authorization of the cloud project owner/editor/viewer is denoted as the condition 4a, 4b, and 4c, respectively.

The latency test is performed from on-premises device to the local public cloud region via SSH, the test takes 300 times measurements with 20ms intervals. The latency result is denoted as L4a, L4b, and L4c, representing the latency of condition 4a/4b/4c, respectively, which includes the minimum, average, maximum, and standard deviation of the Round-trip time(rtt) in ms.

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L4a</b>	0.023	0.051	0.070	0.012
<b>L4b</b>	0.025	0.052	0.071	0.013
<b>L4c</b>	0.024	0.051	0.072	0.013

Table 4.8. Test Result of Condition 4

*Table 4.8 describes L4a, L4b, and L4c, the test result of condition 4a, 4b, and 4c, respectively. In which the security configuration is by default set with the load balancer, firewall, and IAM rules are deployed. The L4a result shows a minimum 0.023ms, average 0.051ms, maximum 0.070ms, and standard deviation 0.012ms. The L4b result shows a minimum 0.025ms, average 0.052ms, maximum 0.071ms, and standard deviation 0.013ms. The L4c result shows a minimum 0.024ms, average 0.051ms, maximum 0.072ms, and standard deviation 0.013ms.*

#### 4.1.5 Test results summarization

To summarize the test result from the default configuration to the advanced security configuration, the conditions are summarized in table 4.9 (“O” denotes the conditions where the configuration applies), while table 4.10 and figure 4.1 below indicate the data.

	<b>Default</b>	<b>Load balancer</b>	<b>Firewall</b>	<b>IAM</b>
<b>L1</b>	<b>O</b>			
<b>L1a</b>	<b>O</b>		<b>O</b>	
<b>L1b</b>	<b>O</b>			<b>O</b>
<b>L1c</b>	<b>O</b>		<b>O</b>	<b>O</b>
<b>L2</b>	<b>O</b>	<b>O</b>		
<b>L2a</b>	<b>O</b>	<b>O</b>		<b>O</b>
<b>L3a</b>	<b>O</b>	<b>O</b>	<b>O</b>	
<b>L3b</b>	<b>O</b>	<b>O</b>	<b>O</b>	
<b>L4a</b>	<b>O</b>	<b>O</b>	<b>O</b>	<b>O</b>
<b>L4b</b>	<b>O</b>	<b>O</b>	<b>O</b>	<b>O</b>
<b>L4c</b>	<b>O</b>	<b>O</b>	<b>O</b>	<b>O</b>

Table 4.9. Test Conditions Comparison

*Table 4.9 summarizes the comparison of security configuration between different conditions.*

<b>rtt(ms)</b>	<b>min</b>	<b>avg</b>	<b>max</b>	<b>mdev</b>
<b>L1</b>	0.020	0.048	0.068	0.012
<b>L1a</b>	0.022	0.048	0.069	0.012
<b>L1b</b>	0.021	0.047	0.068	0.013
<b>L1c</b>	0.022	0.049	0.069	0.013
<b>L2</b>	0.022	0.046	0.065	0.014
<b>L2a</b>	0.023	0.049	0.070	0.013
<b>L3a</b>	0.023	0.050	0.070	0.011
<b>L3b</b>	0.024	0.050	0.071	0.011
<b>L4a</b>	0.023	0.051	0.070	0.012
<b>L4b</b>	0.025	0.052	0.071	0.013
<b>L4c</b>	0.024	0.051	0.072	0.013

Table 4.10. Test Results of All Conditions

*Table 4.10 summarizes the comparison of test results between different conditions. The data refers to the rtt of each condition in ms.*

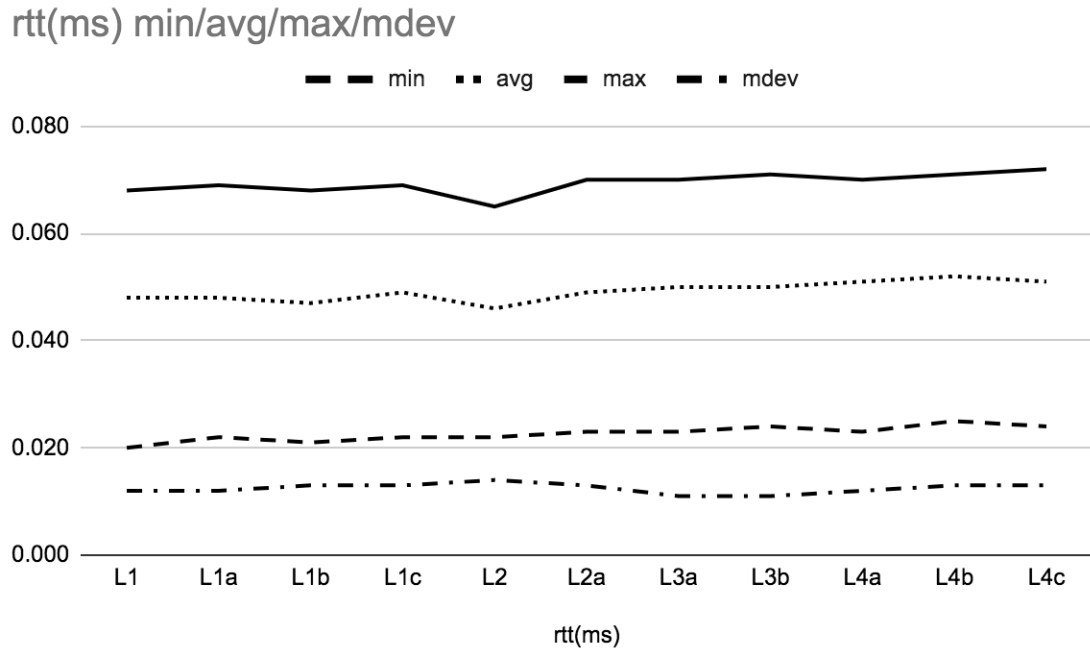


Fig 4.1. Comparison of Test Results under Different Test Conditions

*Figure 4.1 illustrates the comparison of test results under different test conditions. The four different curves show the results of the minimum, average, maximum, and standard deviation of the rtt in ms, respectively.*

## 4.2 Comparison and Discussion

The test data is collected and illustrated, the result and difference between each test condition will be compared and described in this section.

### 4.2.1 Condition 1 and Condition 2

A load balancer is the configuration difference between conditions 1 and 2. The data shows a minor difference in the average rtt of conditions 1 and 2, it slightly decreases 0.002ms, or 4%.

In general, the load balancer balances the traffic to the instances. When the requests are sent from the users' devices and ask for access to the cloud resources, the load balancer takes effect and leads the request to the available resource and improves the performance (Google, 2022). This could be the reason for the difference between conditions 1 and 2.

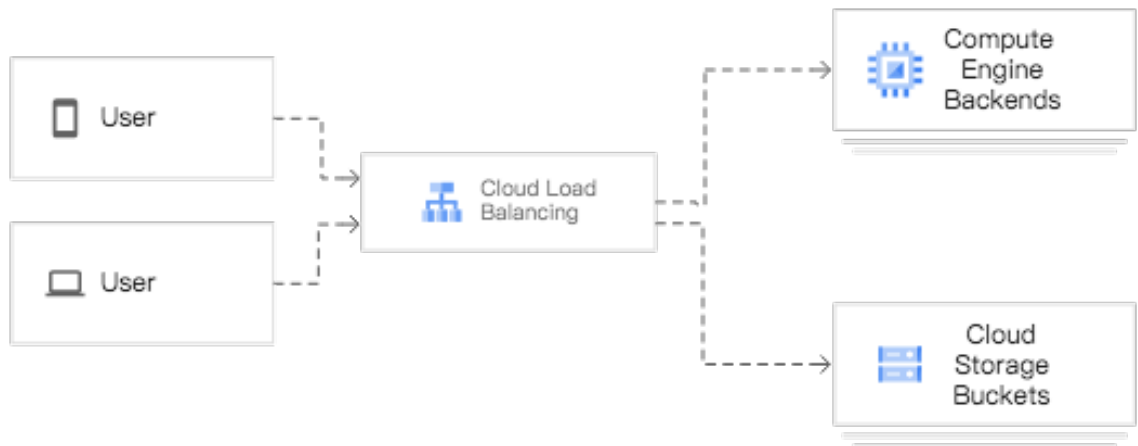


Fig 4.2. The Mechanism of Cloud Load Balancer

*Figure 4.2 illustrates the mechanism of a load balancer in the cloud. When different users try to access the cloud environment (such as compute engine in the backends or*

*cloud storage), the load balancer takes effect, then balances the workload and traffic to the corresponding and optimal cloud resources. Meanwhile, the cloud load balancer also works as one of the security configurations to protect the cloud environment.*

#### 4.2.2 Condition 2 and Condition 3

Between conditions 2 and 3, further firewall rules are applied. For the virtual private cloud (VPC) in the test, the firewall rules have the following characteristics (Google, 2022):

- i. Each firewall rule applies to incoming (ingress) or outgoing (egress) connections, not both.
- ii. Each firewall rule can contain either IPv4 or IPv6 ranges, but not both.
- iii. Each firewall rule's action is either: allow or deny.

In condition 3, all the requests or traffic to the cloud instances must be checked by the firewall rules above. The procedure is

- i. First, the requests from on-premises are seen as incoming connections to the cloud.
- ii. Second, the source IP is within an IPv4 range.
- iii. Third, only the selected source IP is allowed to access the cloud environment.

These checks could lead to the time needed to access the cloud and increase the average rtt. The measured rtt increases 0.004ms or 8% to the average time.

#### 4.2.3 Condition 3a and Condition 3b

Both conditions 3a and 3b are for firewall rules test. The difference lies in the type of firewall rules. In the general scenario of condition 3a, a specific source IP or a group of specific source IP range is allowed (or denied) to access the cloud environment. This could help the user to protect the cloud environment and instances from external access. However, in condition 3b, an additional firewall tag is adopted as one of the further measures to restrict access between different instances, only the request with a predefined source tag can access the instance with predefined target tag.

In both conditions, the source IP is checked and then granted access to the cloud environment. Once the IP meets the restriction, but the source/target tag needs to be further checked. It is one more step of firewall checking in the request code from SSH as well as in the cloud. However, no significant difference is measured in the rtt. The average rtt for condition 3a and 3b are the same, with only minor differences (0.001ms, or <3%) in the minimum and maximum which can almost be neglected.

#### 4.2.4 Condition 3 and condition 4

On top of condition 3 (both 3a and 3b are applied), in condition 4, the IAM rules are applied to create a more advanced security configuration where different roles are set to access the cloud environment. More complicated IAM could be set in a real environment

to meet the complexity of real-world environment management. In this research, the role-based access control (RBAC) is simplified to three types of main access. The test results of L3b and L4a are of the same configuration. Thus, the test results should be almost identical, and the difference should be neglected. From table 4.8 the results are observed and the variables in different conditions 4a, 4b, and 4c can be seen as the impact from IAM.

#### 4.2.5 Condition 4a, 4b and condition 4c

From condition 4a to 4b to 4c, the IAM rules can be seen as becoming stricter. When the user can access as owner (with all access to all the resources within the scope of the project in the cloud), as editor(only has the permission for actions that modify state, such as changing existing resources), as viewer(only has the permission for the read-only actions which do not affect state, and can only view but not modify the existing resources). The difference in 4a, 4b, and 4c is not significant (0.001ms, or <2%), only the maximum and standard deviation of rtt slightly change.

#### 4.2.6 General comparison

From condition 1 to condition 4, no significant latency difference observed when comparing each two adjacent conditions. However, when comparing the general trend from Table 4.8 and Fig 4.1, the rtt slightly increases when more security configuration

applies and creates a more secure environment in the cloud. The more security measures are configured, the more rules and authorization need to be checked, which could cause the rtt varying. However, in the cutting-edge public cloud computing platform, the difference seems not significant to affect the access and the use of the cloud resources.

From Table 4.8 the average rtt increases from 0.046ms to 0.052ms, which might be a >10% difference, nonetheless, the difference of 0.006ms is relatively small and can be neglected in most of the existing applications deployed in the public cloud nowadays, except some of the advanced computing applications which require really low latency.

## Chapter V.

### Conclusion

In this thesis, we explore different security configurations and connectivity performance. Under different conditions, we observe minor differences in latency and when the cloud environment is secured by increasing the security configuration, our results show minor variation in connectivity. Only a few percent difference in the latency can be observed, even though the security configuration could theoretically affect the connectivity.

The variation observed in different tests is only in the order of 0.001ms, which could usually be neglected in practice. The normal variation which could affect the cloud application is usually in the order of 1ms, thus, the variation might not have a real impact on the application in a cloud environment. On the other hand, the test environment deployed in this work is a simplified version compared to that encountered in practice. With the same security measures, the cloud architecture in a real environment could be more complicated along with more intertwined computing resources and network settings, and the configuration could still have some impact on the connectivity.

The most general security configuration, such as a load balancer, firewall rules, IAM rules are set up and tested in our experiments. We should give the following considerations for extending the application of our approach to different environments.

First, the test environment deployed in the cloud in this project is a simplified version of a practical architecture. In a typical environment, a configuration including IAM, firewall, and a load balancer is usually deployed as the fundamental measures, but the instances, network, storage and database architecture is usually more complicated and intertwined. This could lead to more authorization and authentication processes in the whole ingress and egress transmission, which could also increase the latency and create an impact on the connectivity.

Second, as more and more cybersecurity threats emerge, more countermeasures and security products have been created or developed to further protect the fast-growing cloud applications and businesses. Different from the security configuration mentioned in this work, some of the products are designed to be embedded in the cloud environment and monitor most activities in the cloud environment to analyze potential threats. The principle and mechanism could be different from the configurations in this work, and additional methods will need to be developed for an advanced analysis to understand the impact of security products on cloud connectivity.

Finally, cloud computing and cloud security are topics being constantly developed and challenged. Developers and users constantly find new possibilities in new cloud products and applications, while hackers and attackers always try to find vulnerabilities and weaknesses in the cloud environment. The problem is to find the balance between security and performance. As cloud technology and the environment continuously change and evolve, the complexity of cloud computing as well as that of cloud security will increase. We suggest that our methods could serve as a basis to evaluate the relationship

between security and performance and determine the balance for a specific cloud environment.

## References

- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, 305, 357-383.
- Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., & Merle, P. (2017). Elasticity in cloud computing: state of the art and research challenges. *IEEE Transactions on Services Computing*, 11(2), 430-447.
- Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.
- Almulla, S. A., & Yeun, C. Y. (2010, March). Cloud computing security management. In *2010 Second International Conference on Engineering System Management and Applications* (pp. 1-7). IEEE.
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
- Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 288-292). IEEE.

- Aslam, S., & Shah, M. A. (2015, December). Load balancing algorithms in cloud computing: A survey of modern techniques. In 2015 National software engineering conference (NSEC) (pp. 30-35). IEEE.
- AWS (2021, December). AWS Identity & Access Management. Amazon Web Service Documents.
- Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.
- Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In 2011 World Congress on Information and Communication Technologies (pp. 217-222). IEEE.
- Birje, M. N., Challagidad, P. S., Goudar, R. H., & Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. *International Journal of Cloud Computing*, 6(1), 32-57.
- Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. *arXiv preprint arXiv:1109.5388*, 1-15.
- Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. *International Journal of Big Data Intelligence*, 4(2), 81-107.

- Bisong, E. (2019). An overview of google cloud platform services. *Building Machine Learning and Deep Learning Models on Google Cloud Platform*, 7-10.
- Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, 57, 24-41.
- Chen, S. L., Chen, Y. Y., & Kuo, S. H. (2017). CLB: A novel load balancing architecture and algorithm for cloud services. *Computers & Electrical Engineering*, 58, 154-160.
- Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, 59, 126-140.
- Deepa, T., & Cheelu, D. (2017, August). A comparative study of static and dynamic load balancing algorithms in cloud computing. In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)* (pp. 3375-3378). IEEE.
- Etro, F. (2015). The economics of cloud computing. In *Cloud technology: concepts, methodologies, tools, and applications* (pp. 2135-2148). IGI Global.
- Google Cloud (2021, December). Optimizing application latency with load balancing. Google Cloud Documents.
- Google Cloud (2022, October). VPC firewall rules. Google Cloud Documents

- Gupta, D., Bhatt, S., Gupta, M., Kayode, O., & Tosun, A. S. (2020, May). Access control model for google cloud iot. In 2020 IEEE 6th Intl conference on big data security on cloud (BigDataSecurity), IEEE Intl conference on high performance and smart computing, (HPSC) and IEEE Intl conference on intelligent data and security (IDS) (pp. 198-208). IEEE.
- Gupta, B., Mittal, P., & Mufti, T. (2021, March). A review on Amazon web service (AWS), Microsoft azure & Google cloud platform (GCP) services. In Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India.
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, 4(1), 1-13.
- Huang, W., Ganjali, A., Kim, B. H., Oh, S., & Lie, D. (2015). The state of public infrastructure-as-a-service cloud security. *ACM Computing Surveys (CSUR)*, 47(4), 1-31.
- Hussein, N. H., & Khalid, A. (2016). A survey of cloud computing security challenges and solutions. *International Journal of Computer Science and Information Security*, 14(1), 52.
- Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2016). Emerging security challenges of cloud virtual infrastructure. *arXiv preprint arXiv:1612.09059*.

- Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, 21(4), 574-588.
- Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *2009 IEEE international conference on cloud computing* (pp. 109-116). Ieee.
- Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., & Powell, W. (2014, June). Catch me if you can: A cloud-enabled DDoS defense. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (pp. 264-275). IEEE.
- Joshi, G., Soljanin, E., & Wornell, G. (2017). Efficient redundancy techniques for latency reduction in cloud systems. *ACM Transactions on Modeling and Performance Evaluation of Computing Systems (TOMPECS)*, 2(2), 1-30.
- Kanakala, V. R., Reddy, V. K., & Karthik, K. (2015, March). Performance analysis of load balancing techniques in cloud computing environment. In *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1-6). IEEE.
- Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In *2009 IEEE International Conference on Services Computing* (pp. 517-520). IEEE.
- Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of network and computer applications*, 71, 11-29.

- Khare, S., Chourasia, U., & Deen, A. J. (2022). Load balancing in cloud computing. In Proceedings of the International Conference on Cognitive and Intelligent Computing (pp. 601-608). Springer, Singapore.
- Khakpour, A. R., & Liu, A. X. (2012, October). First step toward cloud-based firewalling. In *2012 IEEE 31st Symposium on Reliable Distributed Systems* (pp. 41-50). IEEE.
- Kumar, P., & Kumar, R. (2019). Issues and challenges of load balancing techniques in cloud computing: A survey. *ACM Computing Surveys (CSUR)*, 51(6), 1-35.
- Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, 125, 691-697.
- Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33, 1-48.
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
- Mohammed, I. A. (2019). CLOUD IDENTITY AND ACCESS MANAGEMENT–A MODEL PROPOSAL. *International Journal of Innovations in Engineering Research and Technology*, 6(10), 1-8.
- Moura, J., & Hutchison, D. (2016). Review and analysis of networking challenges in cloud computing. *Journal of Network and Computer Applications*, 60, 113-129.

- Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., & Ullah, A. (2017). Cloud computing environment and security challenges: A review. *International Journal of Advanced Computer Science and Applications*, 8(10).
- Naik, N., & Jenkins, P. (2016, March). A secure mobile cloud identity: Criteria for effective identity and access management standards. In 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) (pp. 89-90). IEEE.
- Namasudra, S., Roy, P., & Balusamy, B. (2017, February). Cloud computing: fundamentals and research issues. In 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM) (pp. 7-12). IEEE.
- Parikh, S., Dave, D., Patel, R., & Doshi, N. (2019). Security and privacy issues in cloud, fog and edge computing. *Procedia Computer Science*, 160, 734-739.
- Pierleoni, P., Concetti, R., Belli, A., & Palma, L. (2019). Amazon, Google and Microsoft solutions for IoT: Architectures and a performance comparison. *IEEE access*, 8, 5455-5470.
- Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE.
- Puthal, D., Sahoo, B. P., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In 2015 International Conference on Computational Intelligence and Networks (pp. 116-123). IEEE.

- Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology*, 55(2), 158-172.
- Rana, M. E., Kubbo, M., & Jayabalan, M. (2017). Privacy and security challenges towards cloud-based access control. *Asian. Journal of Information Technology*, 16(2-5), 274-281.
- Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet computing*, 16(1), 69-73.
- Riti, P. (2018). Identity and Access Management with Google Cloud Platform. In *Pro DevOps with Google Cloud Platform* (pp. 223-244). Apress, Berkeley, CA.
- Sadiku, M. N., Musa, S. M., & Momoh, O. D. (2014). Cloud computing: opportunities and challenges. *IEEE potentials*, 33(1), 34-36.
- Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I. (2016). Cloud security: Issues and concerns. *Encyclopedia on cloud computing*, 1-14.
- Schneider, D. (2012). The state of network security. *Network Security*, 2012(2), 14-20.
- Sen, J. (2015). Security and privacy issues in cloud computing. In *Cloud technology: concepts, methodologies, tools, and applications* (pp. 1585-1630). IGI global.
- Sheng, H., Wei, L., Zhang, C., & Zhang, X. (2016, July). Privacy-preserving cloud-based firewall for iaas-based enterprise. In *2016 International Conference on Networking and Network Applications (NaNA)* (pp. 206-209). IEEE.

- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE internet of things journal*, 3(5), 637-646.
- Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88-115.
- Sqalli, M. H., Al-Haidari, F., & Salah, K. (2011, December). Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing. In *2011 Fourth IEEE international conference on utility and cloud computing* (pp. 49-56). IEEE.
- Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012, August). State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. In *Proceedings of the international conference on advances in computing, communications and informatics* (pp. 470-476).
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1), 1-11.
- Sun, A., Gao, G., Ji, T., & Tu, X. (2018, August). One quantifiable security evaluation model for cloud computing platform. In *2018 sixth international conference on advanced cloud and big data (CBD)* (pp. 197-201). IEEE.
- Sun, X. (2018, May). Critical security issues in cloud computing: a survey. In *2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity)*, *IEEE International Conference on High Performance and Smart Computing*,

(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 216-221). IEEE.

Surya, L. (2018). Streamlining Cloud Application with AI Technology. *International Journal of Innovations in Engineering Research and Technology [IJERT]* ISSN, 2394-3696.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, 76(12), 9493-9532.

White, J. E. (1971). RFC0105: Network Specifications for Remote Job Entry and Remote Job Output Retrieval at UCSB.

Wood, K., & Pereira, E. (2010, November). An investigation into cloud configuration and security. In *2010 International Conference for Internet Technology and Secured Transactions* (pp. 1-6). IEEE.

Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE communications surveys & tutorials*, 15(2), 843-859.

Yu, S., Doss, R., Zhou, W., & Guo, S. (2013, June). A general cloud firewall framework with dynamic resource allocation. In *2013 IEEE international conference on communications (ICC)* (pp. 1941-1945). IEEE.

Zeng, W., & Germanos, V. (2019, August). Benefit and cost of cloud computing security. In *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced &*

Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCCom/IOP/SCI) (pp. 291-295). IEEE.

Zhang, F., Chen, J., Chen, H., & Zang, B. (2011, October). Cloudvisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (pp. 203-216).

Zhe, D., Qinghong, W., Naizheng, S., & Yuhan, Z. (2017, May). Study on data security policy based on cloud storage. In 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 145-149). IEEE.

Zhou, L., Varadharajan, V., & Hitchens, M. (2015). Trust enhanced cryptographic role-based access control for secure cloud data storage. *IEEE Transactions on Information Forensics and Security*, 10(11), 2381-2395.

## Appendix 1.

### Glossary

Cloud Service Provider: CSP, the companies which provide various of cloud service or resources from infrastructures, platforms or software

Data Loss Prevention: DLP, a set of tools or procedures to ensure the data will not be lost, misused or accessed by unauthorized users or other third-parties

Google Cloud Platform: GCP, one of the largest public cloud service platforms provided by Google, provides a series of services including infrastructure, platform and software

Infrastructure as a Service: IaaS, cloud service providers provide public infrastructure for users which users pay for the infrastructure resources and need to develop their own platforms or software

Identity and Access Management: IAM, the security practices which control and manage the identity and access of the users and grant users the necessary access to the resources

Internet Control Message Protocol: ICMP, a supporting protocol in the internet protocol suite, which is used by network devices to send operational information or error messages when communicating with another IP address

Platform as a Service: PaaS, cloud service providers provide public platform which users can develop their own software and pay for the platform resources

**Region:** A specific geographical location where users can host one's own resources. The worldwide public cloud is composed of regions and zones

**Software as a Service:** SaaS, cloud service providers provide public software which users can directly use and do not need to configure the infrastructure or platform, the software on cloud are developed by cloud service providers or other third parties

**Web Application Firewall:** WAF, the security configuration acts as a shield which helps protect web application by filtering or monitoring the traffic between the internet and the web application

**Zone:** A Zone is a standalone physical unit which provides the cloud resources to the user. In general, a region has three or more zones. The resources that live in a zone are referred to as zonal resource