# PRIVATE CLOUD COMPUTING AND IT'S ADVANTAGES

**AHMAD AKMAL HAZIM BIN ZULKIFLI**



**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

# PRIVATE CLOUD COMPUTING AND IT'S ADVANTAGES

[AHMAD AKMAL HAZIM BIN ZULKIFLI]



This report is submitted in partial fulfillment of the requirements for the Bachelor of [Computer Science (Computer Security)] with Honours.



FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

## DECLARATION

I hereby declare that this project report entitled

**PRIVATE CLOUD COMPUTING AND IT'S ADVANTAGES**

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : AHMAD AKMAL HAZIM BIN ZULKIFLI Date : 29/6/2021



I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of [Computer Science (Computer Security)] with Honours.

SUPERVISOR : Ts. Dr. Mohd Rizuan Bin Baharon Date: 5/9/2021
([NAME OF THE SUPERVISOR])

## DECLARATION

**DEDICATION**

To my beloved family especially both of my parents for all the moral support they gave me through my hardships and ease and to my valuable friends for helping me out through this semester.

## ACKNOWLEDGEMENTS

All praise to Allah because of Him, I manage to complete this Final Year Project (FYP). I would like to express my gratitude to my project supervisor, Ts. Dr. Mohd Rizuan Bin Baharon on his invaluable advice, guidance and his enormous patience throughout the development of the project and research. Without his guide, this report and project cannot be completed. Next, I would like to express my gratitude to my beloved parents who have helped and given me support, motivation and encouragement throughout my project. In addition, I would like to thank everyone, especially my friends who had contributed to the successful completion of this project. I managed to complete my report and also my project which is Benefits of Private Cloud Security.

# ABSTRACT

Cloud computing is becoming more popular norm for accessing computing resources. Cloud computing security or also known as cloud security can also be defined as security measures configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. However, when using public cloud, the biggest threat is the potential security issues due to multiuser nature of public clouds. This is because of the users that use them over the Internet on a pay-per-use basis share resources and costs. On the contrary, private cloud security do not have these issues. Private cloud is a cloud computing environment dedicated to a single customer. This project investigates private cloud security by developing a secure private cloud using a private server. By implementing this private cloud, a secure storage space can be provided to the cloud user with an enhanced security feature.

# ABSTRAK

Pengkomputeran awan menjadi norma yang lebih popular untuk mengakses sumber pengkomputeran. Keselamatan pengkomputeran awan atau juga dikenal sebagai keamanan awan juga dapat didefinisikan sebagai langkah-langkah keamanan yang dikonfigurasi untuk melindungi data awan, mendukung pematuhan peraturan dan melindungi privasi pelanggan serta menetapkan peraturan pengesahan untuk pengguna dan perangkat individu. Namun, ketika menggunakan awan awam, ancaman terbesar adalah masalah keselamatan yang berpotensi kerana sifat awan awam yang pelbagai. Ini kerana pengguna yang menggunakannya melalui Internet secara bayar per penggunaan berkongsi sumber dan kos. Sebaliknya, keselamatan awan peribadi tidak mempunyai masalah ini. Awan peribadi adalah persekitaran pengkomputeran awan yang didedikasikan untuk satu pelanggan. Projek ini menyiasat keselamatan awan peribadi dengan mengembangkan awan peribadi yang selamat menggunakan pelayan peribadi. Dengan menerapkan awan peribadi ini, ruang penyimpanan yang selamat dapat diberikan kepada pengguna cloud dengan fitur keamanan yang ditingkatkan.

# TABLE OF CONTENTS

**PAGE**

# LIST OF TABLES

**PAGE**

## LIST OF FIGURES

**PAGE**

# CHAPTER 1: INTRODUCTION

## 1.1 Introduction

Cloud computing was first introduced on August 9, 2006 by Google CEO Eric Schmidt. Cloud computing is the distribution of computing resources. On the Internet, which includes servers, storage, databases, networking, applications, analytics, and intelligence. Customers use cloud computer on a daily basis, sending an email, watching movies or TV, editing documents, playing games, listening to music or storing pictures and other files, is mostly done by using cloud computing. Customers also store their important data over the internet to an offsite cloud storage system that is accessible from any device and location. Cloud security is crucial as customers want to be sure that their data stored in the cloud are safe. Cloud security, also called cloud computing security, is a set of policies, controls, procedures, and technologies that work together to safeguard cloud-based applications, data, and infrastructure. These protection mechanisms are set up to protect cloud data, help regulatory enforcement, protect consumer privacy, and set up authentication rules for individual users and devices.



There are three different types of primary cloud environments. The three different environments are public cloud services, private clouds and hybrid clouds. In public cloud services, identity management, authentication, and access control are critical since they are hosted by third-party cloud service providers and are typically accessible via web browsers. Examples are for this type of environments are Amazon Web Services (AWS), Microsoft Azure, Google Cloud. Private cloud is when the provider provides exclusive access and usage rights on the infrastructure and computational resources to its consumers. The cloud infrastructure and resources may be hosted in consumer premises or outsourced to a third-party hosting organization and so can be

managed by the consumer or by the third party by Rakesh Kumar and Rinkaj Goyal (2019). Hybrid cloud is a composition of two or more clouds (public, on-site private, on-site community, off-site private and off-site community). The individual clouds in composition remains a distinct entity but provide standard or proprietary interfaces for application and data portability between them by Rakesh Kumar and Rinkaj Goyal (2019).

Knowing this, some organizations or companies use the cloud services to store crucial data and information. With cloud computing services, organizations or companies can extremely access data easily at any location and device, maintain consistency between users, allows for remote programs, easy data backup and many more.

However, finding the most suitable and secure type of cloud computing service can be a formidable task because all the different types of cloud computing environment have great benefits. For this research the researcher will focus on private cloud computing environment.

## 1.2 Problem Statement (PS)



Almost every company has incorporated cloud computing into their operations to various degrees. With the introduction of the cloud, however, comes the need to ensure that the organization's cloud protection policy is capable of defending against the top cloud security threats. Cloud data breaches are often caused by misconfigured cloud security settings. Other than data breaches, unauthorized access often occurs in cloud computing system. Many companies' cloud protection posture management policies are insufficient to safeguard their cloud-based infrastructure. Cloud-based deployments, unlike on-premises networks, are outside the network perimeter and directly available from the public Internet. While external data sharing is an amazing feature, it can also be a crucial cloud security risk. Table 1.1 illustrate the summary of problem statement

Table 1.1: Summary of Problem Statement

| PS | Problem Statement |
|---|---|
| PS1 | Data breaches are often caused by misconfigured cloud security settings. |
| PS2 | Unauthorized access often occurs in cloud computing system. |
| PS3 | External data sharing can also be a crucial cloud security risk. |

## 1.3 Project Question (PQ)

In cloud computing, we need to study what is the differences between available models in deep learning. Next, conducting research on the available methods and techniques that can be used or enhanced to mitigate problems stated in Table 1.1. Next, implementing knowledge gained from the research that has been made to show proof of concept is achieved successfully. Table 1.2 shows the summary of project questions.

Table 1.2: Summary of Project Questions



| PS | PQ | Project Question |
|---|---|---|
| PS1 | PQ1 | Which type of cloud computing environment is more secured? |
| PS2 | PQ2 | How to store data in cloud computing system securely? |
| PS3 | PQ3 | Does private cloud computing ensure the confidentiality, integrity and availability of the data? |

## 1.4 Project Objective (PO)

The project will take two objectives to determine that the project done properly and accomplished to the get the required output as issued in the preceding section. The table 1.3 displays the summary of project objective.

Table 1.3: Summary of Project Objective

| PS | PQ | PO | Project Objective |
|---|---|---|---|
| PS1 | PQ1 | PO1 | To compare the security criteria of a cloud computing system that is suitable to store sensitive data. |
| PS2 | PQ2 | PO2 | To store sensitive data using private cloud computing. |
| PS3 | PQ3 | PO3 | To evaluate if private cloud computing security system ensures the confidentiality, integrity and availability of the data. |



## 1.5 Project Scope

The project focused on the security and the benefits of the private cloud security environment in protecting the information stored in the cloud. The process will include creating a private cloud security using Tonido software.

## 1.6 Project Contribution (PC)

Nowadays, cloud computing security is the most widely used service of this era. Organizations with a private cloud have more leverage over security procedures and problems like data residency. In general, due to their familiarity with and understanding of the entire technology solution, private cloud administrators are better able to handle compliance issues. Thus, by using the best approaches and solution it could increase the security and protection for the data and information stored in the cloud.

## 1.7 Report Organization

Chapter 1: Introduction

This chapter contains the introduction, problem statement, project question, project objective, project scope, and project contribution

Chapter 2: Literature Review

This chapter contains the description and the explanation of the project with supporting article, journal, books, and websites.

Chapter 3: Project Methodology

Contain workflow or method to complete the project.

Chapter 4: Analysis and Design

This chapter contains all the design of the project, including the architecture design of the private cloud computing system.

Chapter 5: Implementation

This chapter contains on how I implement the private cloud computing security system.



Chapter 6: Testing and Validation

Contain the testing of the private cloud computing security system for its confidentiality and integrity

Chapter 7: Project Conclusion

Summarize the whole project and what improvement it can do for the future.

## 1.8 Conclusion

To summarize, the purpose of this chapter is to describe the general background and better understanding of the project proposes, how it can help customers and organizations secure and protect important and critical data

into the cloud server and minimize the risk and threats. This research will be focusing on private cloud and its benefits.

# CHAPTER 2: LITERATURE REVIEW AND PROJECT METHODOLOGY

## 2.1 Introduction

The comprehensive chapter will give information in detail on literature studies on cloud computing, cloud computing security and types of cloud computing services. Furthermore, the literature review expresses every single thing affiliated to the research in particulars of definition, architecture, advantages and disadvantages of each method. Moreover, this chapter will also describe the types cloud computing security and tools being used to implement this project. Therefore, this chapter needs to explain the details of the preceding work that implemented research which most alike to the research and development that is currently implementing. Lastly, this part will contrast the method that will be used to the methods of the preceding work.



## 2.2 Keyword

**Cloud computing:** Cloud computing is the transmission of computer services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud") in order to enable faster innovation, more flexible resources, and cost savings.

**Cloud computing security:** Cloud security, often referred to as cloud computing security, is a collection of rules, controls, procedures, and technologies that work together to safeguard cloud-based systems, data, and infrastructure.

**Private cloud:** Computing services provided to a chosen group of users rather than the broader public via the Internet or a private internal network.

**Public cloud:** The public cloud is described as computer services made available to anyone who wishes to use or buy them through the public Internet by third-party providers.

**Hybrid cloud:** A hybrid cloud system is one that mixes a private cloud with one or more public cloud services, with proprietary software allowing communication between them.

## 2.3 Cloud Computing

Cloud computing virtualization technology provides end users with efficient resources. Manageability, scalability, and availability are all properties of cloud computing. Furthermore, cloud computing offers cost savings, on-demand service, convenience, universality, multi-tenancy, flexibility, and stability. Three service delivery methods and three development patterns are primarily provided by cloud computing. Platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS), public cloud, private cloud, hybrid cloud. Iaas treats computer hardware (network storage, virtual server/ computer, data center, processor and memory) as a service and provides infrastructure scalability and provisioning issues without requiring significant capital and time (PanJun Sun, 2020). IaaS also focuses on security features such as firewalls, virtual machine monitoring, intrusion detection, and other areas. PaaS locates in the middleware of the service model and provides services in the form of development tools, frameworks, architectures, programs and integrated development environments (PanJun Sun, 2020). Third-party partnerships, lifecycle development, and underlying infrastructure security are just a few of the problems that PaaS faces. SaaS is a collection of remote computing services that enables thirdparty vendors to remotely deploy applications (PanJun Sun, 2020). Customers can access cloud service provider apps on the cloud infrastructure over the Internet. Private cloud is the provider provides exclusive access and usage rights on the infrastructure and computational resources to its consumers. The cloud infrastructure and resources may be hosted in consumer premises or outsourced to a third-party hosting organization and so can be managed by the consumer

or by the third party by Rakesh Kumar and Rinkaj Goyal (2019). Besides that, it provides businesses with many of the benefits of a public cloud, such as self-service, scalability, and elasticity, as well as the additional control and customization available from dedicated resources over an on-premises computing infrastructure. Public cloud is this deployment model the provider provides cloud services to a diverse pool of cloud consumers and so is named as public. The services are provided over a public network (wireless or wireline) by Rakesh Kumar and Rinkaj Goyal (2019). Storage capabilities, apps, and virtual machines are examples of resources that differ per provider. The public cloud enables scalability and resource sharing that would be impossible for a single company to achieve otherwise. Hybrid cloud is a composition of two or more clouds (public, on-site private, on-site community, off-site private and off-site community). The individual clouds in composition remains a distinct entity but provide standard or proprietary interfaces for application and data portability between them by Rakesh Kumar and Rinkaj Goyal (2019). Hybrid cloud services are advantageous because they provide companies more control over their sensitive data. An organisation can store sensitive data in a private cloud or local data centre while also taking advantage of the managed public cloud's powerful processing resources. Unlike a multi-cloud architecture, where admins must manage each cloud environment independently, a hybrid cloud relies on a single plane of management. Figure 2.1 shows the cloud computing framework.

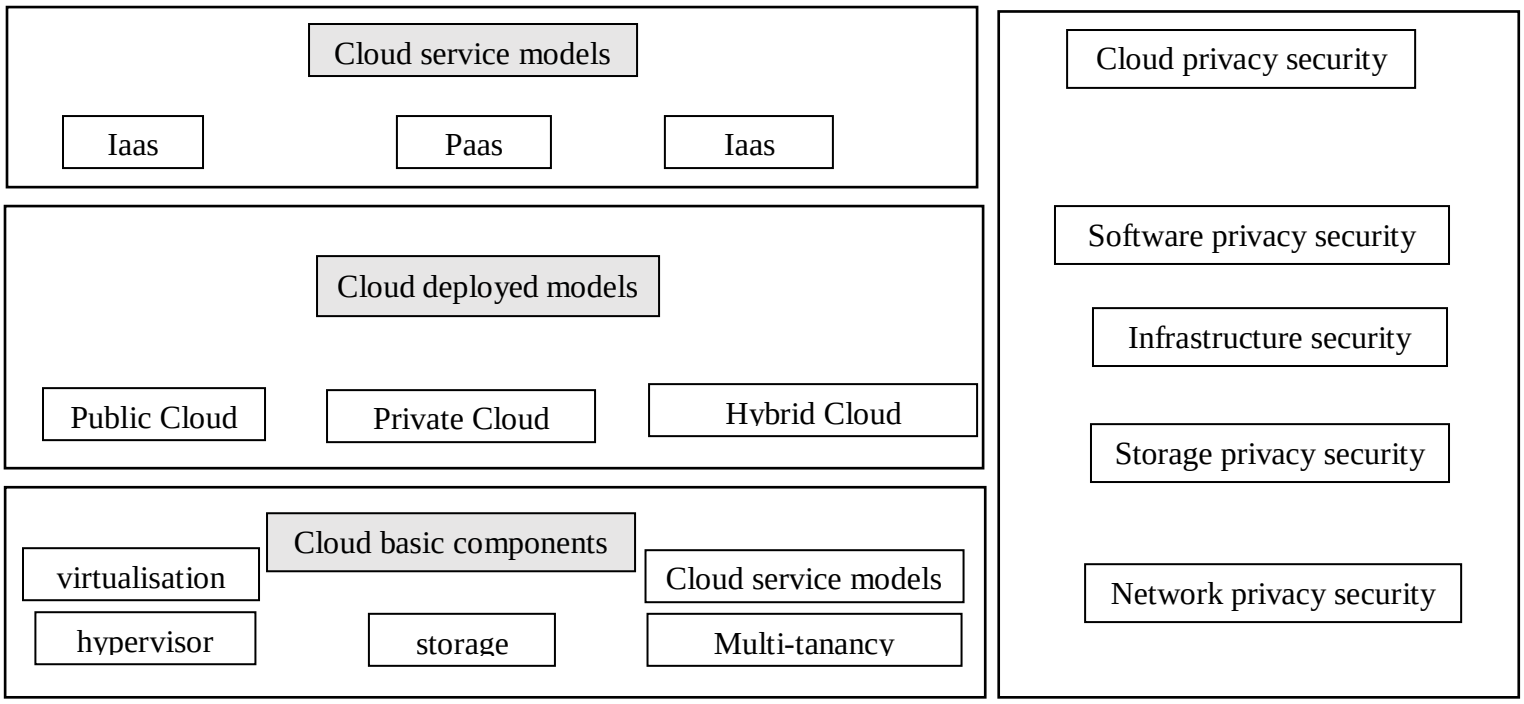


Figure 2.1: Cloud computing network

## 2.4 History of cloud computing

Prior to the advent of cloud computing, there was Client/Server computing, which is essentially a centralised storage system in which all software applications, data, and controls are stored on the server side. If a single user needs to access specific data or run a programme, he or she must first connect to the server and get authorised access before proceeding. In a speech at MIT in 1961, John MacCharty proposed that computer be sold as a utility, similar to water or electricity. It was a fantastic idea, but like many excellent ideas, it was ahead of its time, as despite interest in the model, technology was simply not ready for it for the following few decades.

## 2.5 Related work

Based on PanJan Sun (2020) research paper, the main sources of security issues are the fundamental aspects of the cloud computing environment. First, the computational nodes are heterogeneous, sparsely distributed, and frequently inaccessible to effective control. Second, the cloud service provider (CSP) runs the risk of revealing personal information throughout the transmission, processing, and storage of data. Because cloud computing is dependent on

technology, existing technological security flaws will be directly transferred to a cloud computing platform, posing even more security risks. The confidentiality and privacy protection of information is a consistent necessity of security, from information security to network security to cloud computing security. We may deduce many threats to privacy security risk based on the annual report of the Cloud Security Alliance (CSA) and the study results of relevant scholars in the literature. The security risk of cloud privacy, such as data revelation, privacy disclosure, access rights management, and data deletion challenges, is particularly important due to the service outsourcing method. Access control and identity authentication: Because cloud computing uses a lot of resources, access control and identity authentication administration becomes a lot more complicated.

Meanwhile based on Nureni Ayofe Azeez and Charles Van der Vyver (2019), private cloud is the most secured model out of the three models. According to Nureni Ayofe Azeez and Charles Van der Vyver (2019), this model is considered the most secured of all the models. There is a complete restriction to the public internet. The Electronic Medical Records (EMRs) in a private cloud can only be accessed by healthcare staff who have been identified as trustworthy and reliable. For public cloud, this model consists of shared infrastructure that is in total control of the third-party provider by Nureni Ayofe Azeez and Charles Van der Vyver (2019). Cloud Service Providers (CSPs) provide the services for this type of cloud system. Electronic Health Record EHRs are typically shared among several organisations under this paradigm. Because EHRs are stored on off-premises servers under the control of CSPs, they are extremely vulnerable to numerous attacks and manipulations. Effective cryptographic algorithms and fine-grained access control systems are necessary to overcome this security dilemma. Figure 2.2 shows public cloud for electronic health.

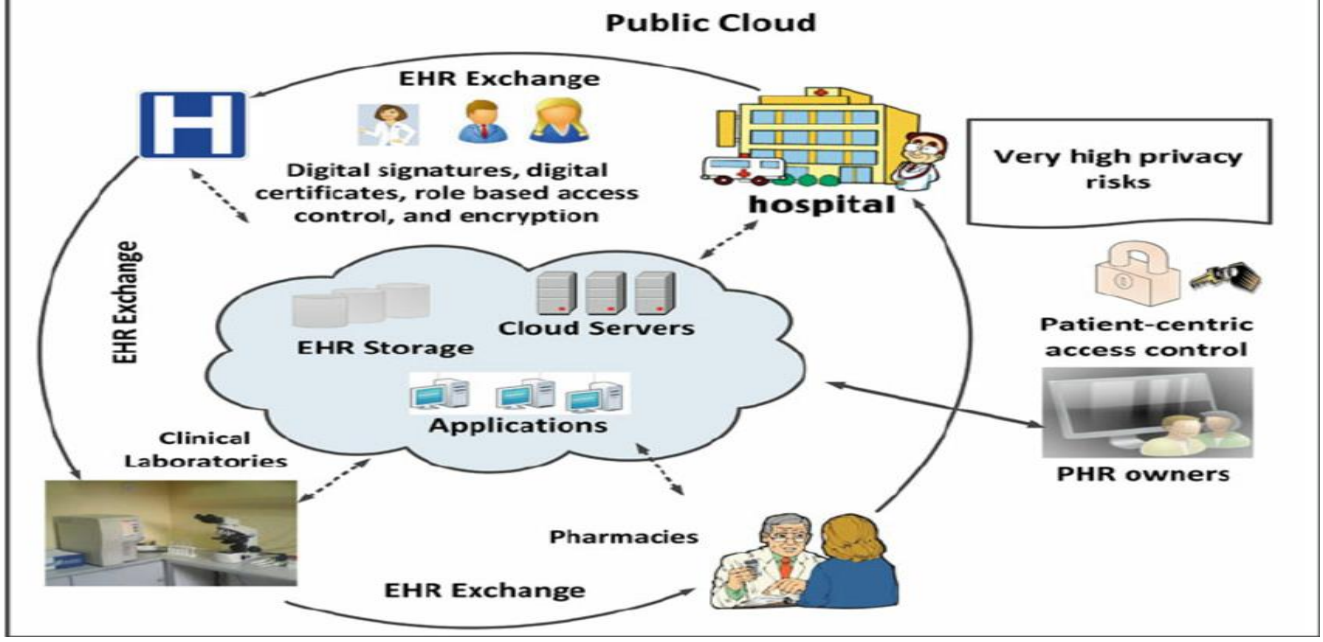


Figure 2.2: Public cloud for electronic health

In another research done by Rakesh Kumar and Rinkaj Gopal (2019), as with any other information security management system, NIST (National Institute of Standards and Technology) has listed confidentiality, integrity, and availability as essential cloud security requirements. It includes additional cloud security requirements such as authentication, authorization, responsibility, and privacy. In their article on cloud security requirements, the CSA stressed the same point. The researchers at the Cloud Security Alliance (CSA), a cutting-edge group that provides cloud security counsel to the cloud community, have been identifying and analysing risks to the cloud ecosystem, and have published a series of publications on top cloud risks.

## 2.6 Method

It is nearly difficult to go through all of the available literature on benefit of private cloud security. As a result, we were able to review a number of articles. After selecting over twenty original publications, the literature study was conducted, and many models used in their solutions were identified. We obtained twenty publications from Science Direct digital libraries in order to obtain a reasonable and substantial quantity of reviewed articles. Other papers were obtained from the digital libraries of Springer, Elsevier, and Science

Direct. Only a few publications were downloaded from publications that were not as well-known or ranked as the ones indicated. Because of similarities in the models used by several researchers, the number of peer-reviewed articles was reduced to the current number. We examined and analyzed the strengths of each of the strategies used in finding a solution to the benefits of private cloud security in the papers. After that we created our own private cloud and run some tests on it. By creating users and sharing files only that certain users can open.

## 2.7 Proposed solution

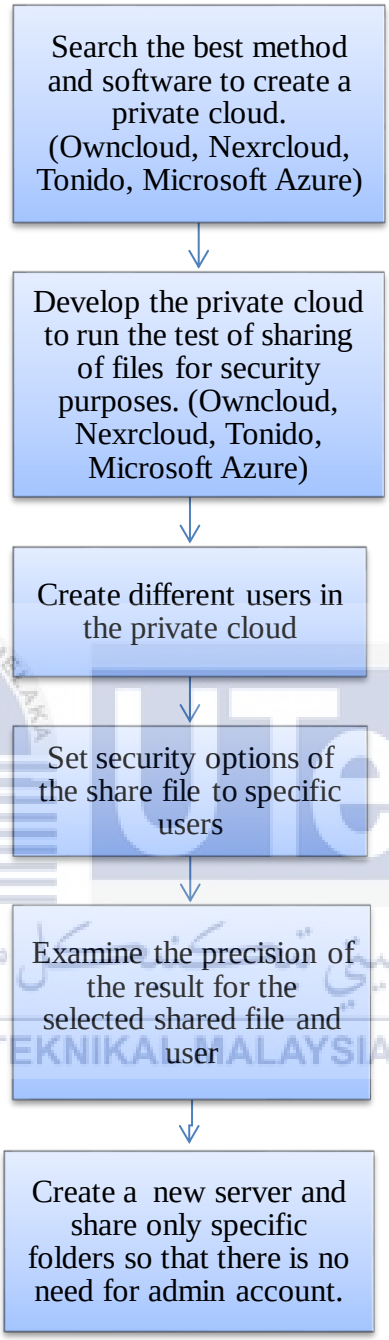


Figure 2.3: Overview of propose solution.

## 2.8 Conclusion

This chapter is about this project's literature review. It symbolizes the project's written survey. Citations and sources of information for the literature review are gathered from many sources that are suitable to be used. The next chapter will explain more in detail in designing the proposed solution.

# CHAPTER 3: ANALYSIS

## 3.1 Introduction

Previously, the literature reviews are discussed and explain in the chapter 2. This chapter will be focus on discussing the related work research on this project. According to Merriam-Webster describes “Methodology” as a set of methods, rules, and postulates that a discipline employs: a specific procedure or set of procedures.

## 3.2 Methodology

This project will utilize the following waterfall method as shown in the figure below. The main purpose of using the waterfall model is that it is based on the sequence of phases and activities that must be complete in order to proceed to the next phases. The chosen model gives a clear insight of what the researcher should do in every phase and it very helpful to complete the task in order to achieve the final goal of the study. Figure 3.1 shows the waterfall method.

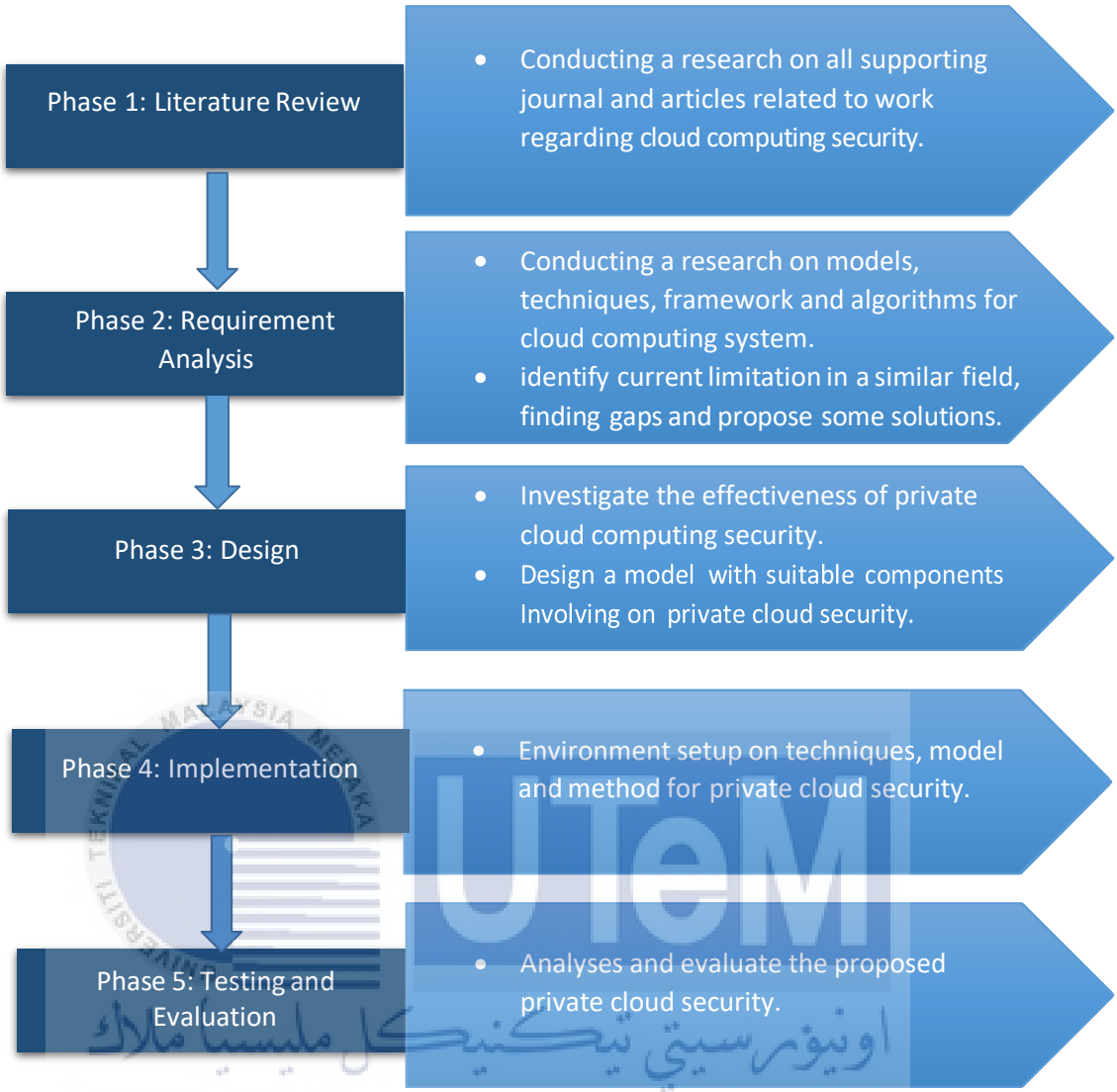




Figure 3.1: Project Methodology

### 3.2.1 Phase 1: Literature Review

This phase is about a process of literature review which the researcher will gather all supporting journals, articles, and related work regarding sentiment analysis on Twitter data. This literature will be used as guide and proper reference about the topic of the study.

### 3.2.2 Phase 2: Requirement Analysis

All the required software, hardware and tools needed will be listed down in this phase:

I. Setup environment

The cloud computing software which is Tonido and all required tools will be installed on the Windows desktop in this project. The hardware will be used is the Acer Aspire e15 specs e5-575g-71mn. The details of the Acer Aspire e15 specs e5-575g-71mn are given in Table 3.1 below.

Table 3.1: Acer Aspire e15 specs e5-575g-71mnSpecifications

| Specification | Details |
|---|---|
| Processor | Intel(R) Core(TM) i7-7500U CPU @ 2.75GHz with Turbo Boost up to 3.5GHz |
| Cache Memory | L3 cache - 3.0 MB |
| Storage | 1TB |
| Memory | 4.00 GB DDR4 Memory |
| RAM | 4.00 GB |
| Networking | Ethernet, WLan, |



II. Develop the system

The cloud computing software which is Tonido will be installed after setting up the environment is done.

III. Executing the cloud computing system

After the environment has successfully been set up, the private cloud will be tested by sharing certain folders to certain users. All the data will be evaluated based on its confidentiality and integrity.

### 3.2.3 Phase 3: Design

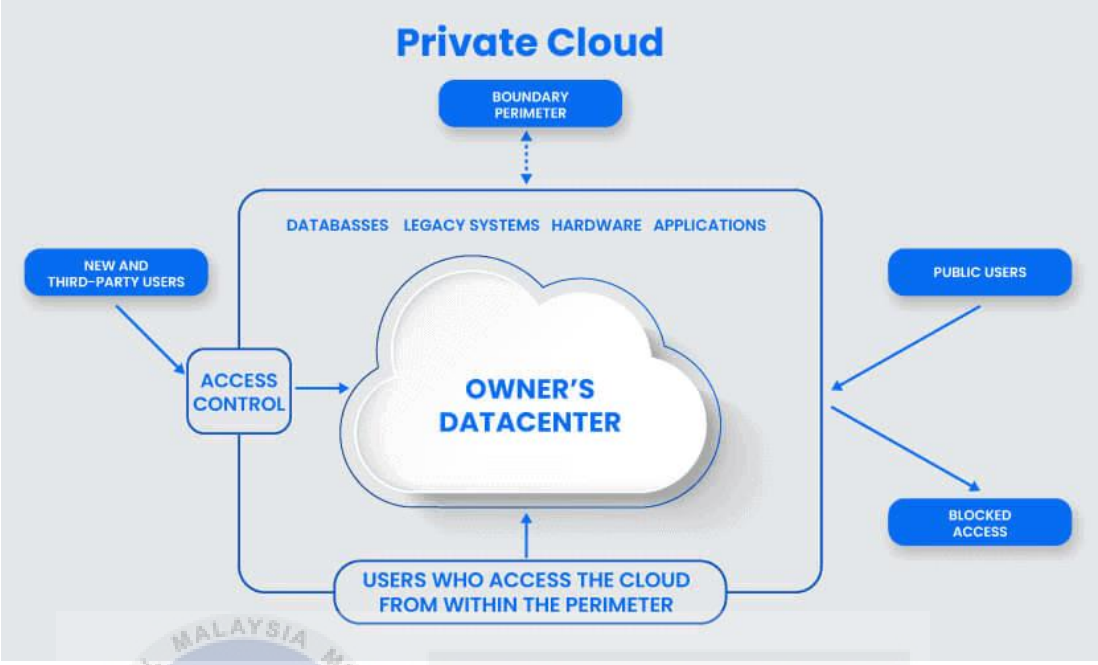


Figure 3.2: Private cloud model

A private cloud is a single-tenant environment, which means that the tenant does not share resources with other users. Those resources can be managed and hosted in a number of ways. The private cloud could be built on existing resources and infrastructure in an organization's on-premises data center or on new, distinct equipment offered by a third-party provider. In some circumstances, virtualization software is used to create a single-tenant environment. In any case, a single user or tenant has access to the private cloud and its resources.

### 3.2.4 Phase 4: Implementation

This method is used to implement of the process of private cloud security system.

I. System development.

II. Testing of sharing of documents and files in the private cloud system.

III. Evaluating of the confidentiality and integrity.

### 3.2.5 Phase 5: Testing and evaluation

Under testing phase, verification will be done to verify whether the proposed model gives high security for data storing and sharing. In evaluation phase, comparison will be made between others related work from previous researcher to see differences of security between different model.

## 3.3 Project schedule and milestone

The timeline along this research project will be Project Milestone. It will allocate the specific time from beginning to the end of this research project for each phase. In addition, the Gant chart is the chart with a series of horizontal lines specifying the amount of time or time for specific tasks.

Table 3.2: Project Milestone

| No | Date | Activity | Description |
|---|---|---|---|
| 1 | 15/4/2021 | Phase 1: Literature Review | • Conducting a research on all supporting journal and articles related to work regarding cloud computing security.<br>• Identify current limitation in a similar field, finding gaps and propose a solution. |
| 2 | 20/5/2021 | Phase 2: Requirement Analysis | • Focusing the requirements on models, framework and algorithms for cloud computing security. |

| | | | |
|---|---|---|---|
| 3 | 5/6/2021 | Phase 3: Design | • Investigate the most effective of cloud computing models.<br>• Design a model with suitable components involving private cloud. |
| 4 | 10/7/2021 | Phase 4: Implementation | • Environment setup on private cloud system. |
| 5 | 20/7/2021 | Phase 5: Testing and Evaluation | • Analyses and evaluate the security, confidentiality and integrity of private cloud system. |

Table 3.3: Project Gantt chart

| **Activity/Week** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** | **11** | **12** | **13** | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phase 1: Literature Review | | | | | | | | | | | | | | |
| Phase 2: Requirement Analysis | | | | | | | | | | | | | | |
| Phase 3: Design | | | | | | | | | | | | | | |
| Phase 4: Implementation | | | | | | | | | | | | | | |
| Phase 5: Testing and Evaluation | | | | | | | | | | | | | | |

## 3.4 Conclusion

This section offers an overview of the present stage in the execution of this project. This waterfall model is intended for assessment, design phase, development phase, execution phase, as well as testing phase and documentation phase. The design of the project will be reviewed in the next section.

# CHAPTER 4: DESIGN

## 4.1 Introduction

This chapter will deeply analyze the overview of the assignment to be carried out. In the previous chapter, a brief explanation is provided for the waterfall model which will be tailored to the job development studies. This will therefore illustrate the important part for this research which is model for logical and physical structure, system UI design and then explain how the system works.

## 4.2 Project Requirement

This subchapter cites the project specification that will be used in this project. This requirement must be made to complete the project's flows in time.

### 4.2.1 Hardware Requirement

This project would include the private cloud system on a Windows desktop. The Acer Aspire e15 specs e5-575g-71mn will become the hardware used. Table 4.1 below gives the detailed information on the Acer Aspire e15 specs e5-575g-71mn.

Table 4.1: Acer Aspire e15 specs e5-575g-71mnSpecifications

| Specification | Details |
|---|---|
| Processor | Intel(R) Core (TM) i7-7500U CPU @ 2.75GHz with Turbo Boost up to 3.5GHz |
| Cache Memory | L3 cache - 3.0 MB |
| Storage | 1TB |

| | |
|---|---|
| Memory | 4.00 GB DDR4 Memory |
| RAM | 4.00 GB |
| Networking | Ethernet, WLan, |

### 4.2.2 Software Requirement

Software that will be used during the execution of this project are listed below:

i. Windows Desktop

Windows is an operating system that owns by Microsoft, is a group proprietary graphical operating system family.

ii. Tonido Server

A free cloud server software. Turn your computer into your own personal cloud server. Sync and remotely access files via web browser, mobile devices.



## 4.3 Design

This subtopic will explain the architecture, physical and logical design for this project.

### 4.3.1 Architectural design

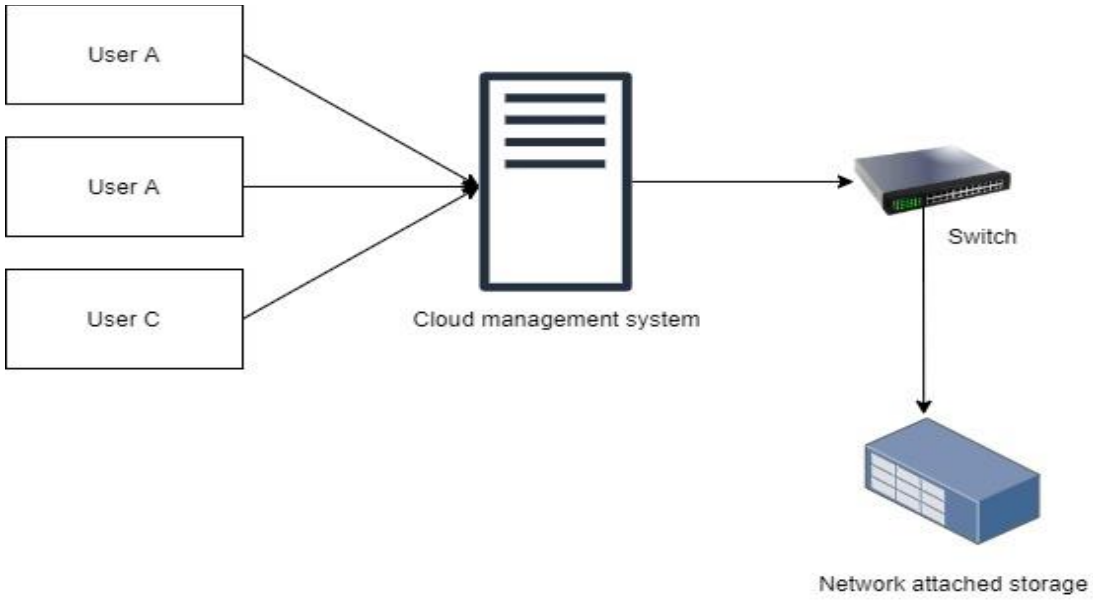


Figure 4.1: Architectural design

Figure 4.1 shows the architectural design. A private cloud is a single-tenant environment, which means that the company utilizing it (the tenant) does not share resources with other users. Those resources can be hosted and handled in a number of different ways. The private cloud might be built on existing resources and equipment in an organization's on-premises data center or on new, independent infrastructure offered by a third-party provider. In certain situations, virtualization software is used to create a single-tenant environment. In any instance, a single user or tenant has access to the private cloud and its resources.



### 4.3.2 Physical design


Figure 4.2: Physical design

The figure 4.2 shows the physical design that will be used in this project research. The laptop acts as the company's private cloud server. The laptop is installed with the required software which is Tonido server software to run as the private cloud.

## 4.4 Flowchart

A flow chart is a graphical or symbolic representation of a process. Each step in the process is represented by a different symbol and contains a short description of the process step. This flow diagram demonstrates a moving diagram describing the information flow gathered by the data gathering and feature generation from the dataset to be train into the model. Then, pre-processing and feature selection part will take place when the model has been trained. Lastly, learning evaluation phase will take place to evaluate the data and analyzed the information data from the model

### 4.4.1 Searching for a cloud server software

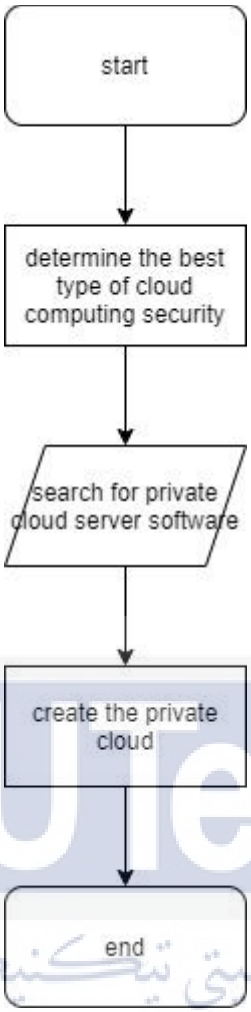




Figure 4.3: Search for a cloud server software

Figure 4.3 shows the flowchart of the process for searching for a cloud server software. In this figure states there are several processes involved in this phase.

### 4.4.2 Creating a Tonido account

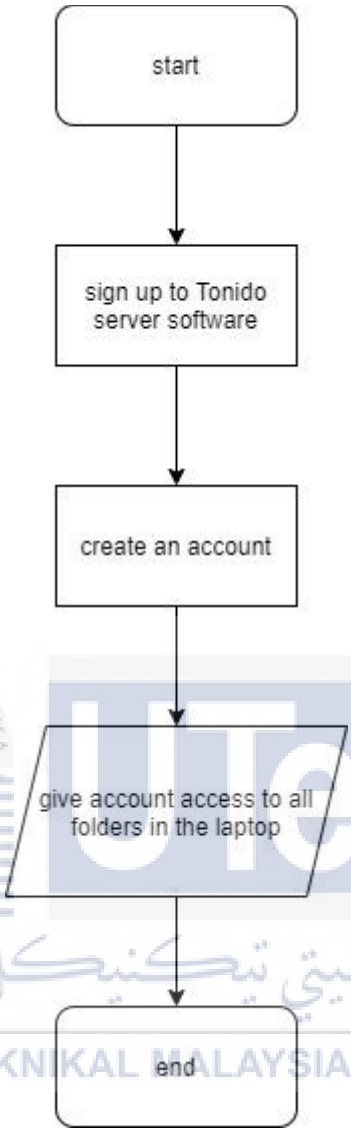




Figure 4.4: Creating a Tonido account

Figure 4.4 shows the process of creating a Tonido account. This is important as the Tonido software server will be the server for our private cloud.

### 4.4.3 Sharing data using private cloud

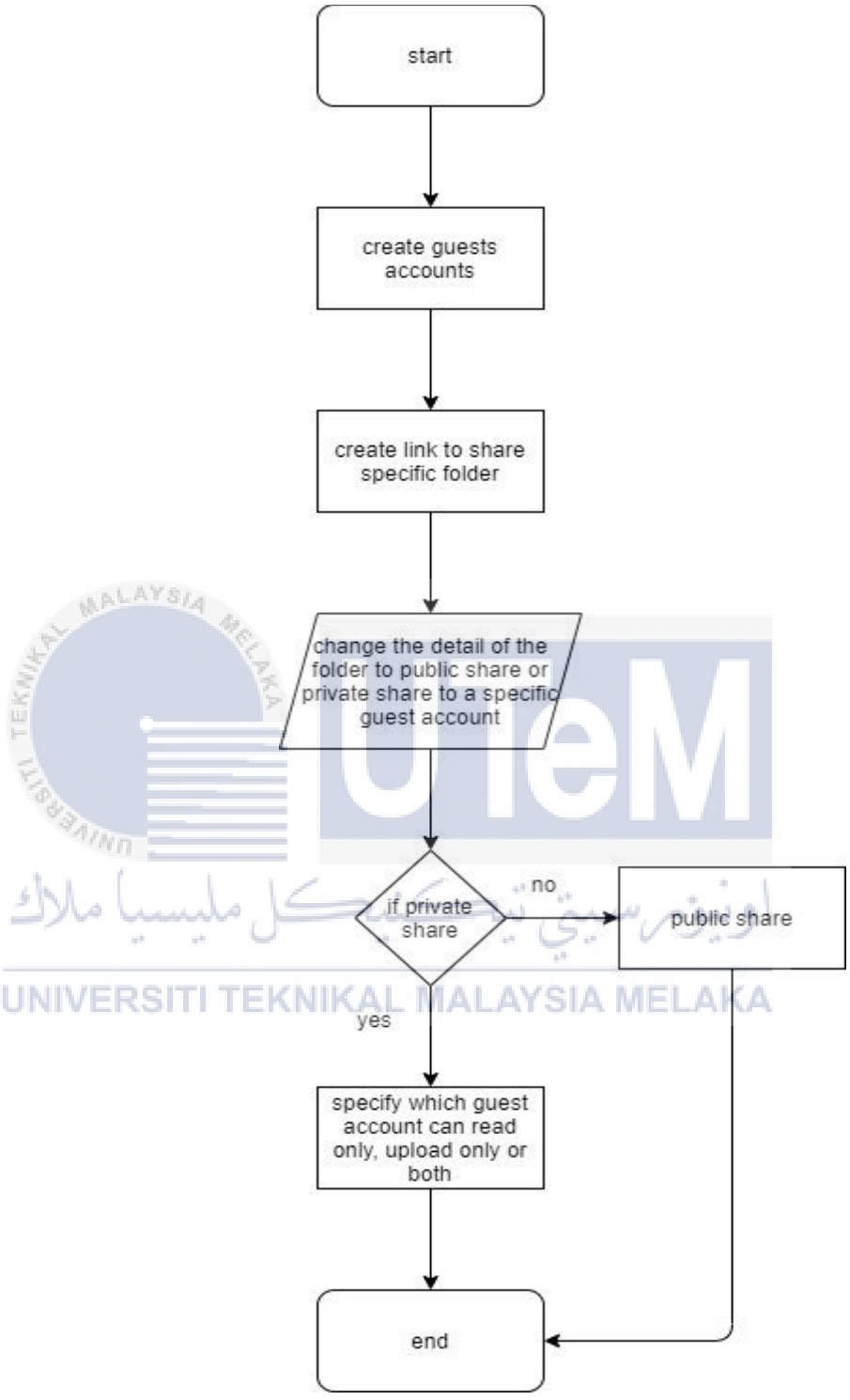




Figure 4.5: Sharing data

Figure 4.5 shows the process to share data using private cloud. The user must specify either to make it a public share or a private share. If the user chooses to make a private share then the user must give permission either to read only, upload only or both.

### 4.4.4 Analyze information

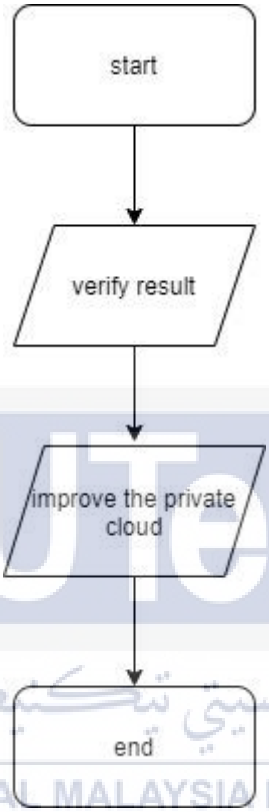




Figure 4.6: Analyze information

Figure 4.6 depict the data analyze process. In this phase the, the researcher analyzes if the sharing process is secured or not. Based on the result, the researcher will determine to improve the private cloud.

### 4.4.5 Compare result

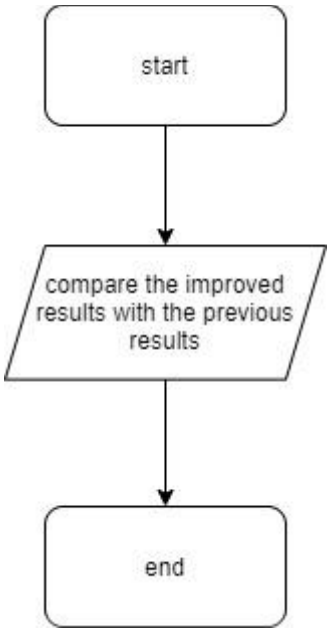


Figure 4.7: Compare result

In figure 4.7 is the compare result flow. This phase involving such activity of comparing the improved result with the previous result from the private cloud.

## 4.5 Conclusion

This chapter highlights the research design and implementation of the project flow to facilitate this section. The design is critical in ensuring that development is made in a systematic manner. This procedure is necessary in order for the project to run smoothly and efficiently.

# CHAPTER 5: IMPLEMENTATION

## 5.1 Introduction

The implementation chapter is a field that shows the implementation of the architecture and security of private cloud security using Tonido software.

## 5.2 Search and Download Cloud server software

There are several types of cloud server software available to download from the internet. For this project, Tonido cloud server software will be used for creating the private cloud. Tonido is a free cloud server software. Figure 5.1 shows the website of the Tonido cloud server software that is being used to create the own personal private cloud.

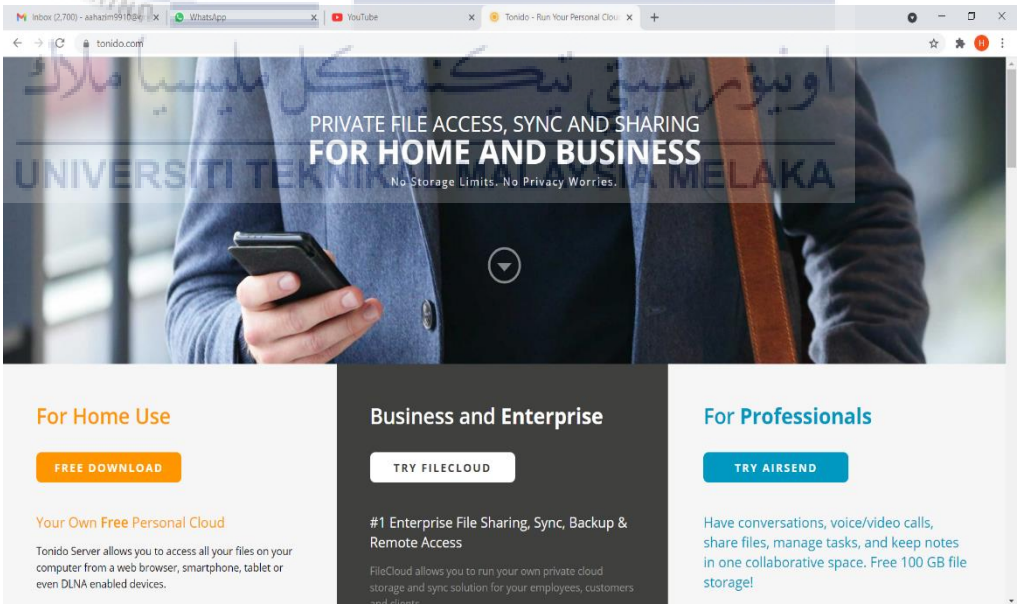


Figure 5.1: Tonido software website

## 5.3 Installation and setup for Tonido software

After downloading Tonido software, run the Tonido software and then we have to give an account name for the cloud server. After that, set the password and give an email address. Next, we need to setup the folders for remote access sharing. Tick the 'Allow remote access to all folders' and then disable indexing. Figure 5.2, figure 5.3 and 5.4 shows the steps how to setup Tonido server and the private cloud.




Figure 5.2: Tick Allow remote access to all folders

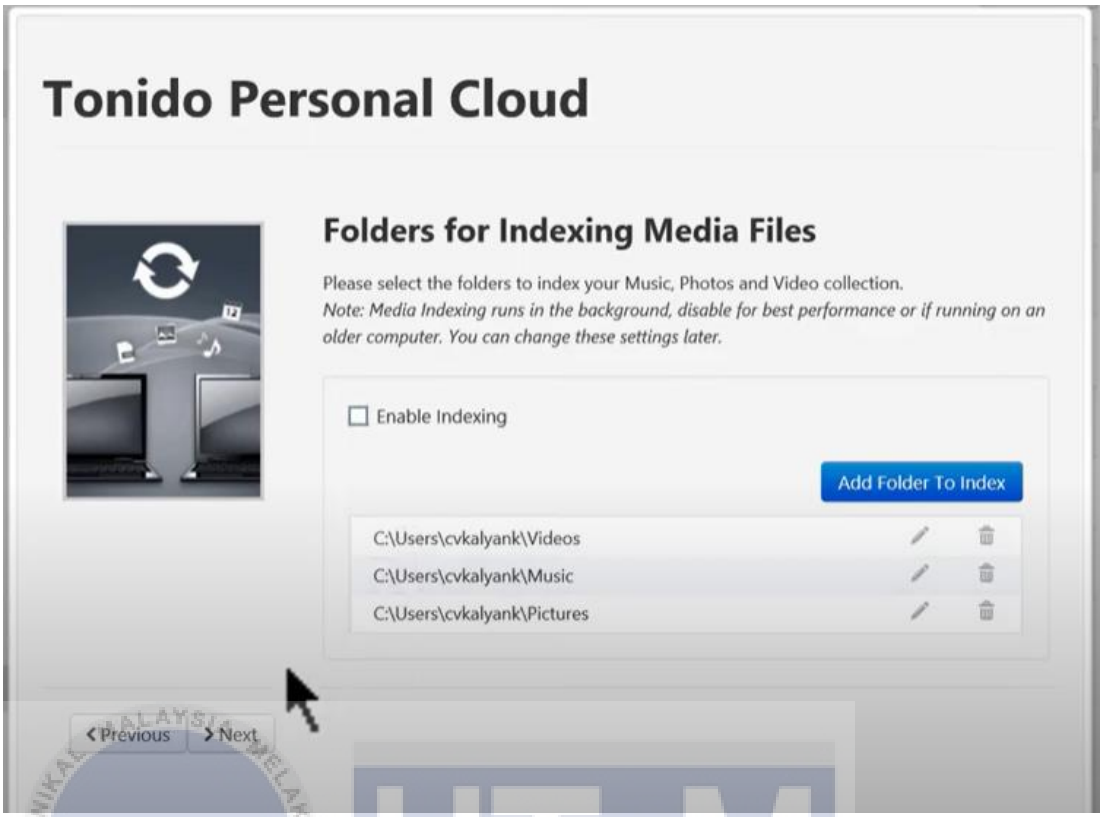


Figure 5.3: Disable indexing

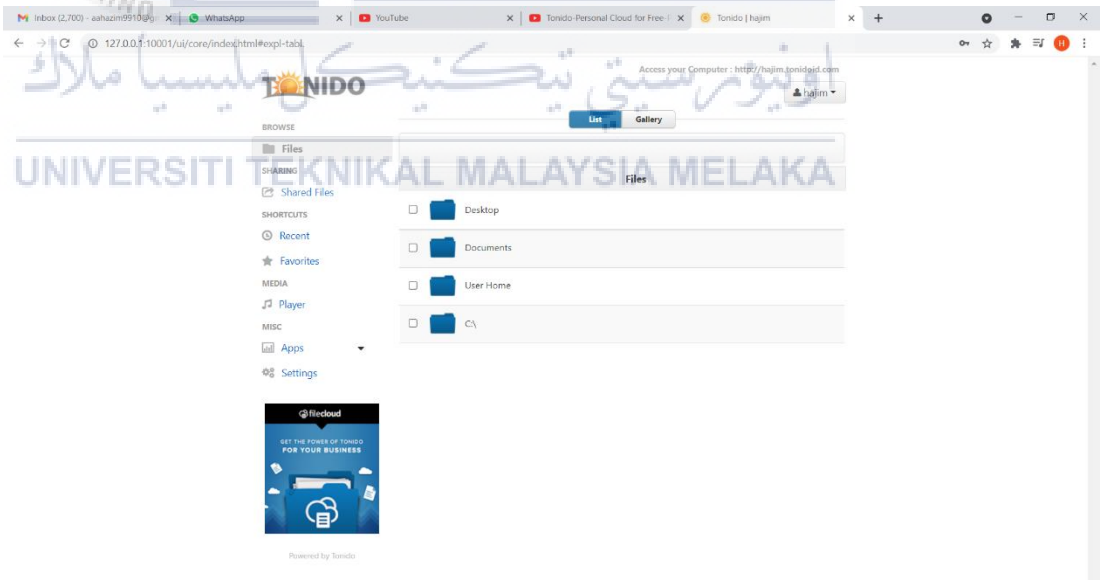


Figure 5.4: Tonido private cloud server

## 5.4 Running multiple instances of Tonido server from a single device

Running multiple Tonido servers allows the users to not need an admin. This makes the private cloud more secure because only specific users can access their specific files. First go to roaming in appdata and click the tonido folder. Click the tonido folder and copy all the files in the folder. Figure 5.5 and 5.6 shows the folder.

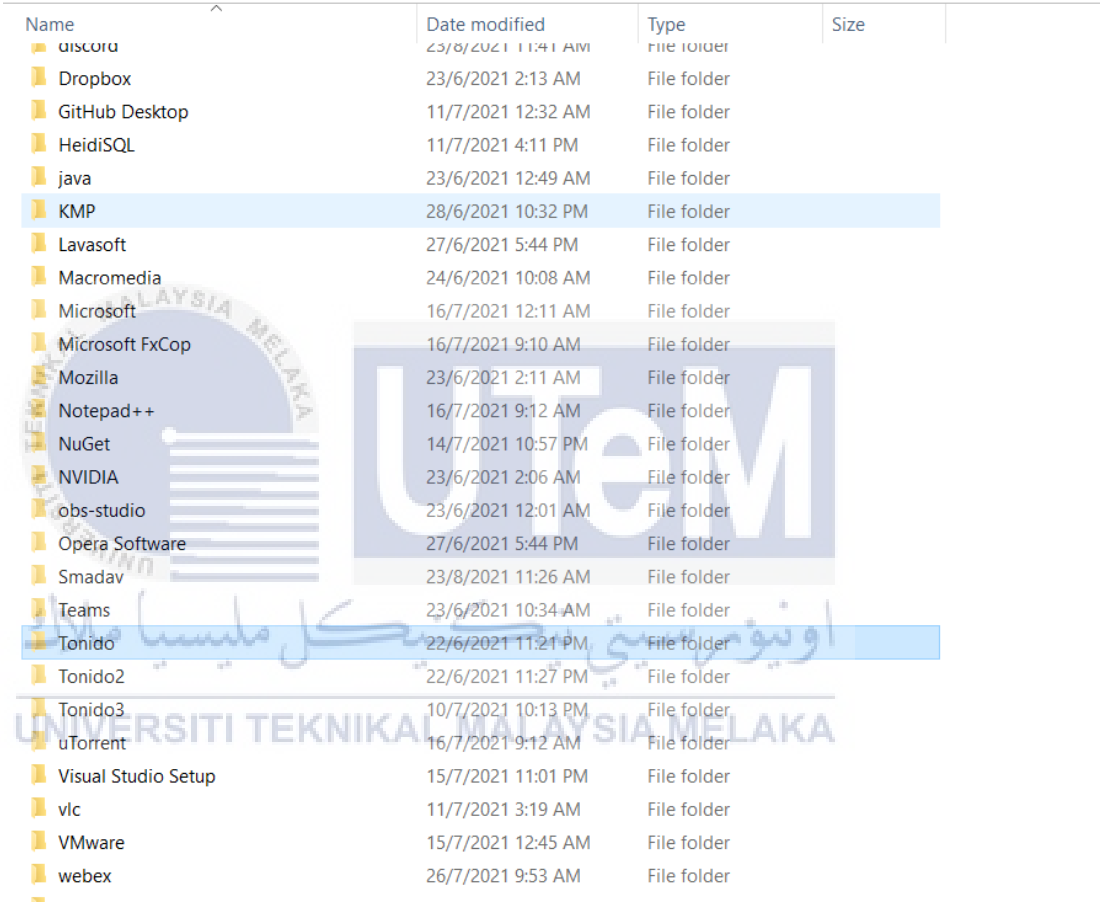


Figure 5.5: Tonido file

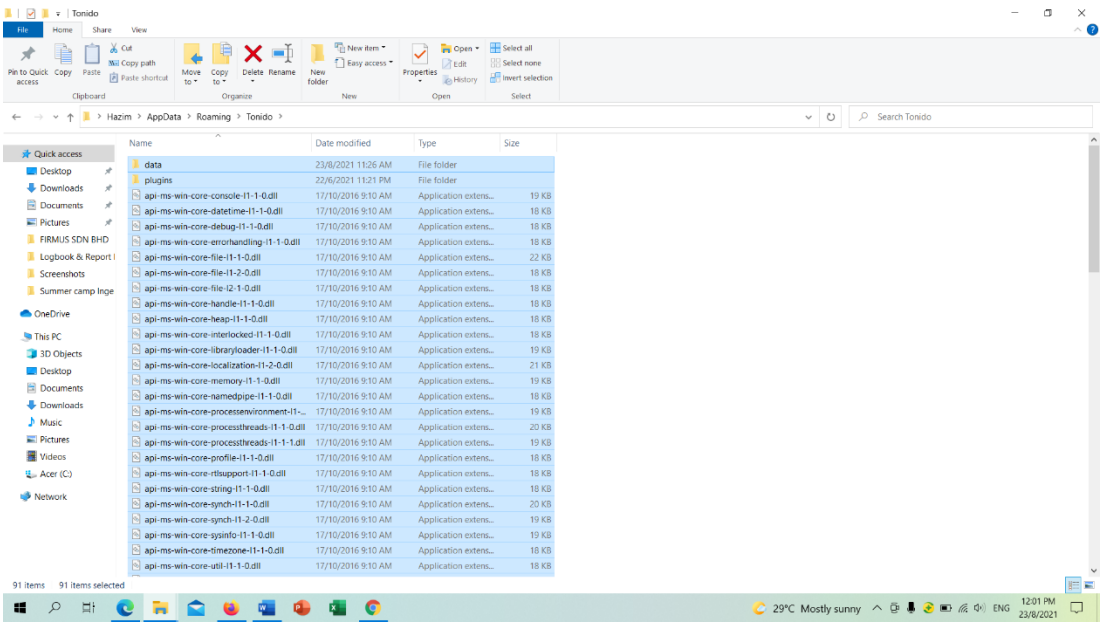

Figure 5.6: Copy all the files in the folder

Create a new folder in Roaming called Tonido4 and paste the files in Tonido4. Then search and select localconfig.xml. Open the file with WordPad. Change the HOME value to HOME3 and save it. Figure 5.7, 5.8, 5.9 and 5.10 shows the steps.

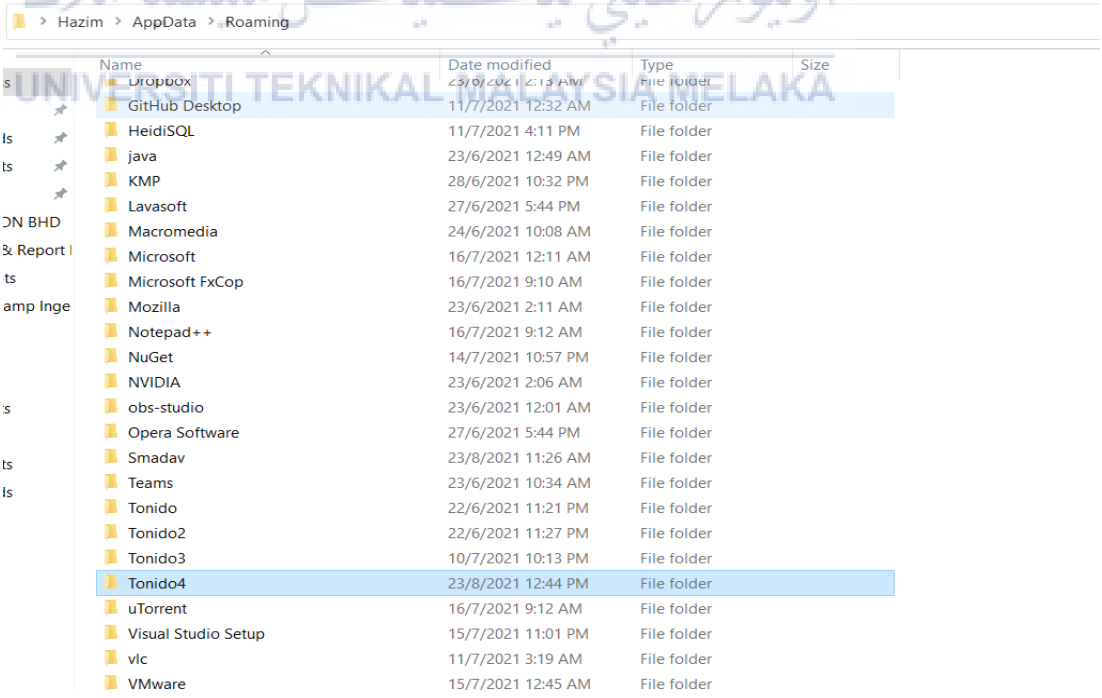


Figure 5.7: Create a folder called Tonido4

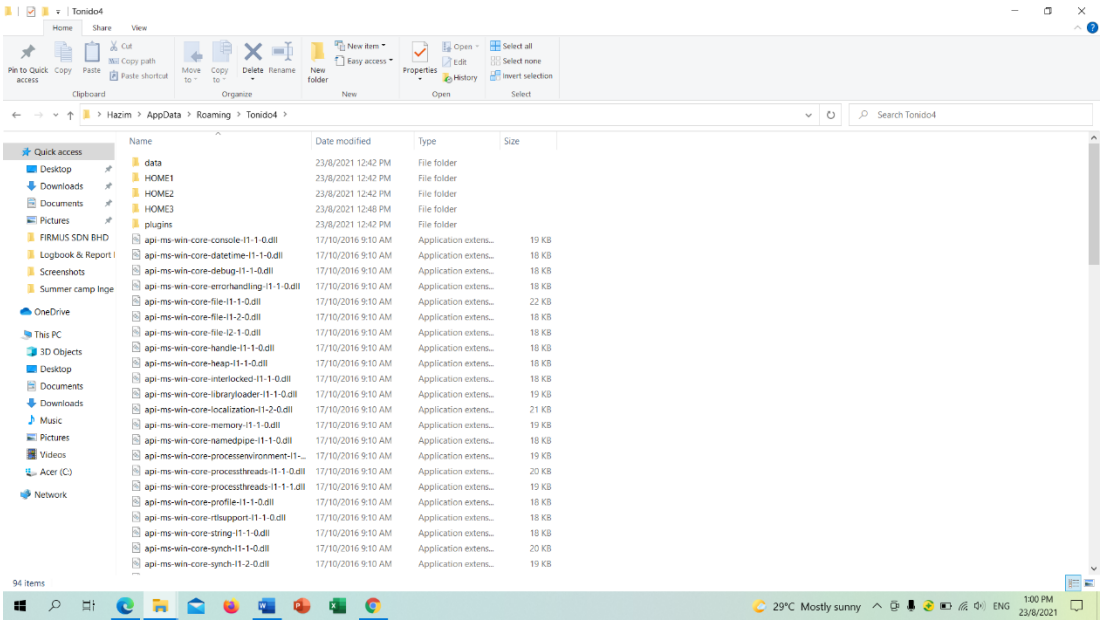

Figure 5.8: Paste the files in Tonido4

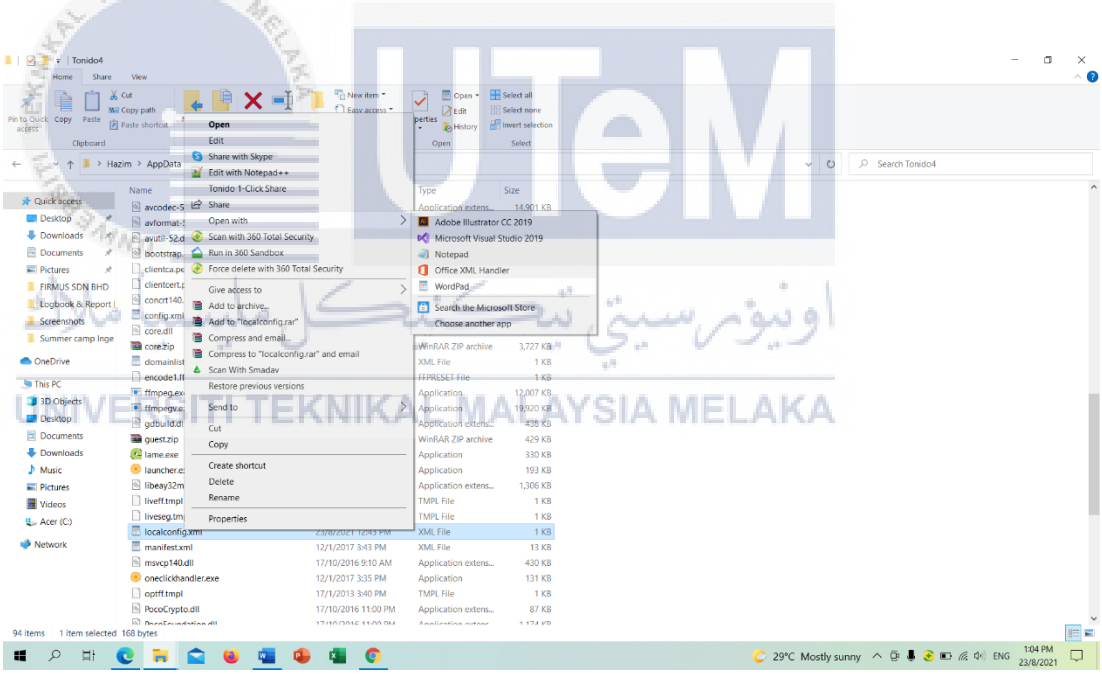

Figure 5.9: Open localconfig.xml with WordPad

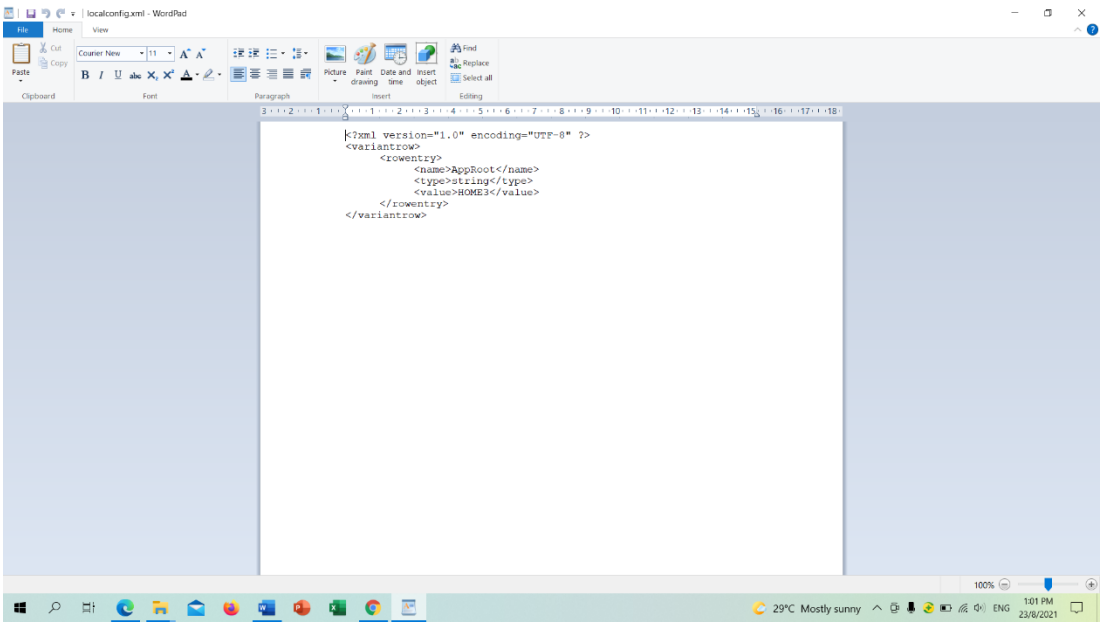


Figure 5.10: Change the HOME value to HOME3

Now go to data and look for configex.xml and open it with WordPad and change the HttpPort value to one more than the previous value. After that look for the UDPPort and give it the next value and then save. Figure 5.11, 5.12, 5.13 and 5.14 shows the steps.

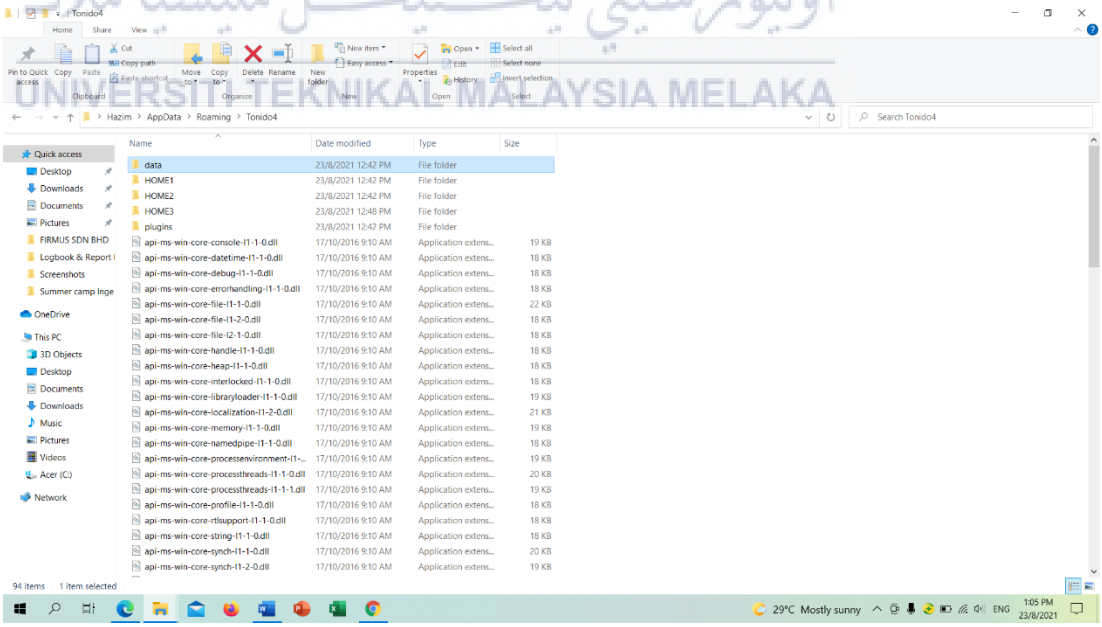


Figure 5.11: data folder

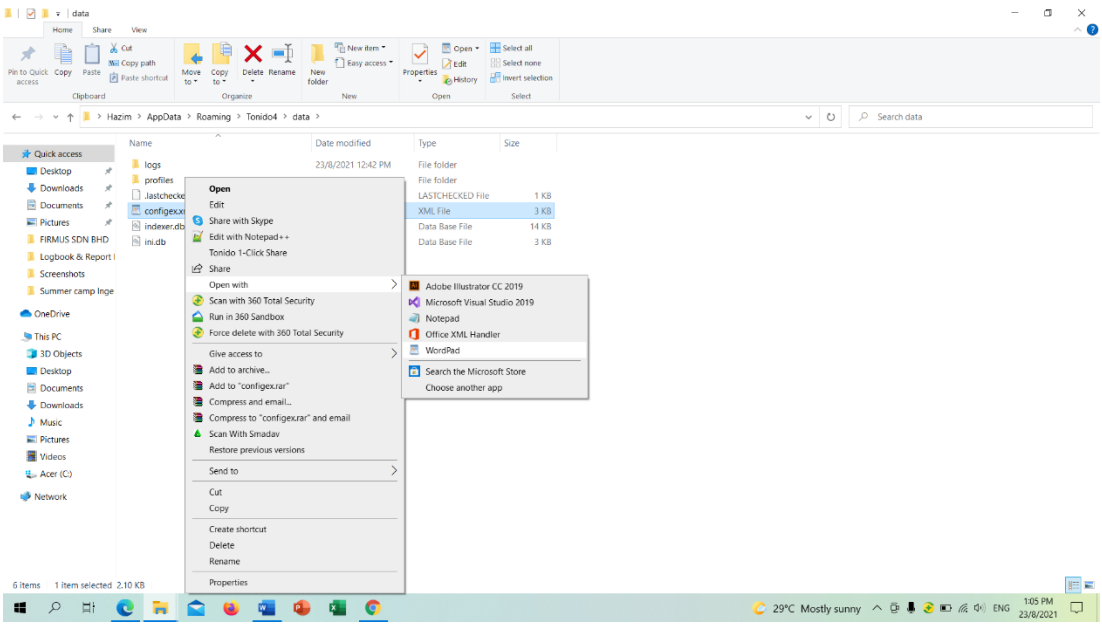


Figure 5.12: Open configex.xml file with WordPad


Figure 5.13: Change the HttpPort value


Figure 5.14: Change the UDPPort value

Next launch the Tonido server and and create a new server. Then choose a specific folder to access and disable indexing. After finish creating the Tonido server go to settings and then network and change the HTTP Port to the one

that has been changed in the WordPad. Figure 5.15, 5.16, 5.17, 5.18, 5.19, 5.20 and 5.21 shows the steps.

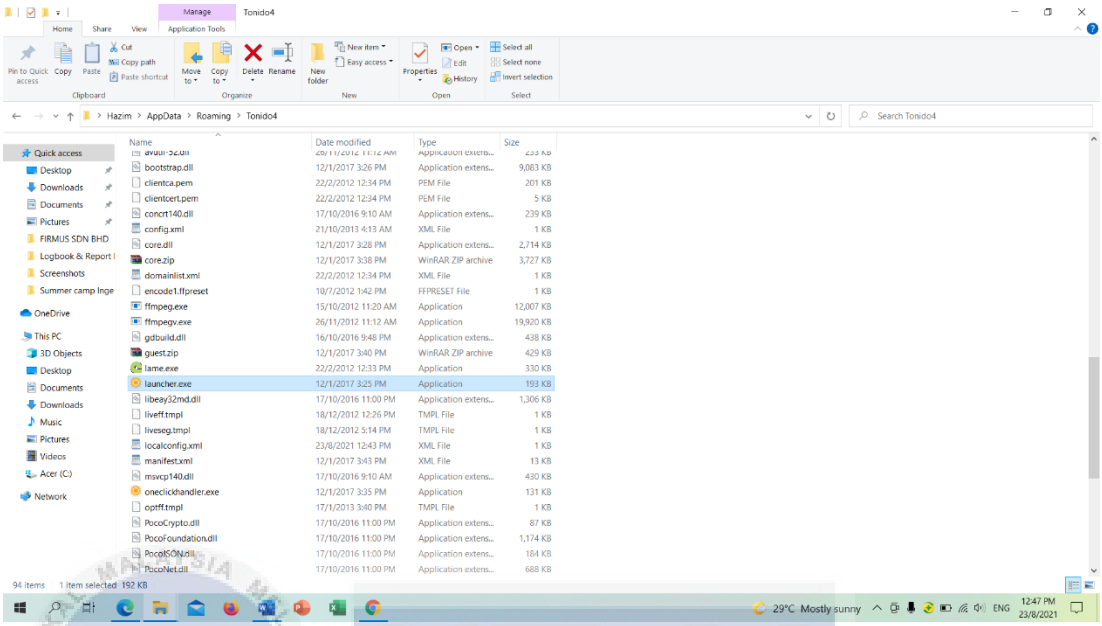


Figure 5.15: launch the server

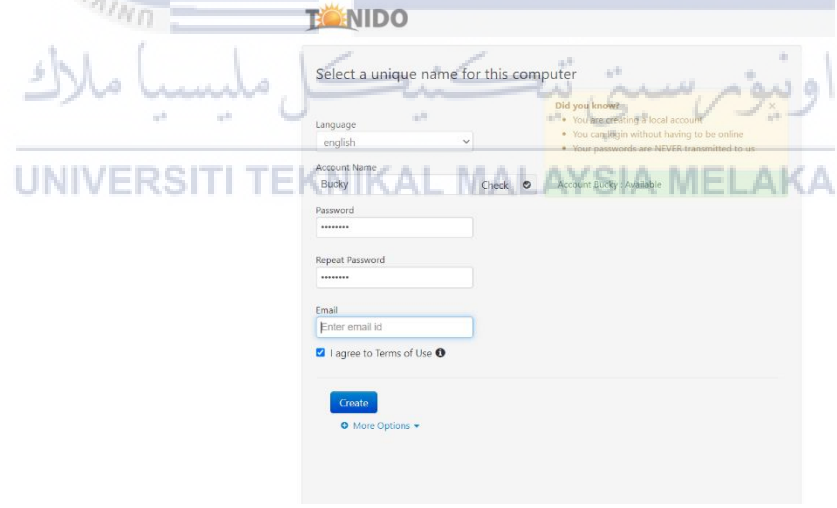


Figure 5.16: Create the new Tonido server

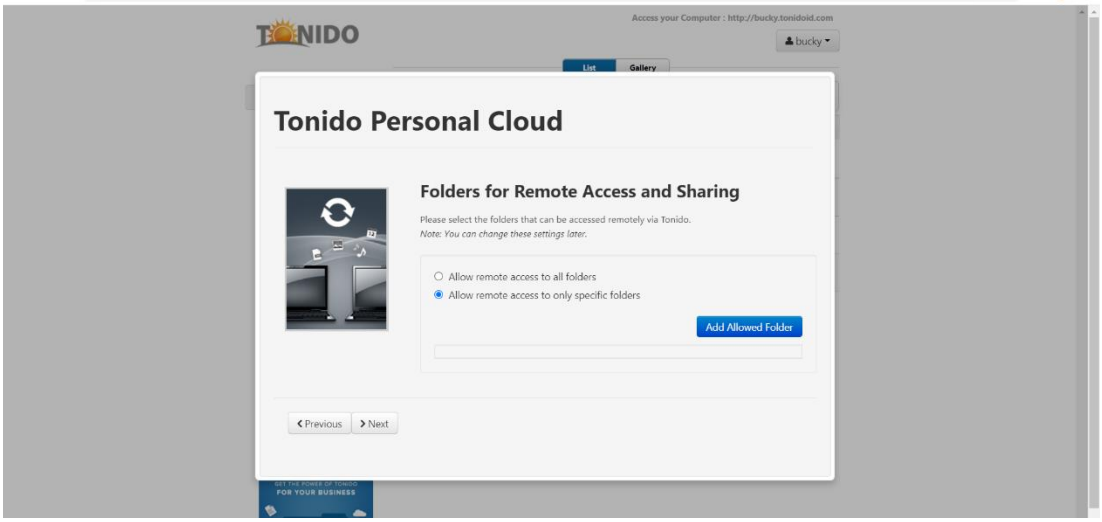


Figure 5.17: Choose a specific folder


Figure 5.18: python folder is chosen

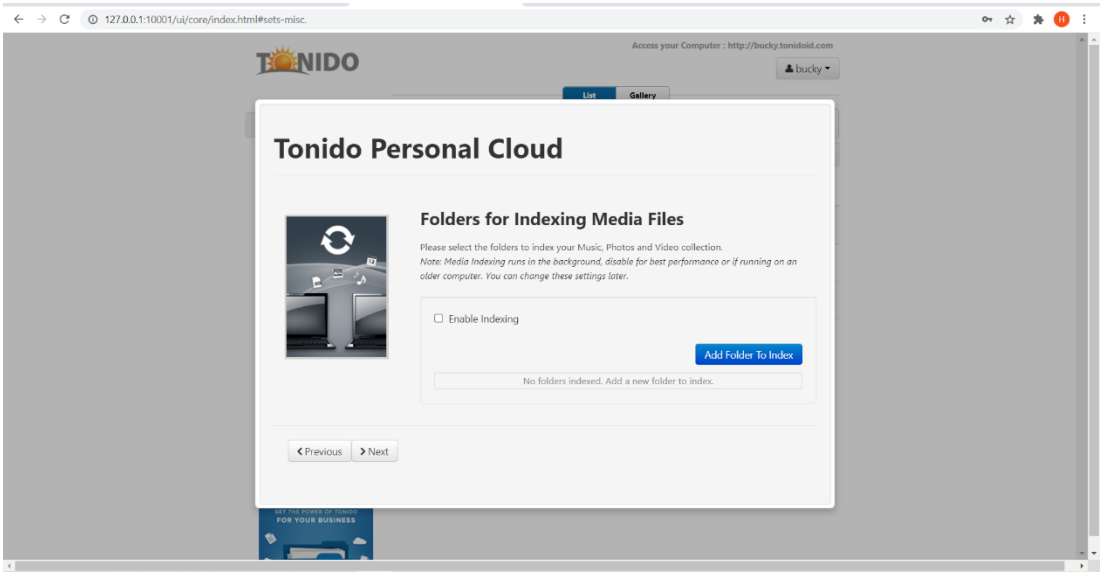


Figure 5.19: Disable indexing




Figure 5.20: Change the HTTP Port value to the one in the WordPad

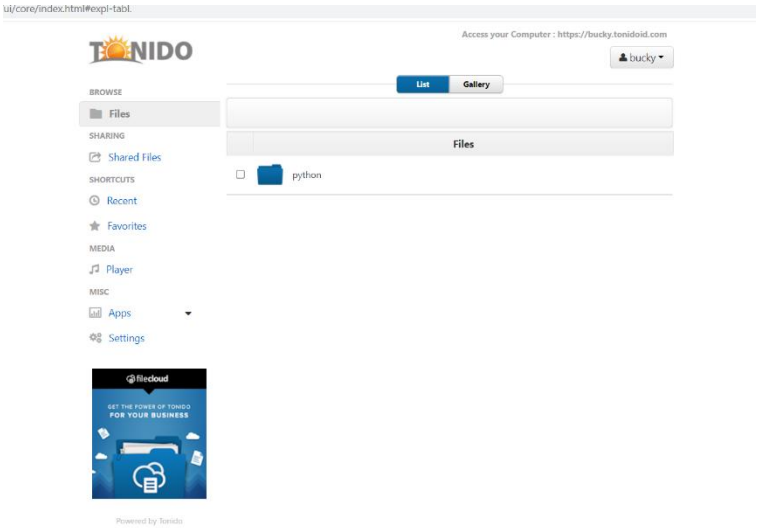


Figure 5.21: The Tonido server with the specific python folder

## 5.5 Accessing Tonido server with a smart device

The Tonido server can also be accessed using a smart device such as tablet, iPad, smart phone and more. To access the private cloud server using a smart device, first download the Tonido app in the play store or apple store. After that, add the server, the account and the password. Finally, the server is accessible with the shared files. Figure 5.22, 5.23 and 5.24 shows the application and the server accessed through a smart phone.



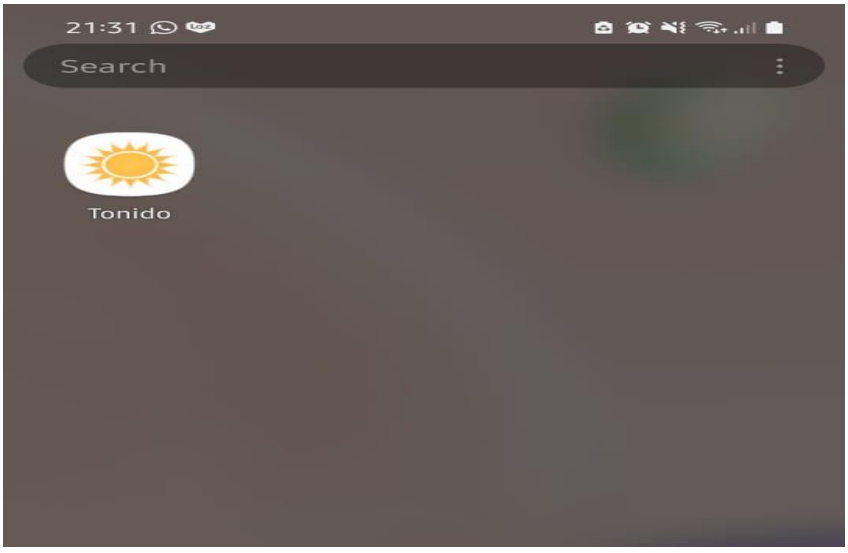


Figure 5.22: Tonido application

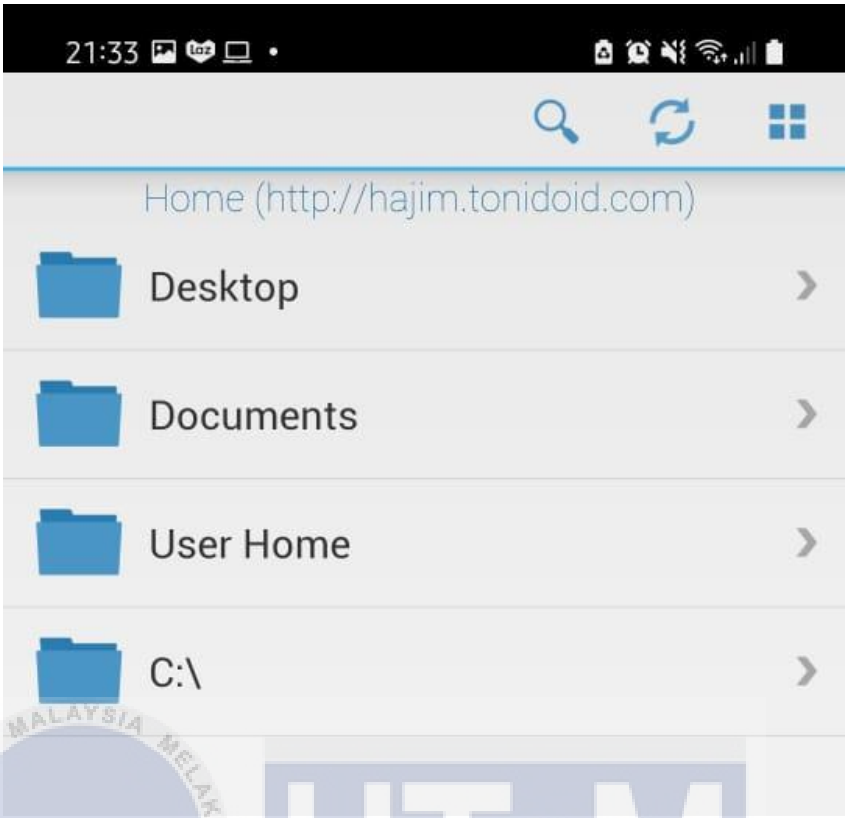


Figure 5.23: Server hajim accessed through a smart phone

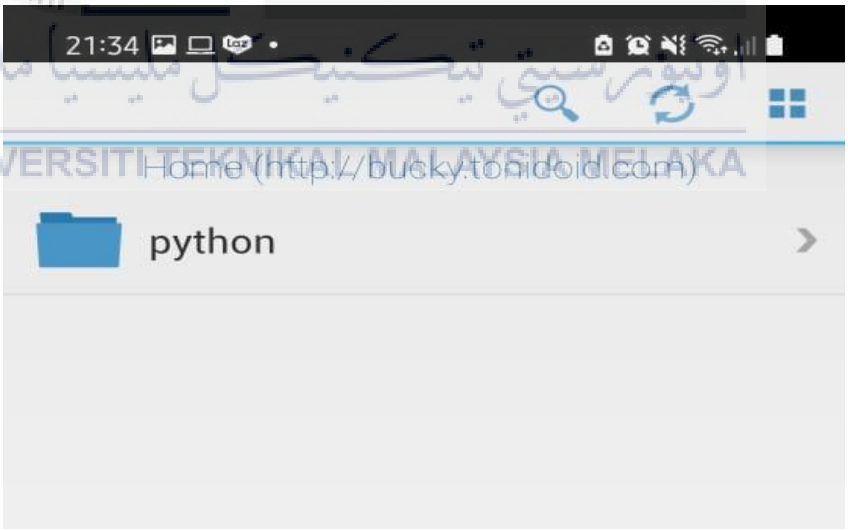


Figure 5.24: Server bucky accessed through a smart phone

## 5.6 Conclusion

This section is the most important to help in understanding the flow of whole analysis and how to create and access the private cloud to reach all objectives for this research. Hence, this section also discusses how to modify the private cloud to enable the usage without the use of an admin server and each specific user can access only each specific folder shared to them.

# CHAPTER 6: TESTING AND ANALYSIS

## 6.1 Introduction

This chapter elaborates on the analysis of security of the private cloud based on the authorization of users and the shared files. The result is based on the private cloud that consist of several servers that have been created and modified in the previous chapter.

## 6.2 Security of user authorization through the website

After creating the private cloud and multiple servers of Tonido, the servers will be secured with a password set by the user and can also be accessed by the guest user. Figure 6.1 and 6.2 shows the login page and the unauthorized access for the server hazim.



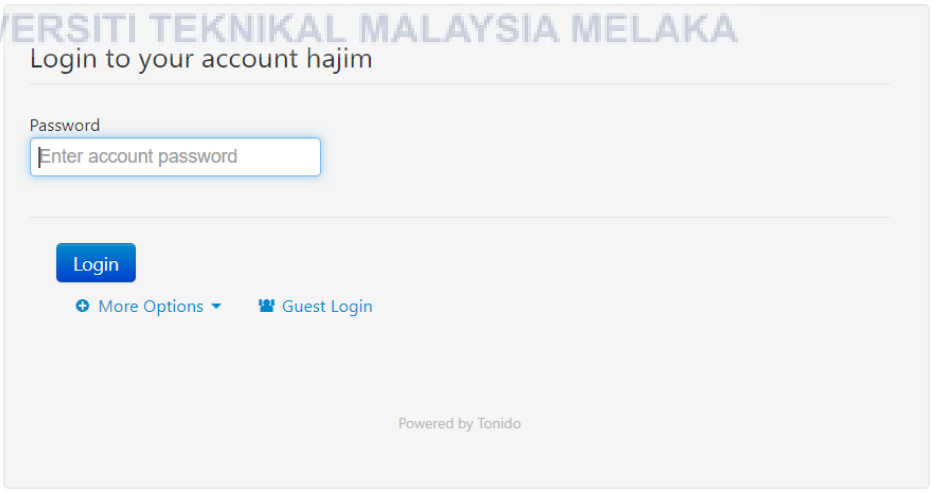


Figure 6.1: Login for hajim server

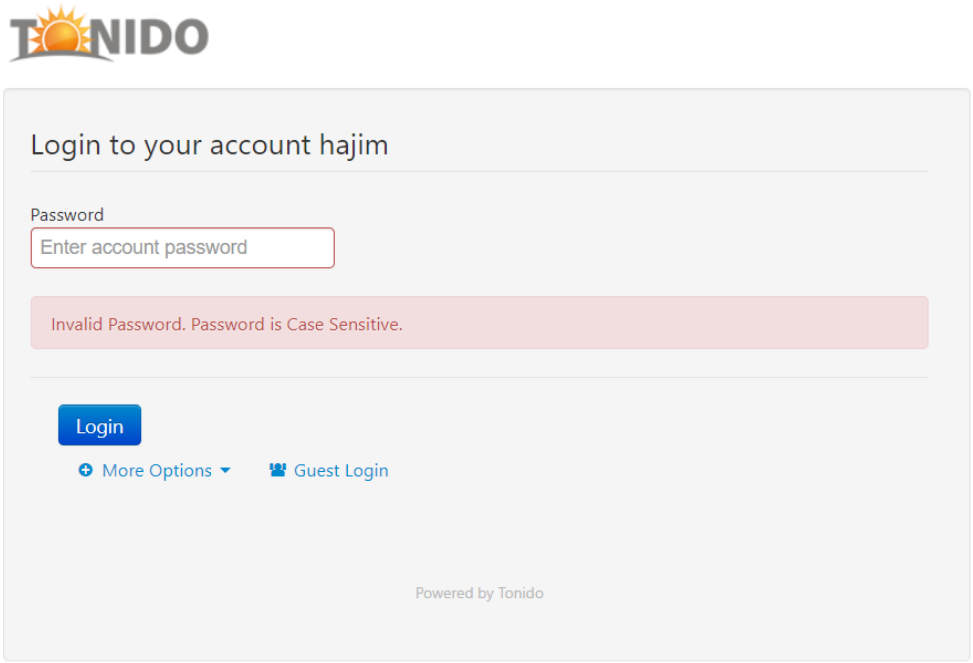


Figure 6.2: Unauthorized access for server hajim

Figure 6.3 and 6.4 shows the sign in page and the unauthorized access for the guest user in server hazim.



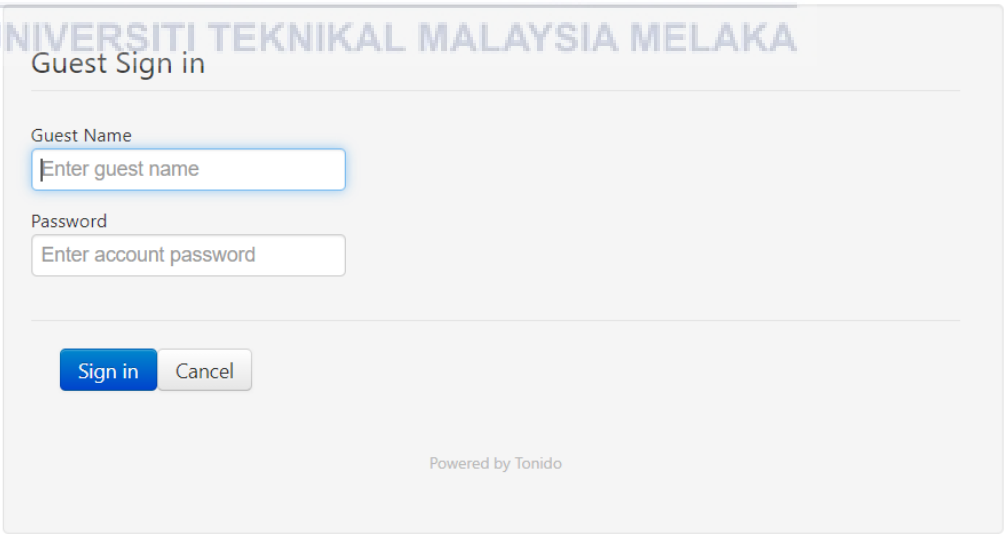


Figure 6.3: Sign in for the guest user of server hajim

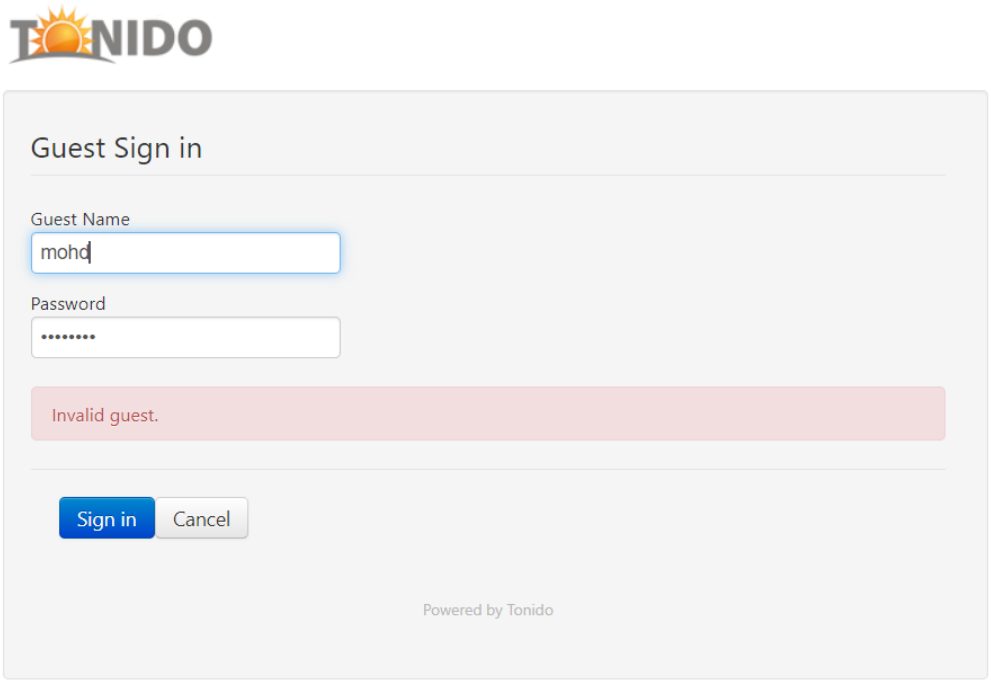


Figure 6.4: Unauthorized access for the guest sign in

Figure 6.5 and 6.6 shows the login page and unauthorized access for the server abutalhah.



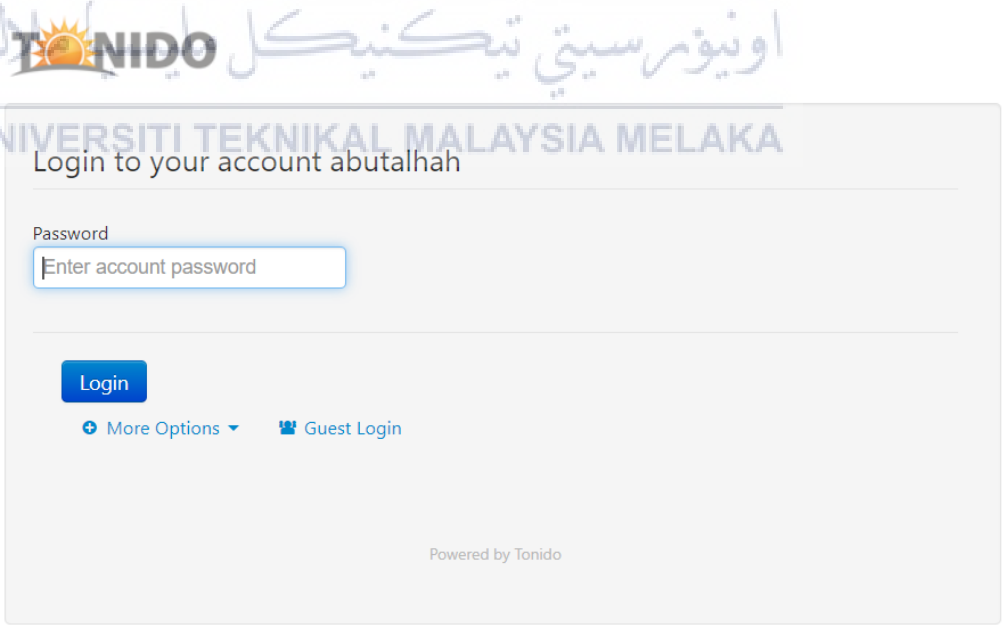


Figure 6.5: Login for abutalhah server

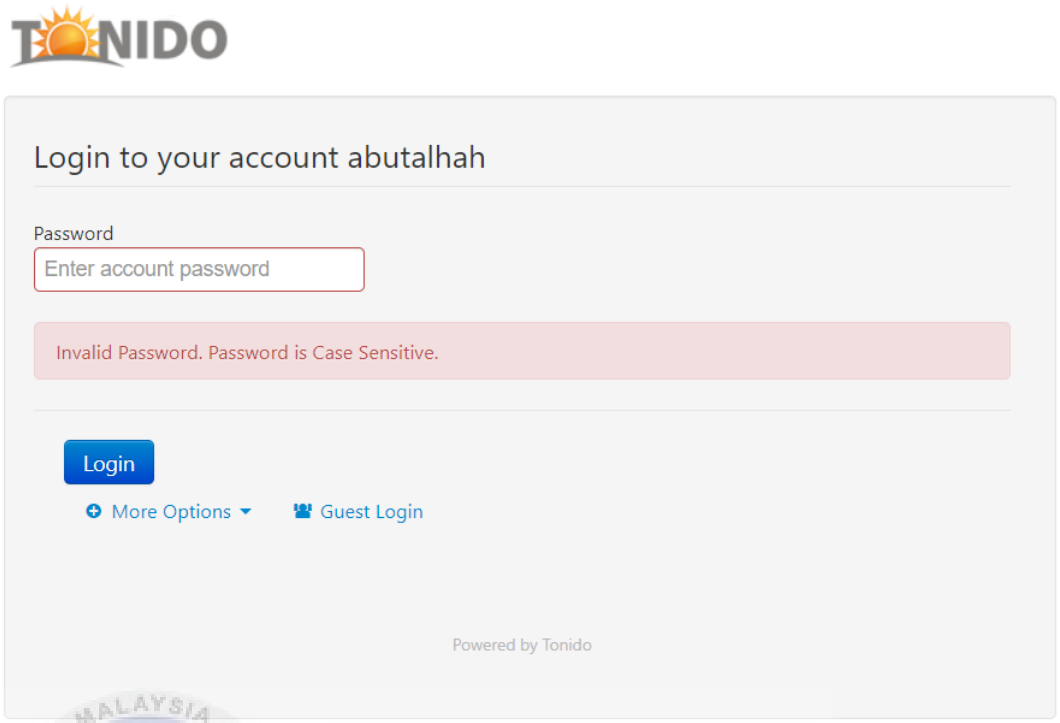


Figure 6.6: Unauthorized access for server abutalhah

Figure 6.7 and 6.8 shows the login page and unauthorized access for the server bucky.



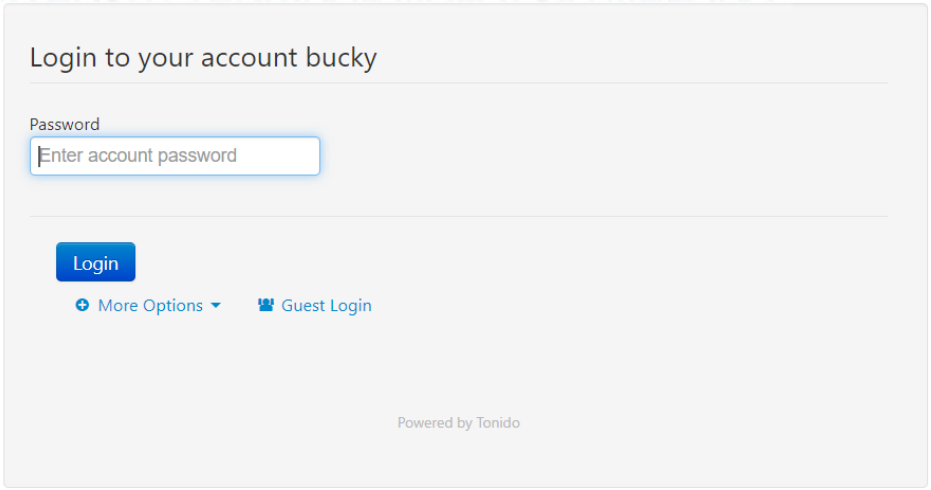


Figure 6.7: Login for bucky server

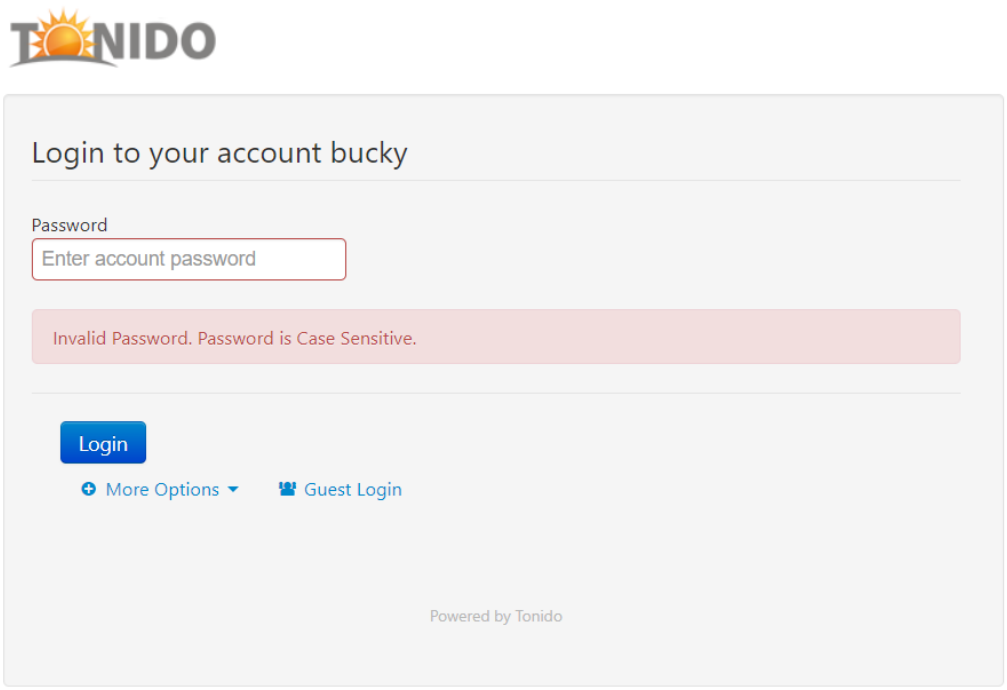


Figure 6.8: Unauthorized access for server bucky

The above log in pages ensures each user can only access their specific server that contains the folder that is shared only to them. The guest sign in page also ensures the security of the data and file shared to the specific guest.



## 6.3 Security of user authorization through a smart device

Accessing the Tonido server using a smart device requires details only the specific users have knowledge to. When adding a new server using a smart device, the user must enter the link of the server, the account name, password and the answer to the question set by the user. Figure 6.9, 6.10 and 6.11 shows the details needed to add a new server into the Tonido application and the results if the user enters the wrong password and wrong answer for hajim server.


Figure 6.9: Add the hajim Tonido server



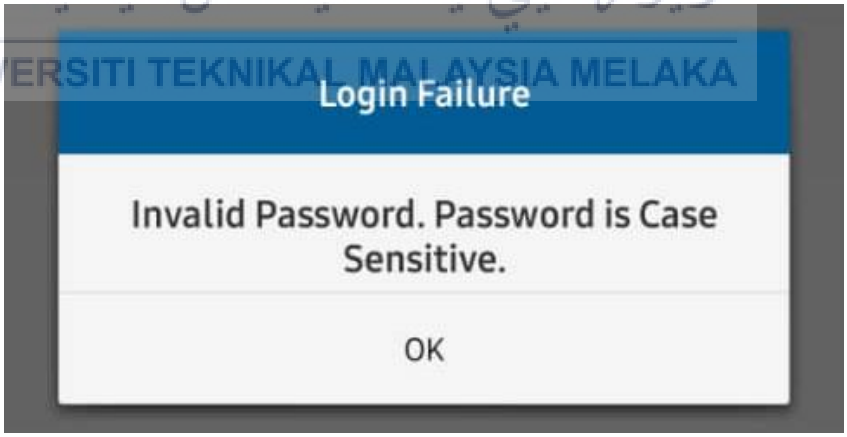


Figure 6.10: Invalid password entered by the user for the server hajim


Figure 6.11: Invalid answer entered by the user for hajim server

Figure 6.12, 6.13 and 6.14 shows the details needed to add a new server into the Tonido application and the results if the user enters the wrong password and wrong answer for abutalhah server.



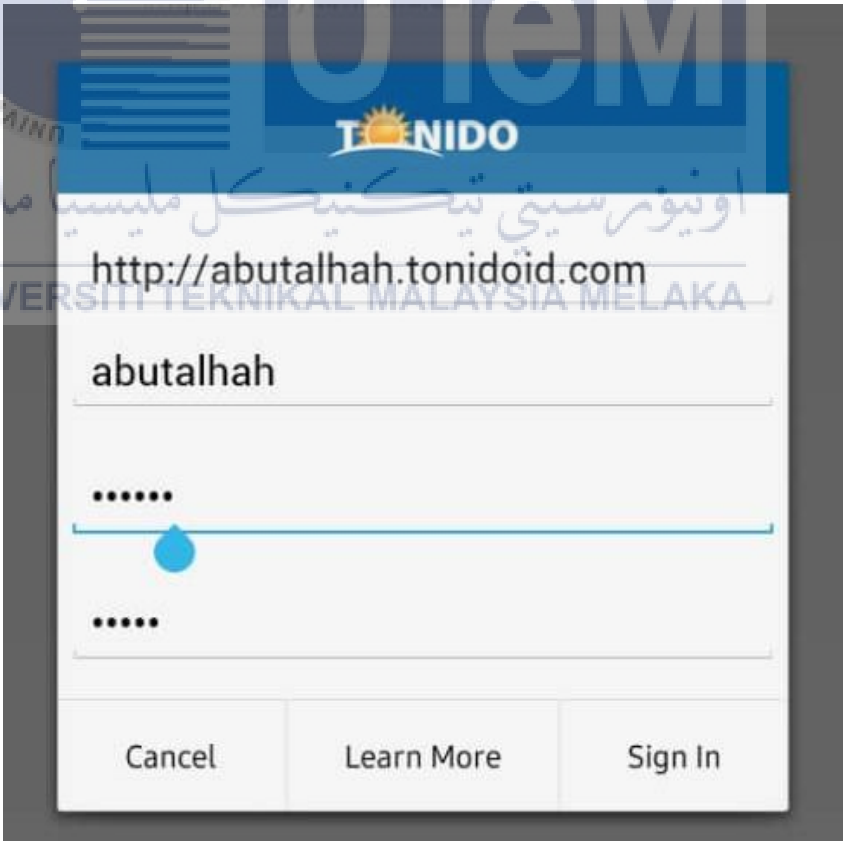


Figure 6.12: Add the abutalhah server


Figure 6.13: Invalid password entered by the user for the server abutalhah

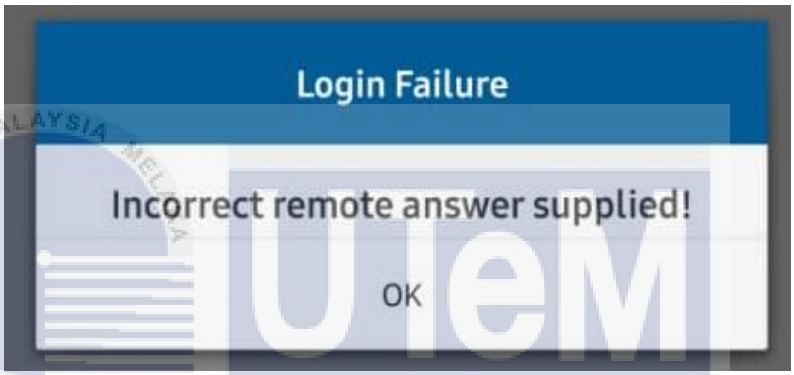


Figure 6.14: Invalid answer entered by the user for hajim server



Figure 6.15, 6.16 and 6.17 shows the details needed to add a new server into the Tonido application and the results if the user enters the wrong password and wrong answer for bucky server.


Figure 6.15: Add the bucky server

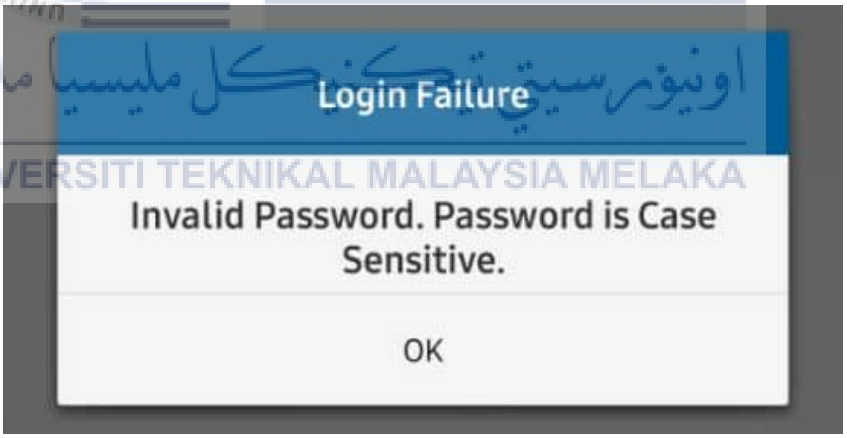


Figure 6.16: Invalid password entered by the user for the server bucky


Figure 6.17: Invalid answer entered by the user for hajim server

Figure 6.18 shows the login for the guest account which is gues1 in the hajim server while figure 6.19 shows the result when the users enter the wrong password.



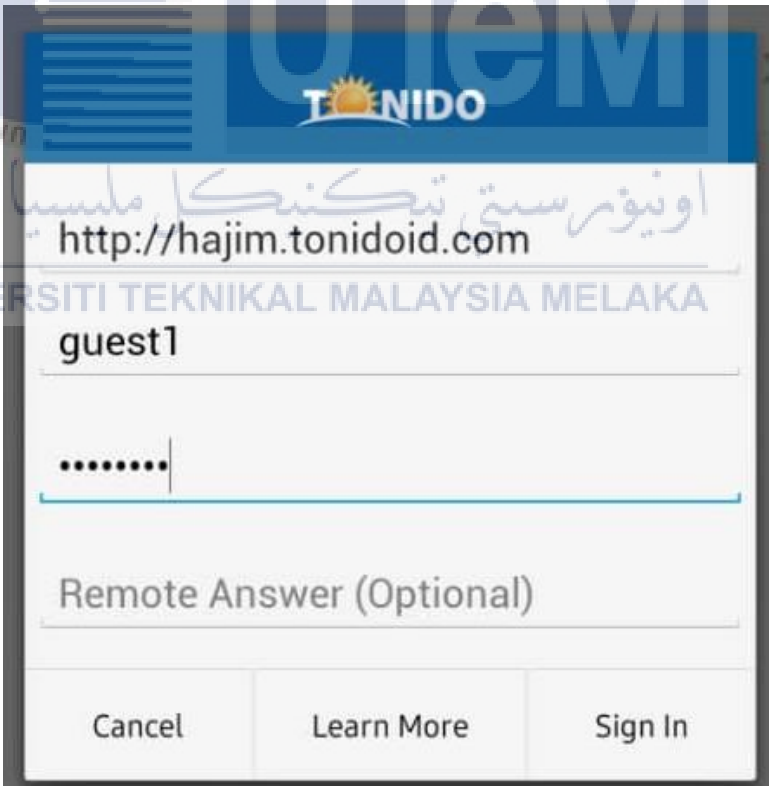


Figure 6.18: Login for the account guest1 in hajim server

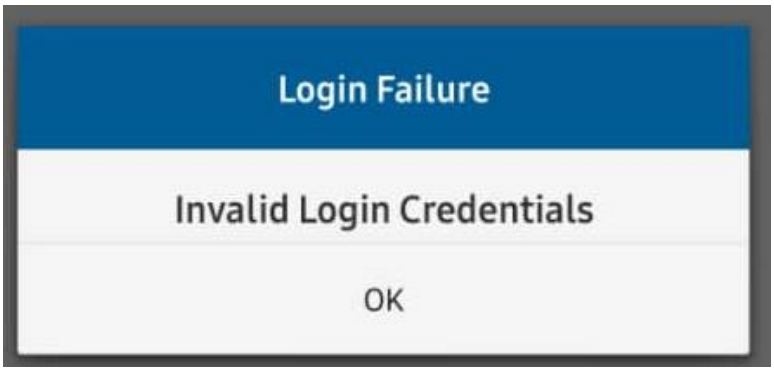


Figure 6.19: Invalid password entered by the user of the guest1 account

## 6.4 Sharing files in the Tonido server

In the Tonido server, the user can share the folders in the server to other users either publicly or privately. The user can choose either to let the receiver of the shared files to either view only or view and upload in to the shared files. If the user uses a public share, the user just needs to create the link and can send the link via email or other social media. Figure 6.20, 6.21, 6.22 and 6.23 shows the steps in how to create a public share link and the file chosen.

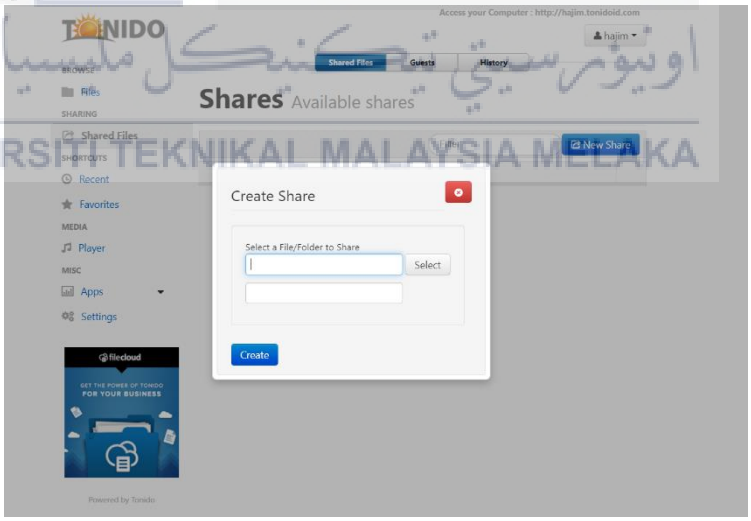


Figure 6.20: Create a share link

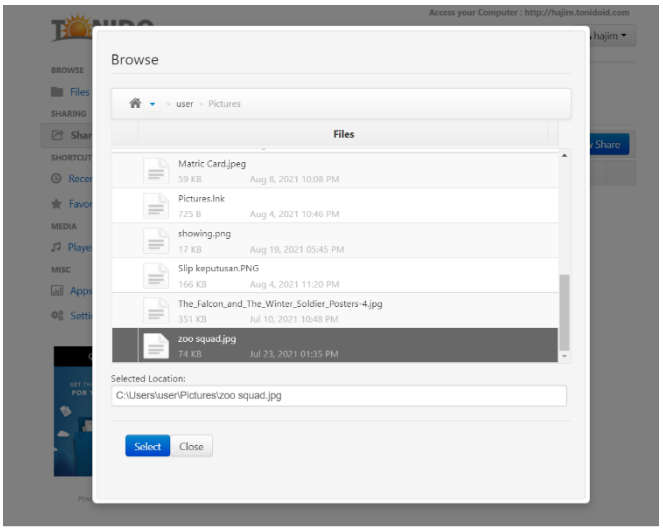


Figure 6.21: Choose a specific file to share

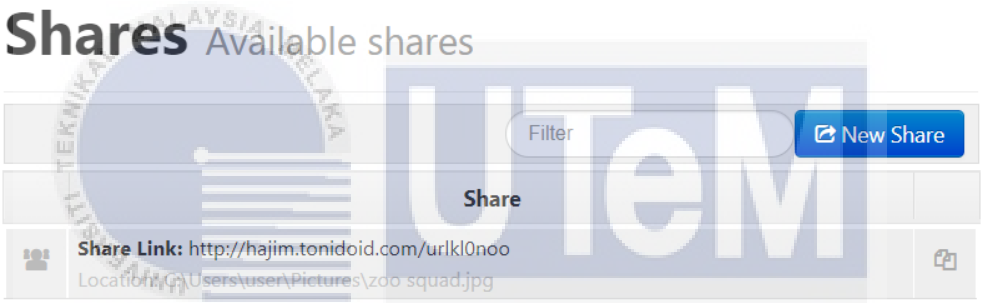


Figure 6.22: The share link created




Figure 6.23: The file shared using the public share link is a picture

The user can also set either to make the link have an expire date or not have one at all. This also increases the security of the public share link so that if the user does not open the link in the time given then no one else might open it. Figure 6.24 shows the setting to choose an expiry date.

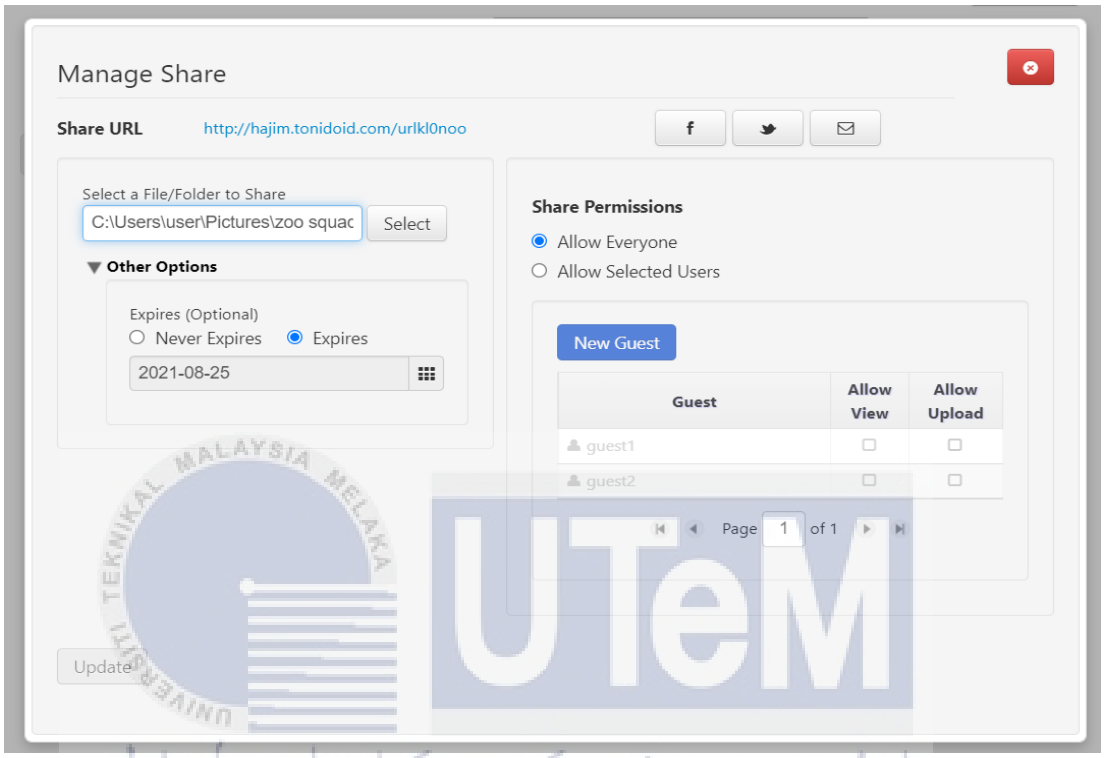


Figure 6.24: choosing an expire date



After creating the public share link, the user can share the link via email or any other social media. Figure 6.25 and 6.26 shows the steps to send the link via email.

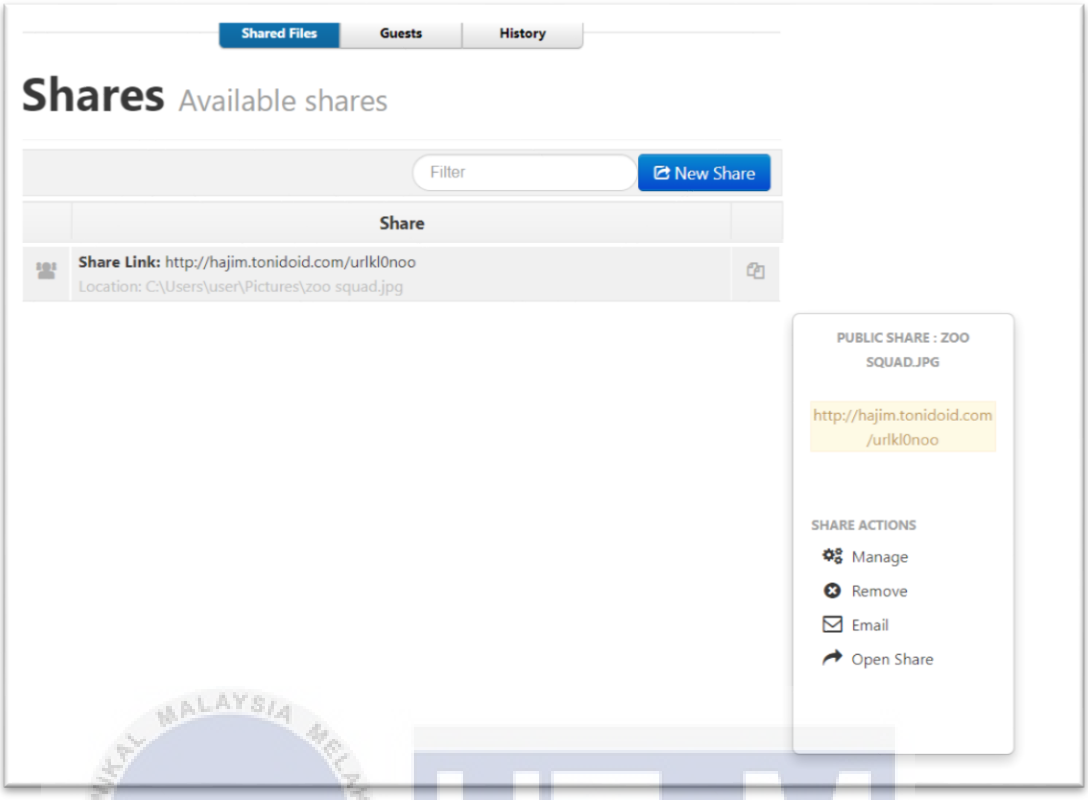


Figure 6.25: Send the link via email

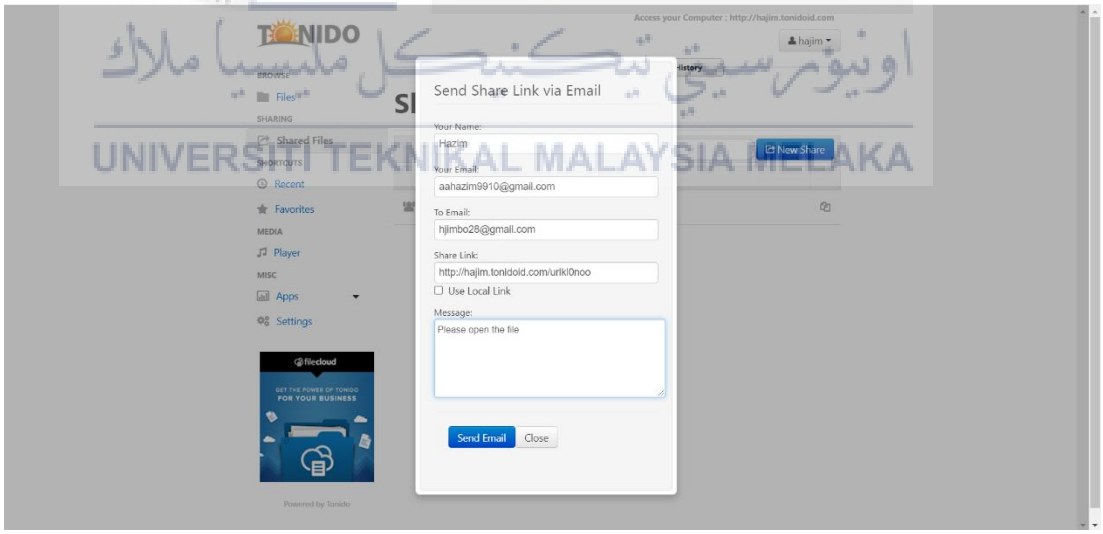


Figure 6.26: Enter the recipient's email

The recipient will receive an email of the link that is shared. The recipient must click the link to access the file that is shared. Figure 6.27 and 6.28 shows the email and file received by the recipient is the same as shared by the user.




Figure 6.27: The email received by the recipient


Figure 6.28: The file received by the recipient

Besides public share, the user can share the file privately to someone. To share a file privately, the user must first create a guest account and password for the recipient. Figure 6.29 and 6.30 shows the steps to create a guest account.

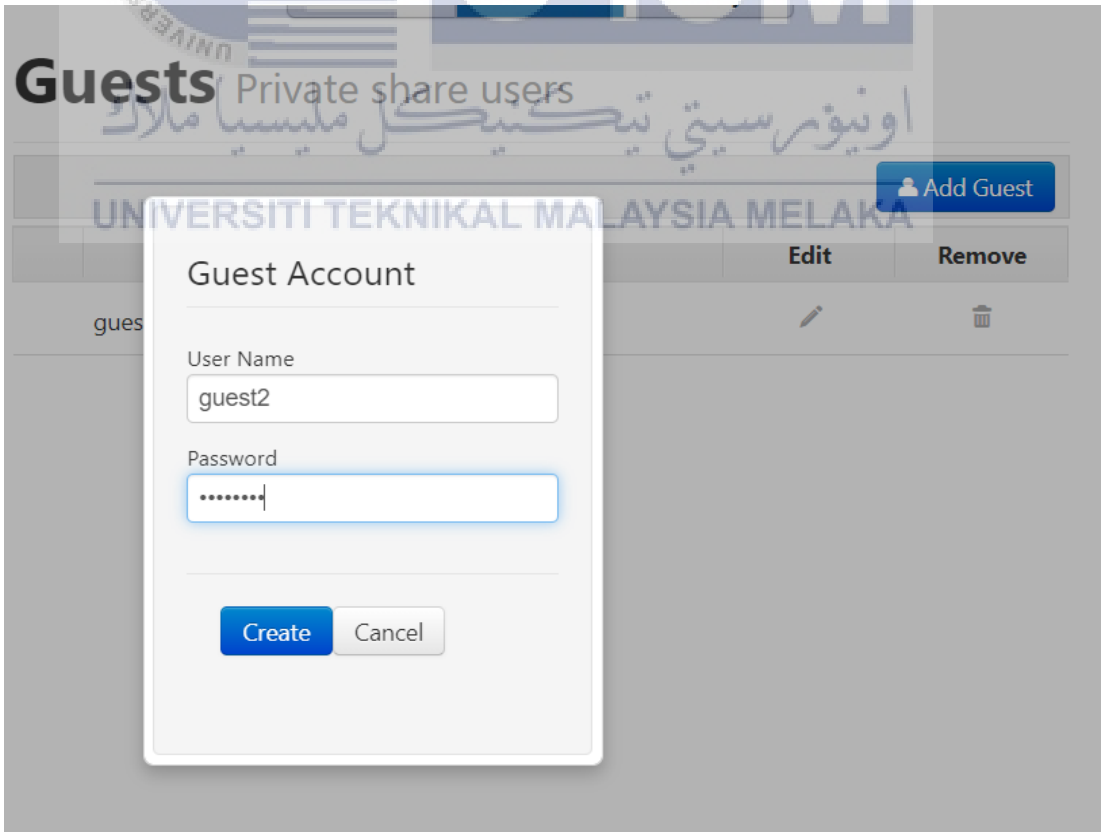


Figure 6.29: Creating a guest account called guest2

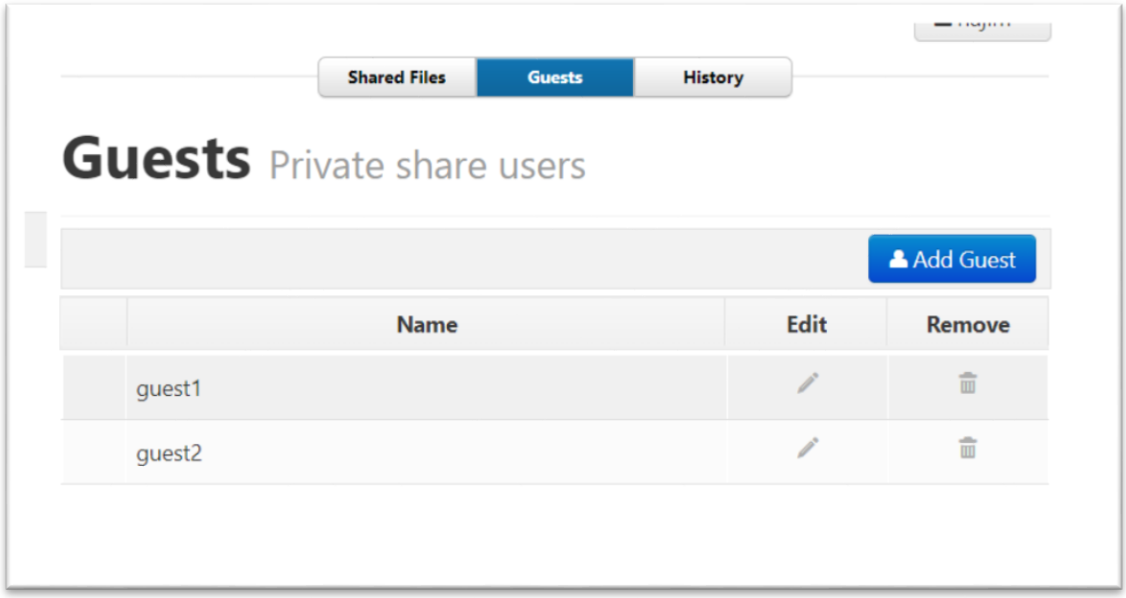


Figure 6.30: Guest account created

After creating the guest account, create the private share link by choosing the file to share. After choosing the file, the user can set which guest can view and upload and which guest can only view or only upload to the shared file. The user can also set to limit the upload size. Figure 6.31, 6.32, 6.33 and 6.34 shows the steps to create a private share link and how to send the link to the recipient.

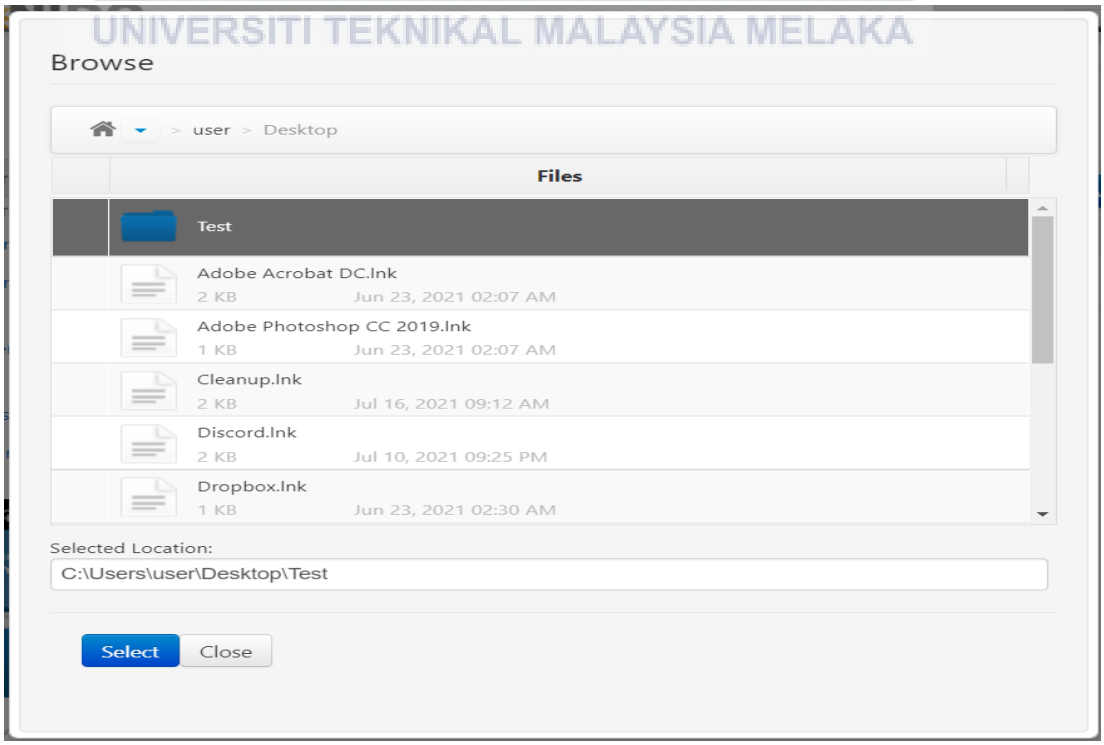

Figure 6.31: Choose a file to share privately

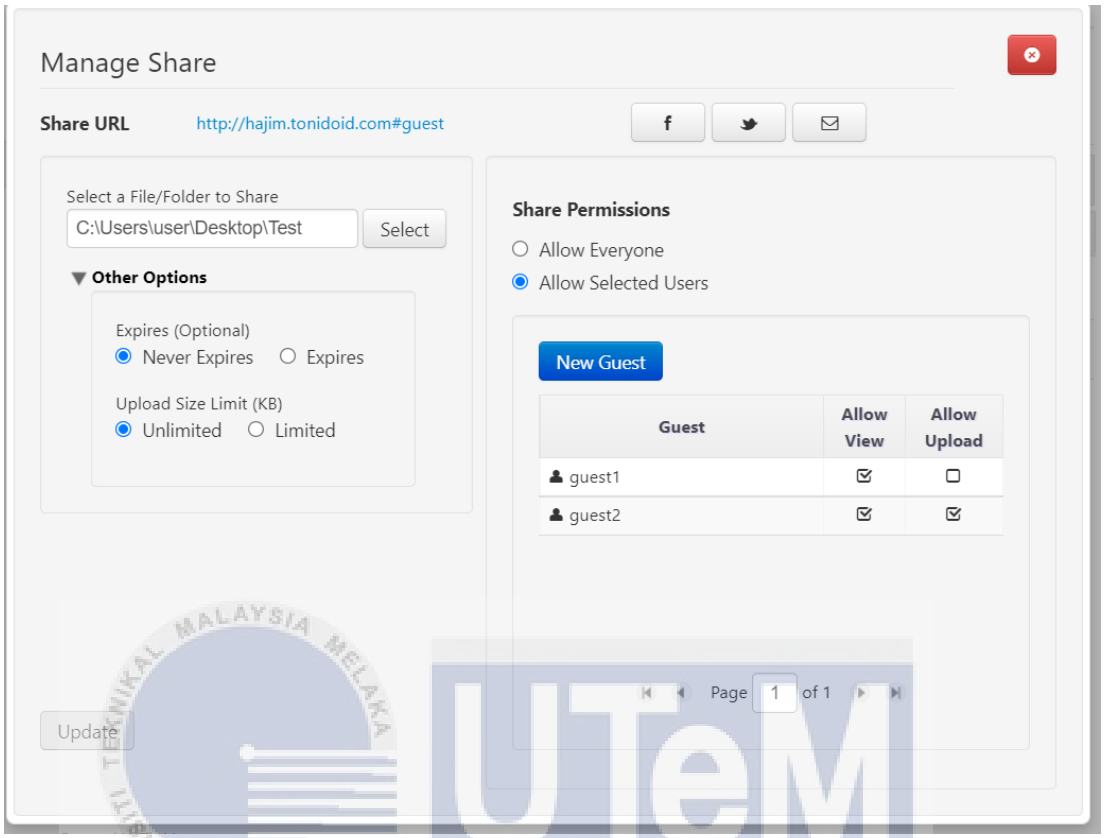


Figure 6.32: Set which guest can view and upload to the shared file



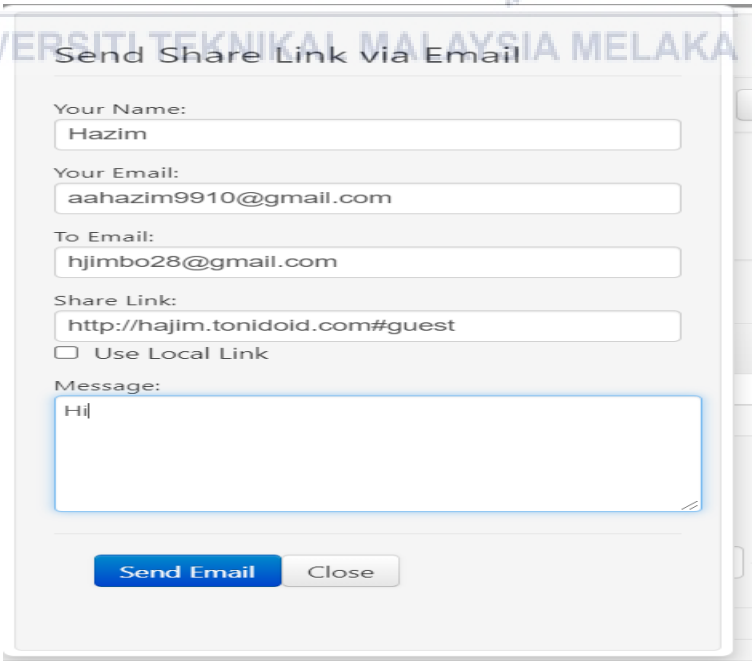


Figure 6.33: Send the private share link via email

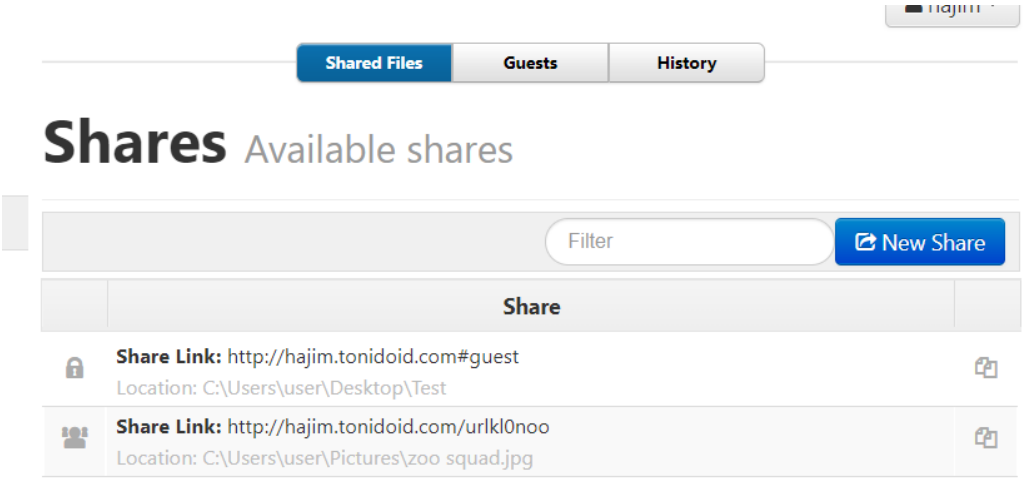


Figure 6.34: Private share link created

The recipient will receive the email containing the private share link. Clicking the email will send the recipient to the login page for guest users. The recipient must login to the account to be able to access the shared file if the recipient has the privilege. Figure 6.35 and 6.36 shows the email received and the login page for the guest account.

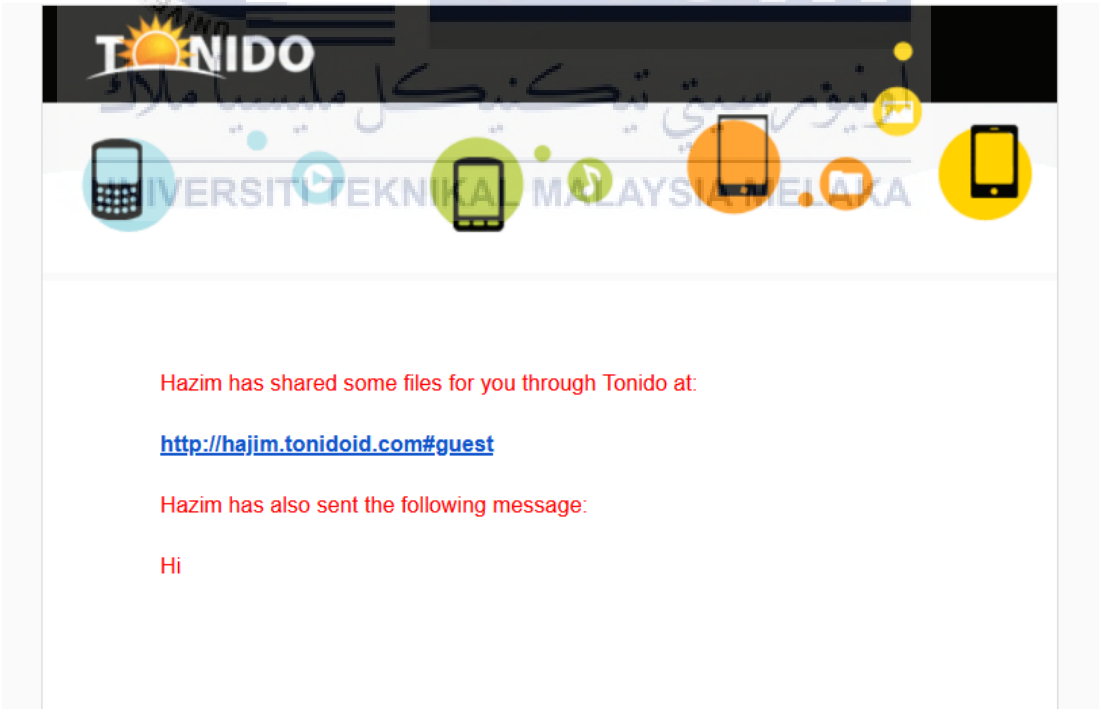


Figure 6.35: Email received by the recipient

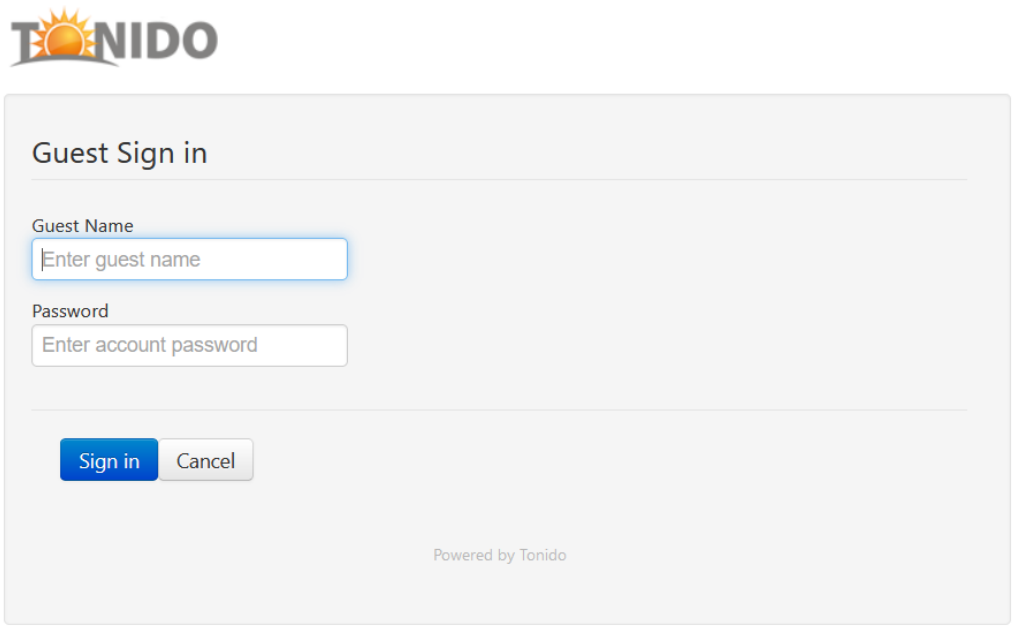


Figure 6.36: Guest login page

Upon logging in, the recipient is able to see the shared file. The recipient is also able to download, rename and upload into the file because of the privilege set by the user of the server as the recipient is guest2. Figure 6.37 and 6.38 shows the file shared by the user and the privilege of the recipient.



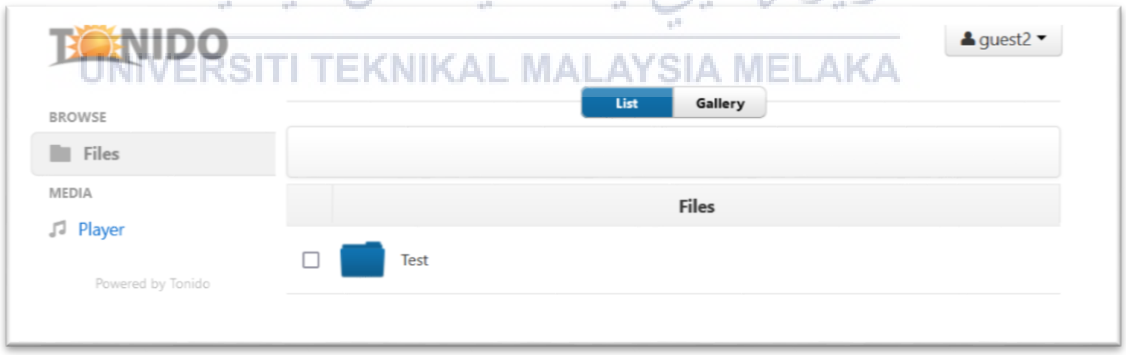


Figure 6.37: The file shared by the user

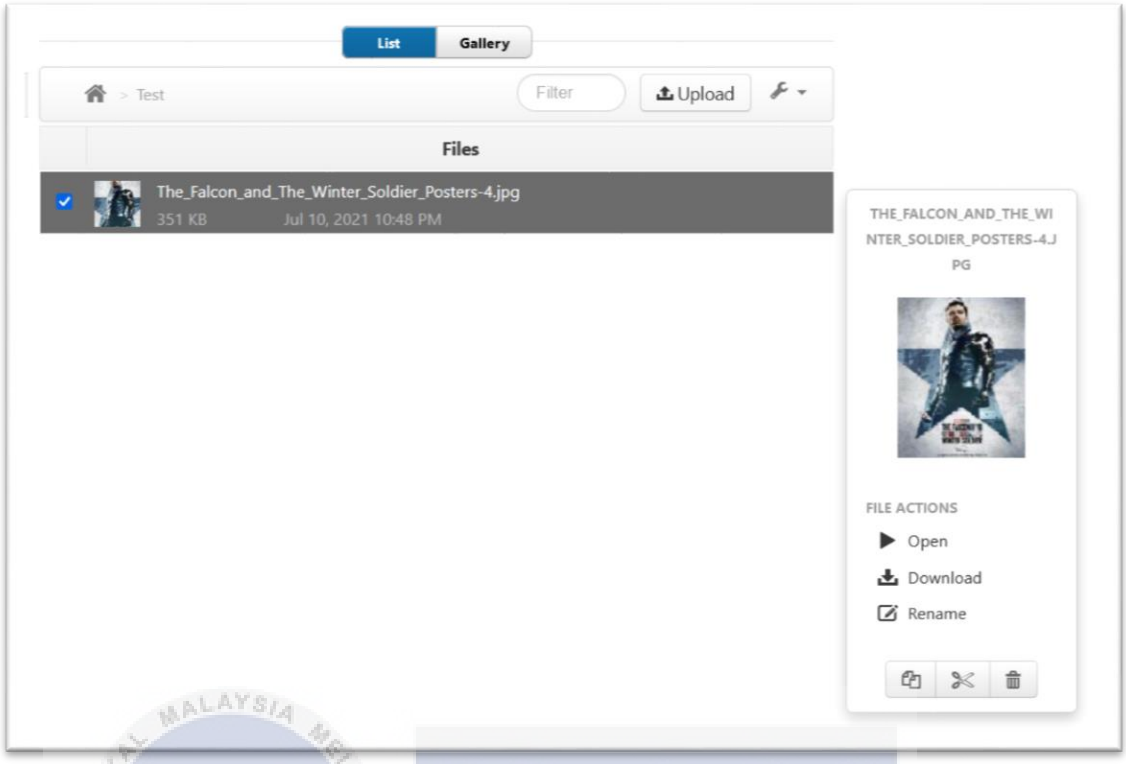


Figure 6.38: Guest2 is able to upload, download, view and rename the file

However, if the recipient logs in as guest1, he or she will not be able to upload to the file or rename the file. The recipient can only view and download the file. Figure 6.39 shows the privilege of the guest1 account.

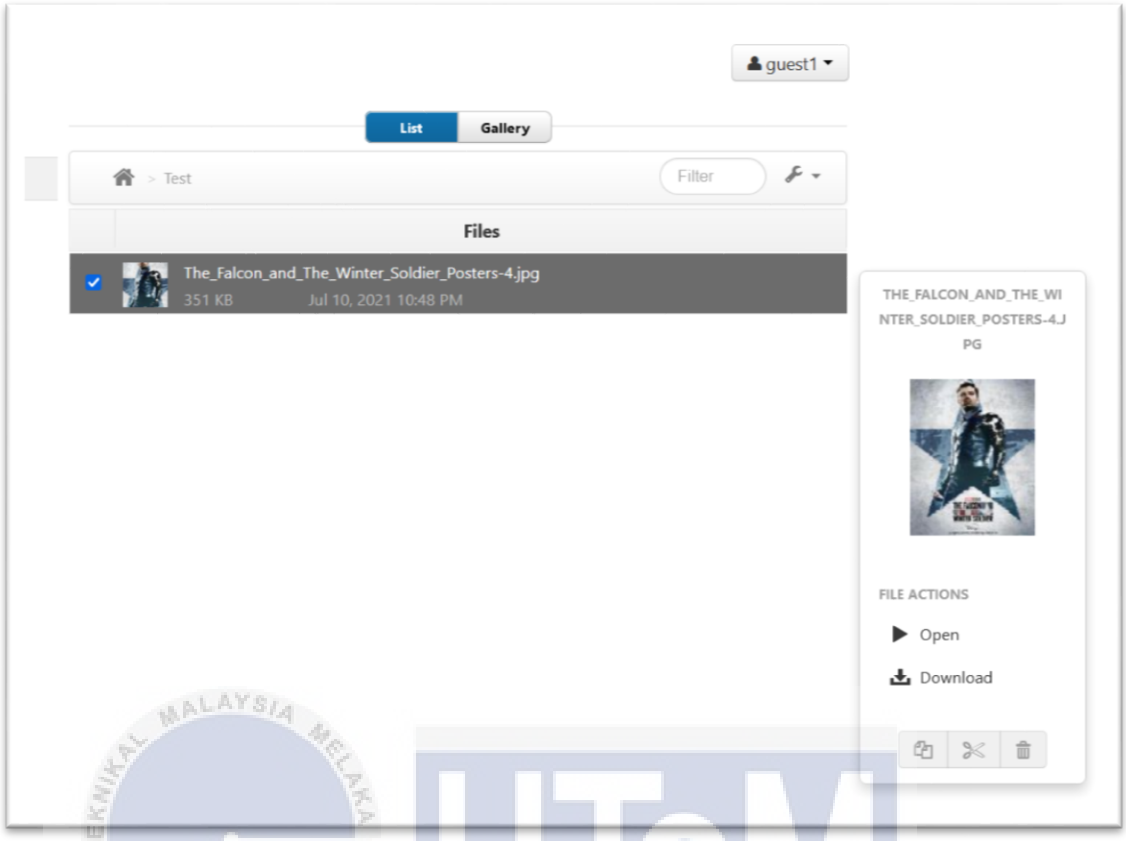


Figure 6.39: Guest1 is only able to download and view the file

## 6.5 Sharing files in the Tonido server using smart device

Using the Tonido application installed in the smart device, the user can share and access files in the server. This increases the accessibility, efficiency and also the security of the Tonido private cloud. The users just need to login to their respective accounts to access the files. Figure 6.40 and 6.41 shows how to login to the guest account.

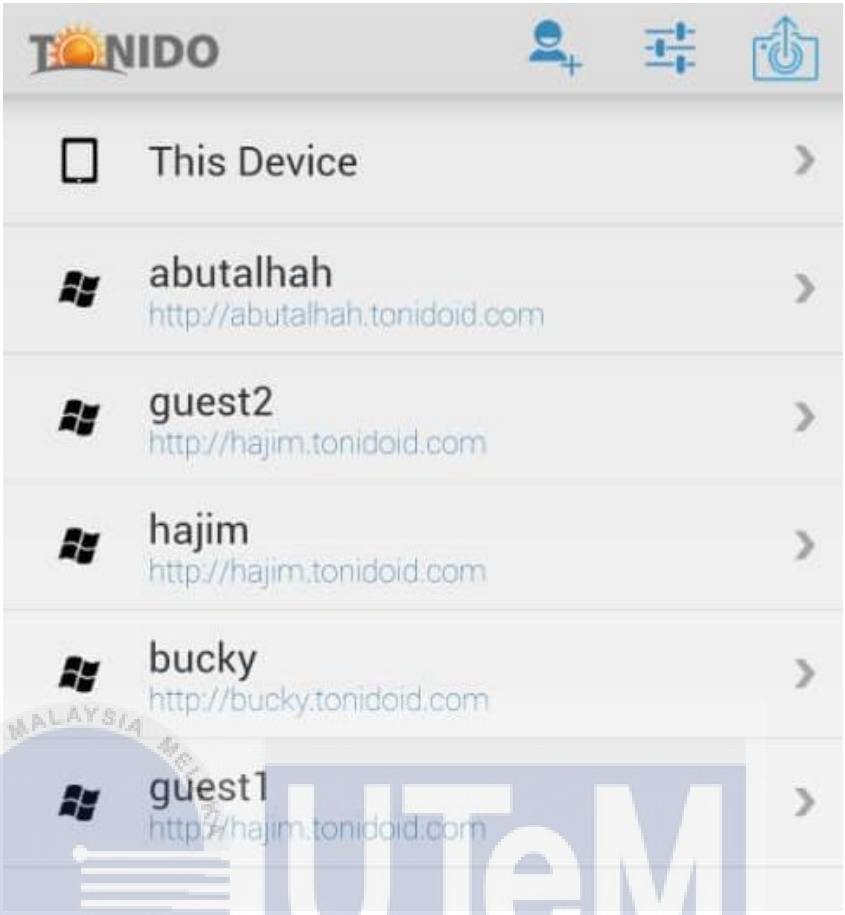


Figure 6.40: Login to the users or guest account

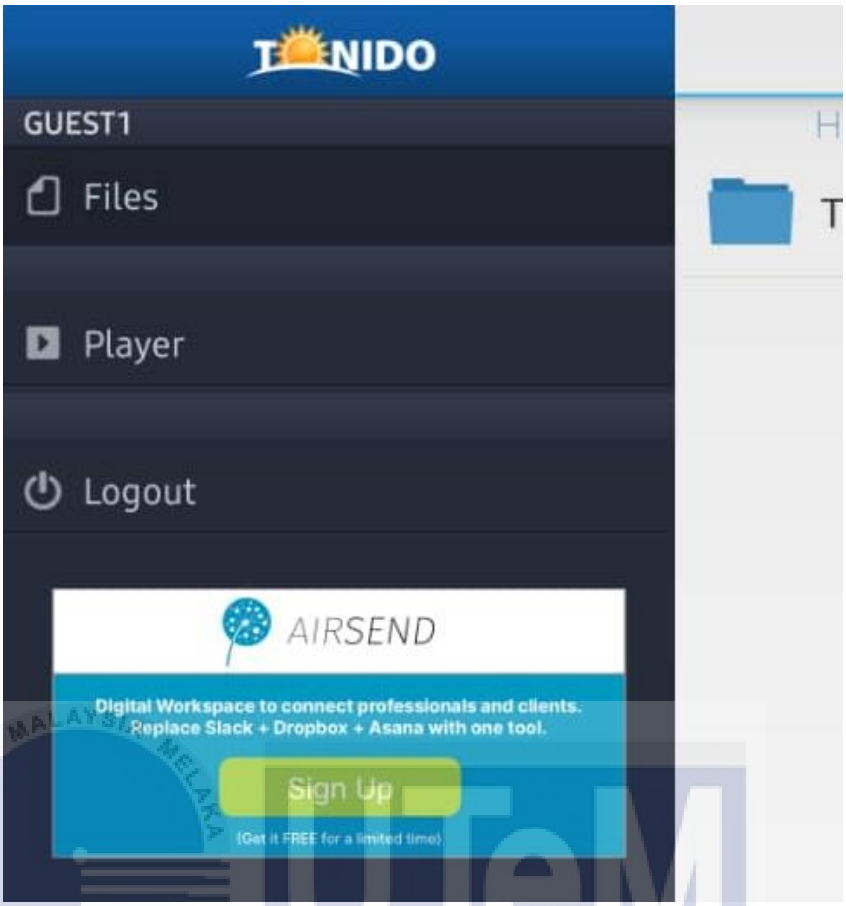


Figure 6.41: The account for guest1

The guest1 account can only view and download the shared filed but cannot upload to the shared folder. Figure 6.42 and 6.43 shows the Test folder shared and the picture file inside the folder.


Figure 6.42: The shared folder


Figure 6.43: The picture file

Figure 6.44 and 6.45 shows the guest2 account and the Test folder shared with guest2.




Figure 6.44: Guest2 account


Figure 6.45: Shared Test folder

The guest2 account can view, download and upload to the folder as set by the user of hajim server. Figure 6.46 shows the picture file inside the shared Test folder.


Figure 6.46: Picture file in the shared Test folder

## 6.6 Comparison between the three cloud models

The result of the test for the proposed private cloud model is recorded, analyzed and compared with the other models of cloud computing. Table 6.1 shows the comparison between the cloud computing models.

Table 6.1: Comparison between the three models of cloud computing

| Difference | Public | Private | Hybrid |
|---|---|---|---|
| **Data Tenancy** | The data of numerous companies is stored in a shared environment | The data of only a single organization is stored in the cloud | The data stored in the public cloud is shared, and the data stored in the private cloud is not shared and kept confidential |
| **Security** | - Least secure<br>- Multitenancy | Most secure | Control of security between Private and Public clouds |

| | | | |
|---|---|---|---|
| | - Transfers over the net | | |
| **Cloud Services** | Open to public | Only that specific organization can use the cloud services | Services on the public cloud can be accessed by everyone, whereas services in the private cloud can be accessed only by that organization |
| **Cost** | Less expensive as the cloud service provider offers all the resources | Very expensive as the organization has to purchase all the resources | Less costly for public cloud and more expensive for private cloud resources |
| **Software and Hardware Components** | The cloud service provider manages these components | That particular organization operates these components | Public cloud components – Cloud Service provider<br><br>Private cloud components – Organization |
| **Management of cloud services** | Managed by the cloud service provider | Managed by the administrators of that specific organization | service provider, whereas the administrators of that particular organization manage the private cloud |

## 6.7 Conclusion

In this section, it offers the results of the security for the storing and sharing data using a private cloud. It shows that by creating multiple instances of Tonido server the unauthorized access, data breaches and external data sharing problems stated in the problem statement could be mitigated by using this method. The chapter above concludes the research as a whole by achieving the objectives of this project.

# CHAPTER 7: PROJECT CONCLUSION

## 7.1 Introduction

This segment discusses the overall results of the project and concludes them. This section is the final stage of the project's development. Conclusion of the project controls whether the goals, scopes and project design fulfil the demands. Project summary, project contribution and project restriction can summarize the project. Project restriction is essential to discuss and improve the project for future work.

## 7.2 Project Summarization

This project focusses on the benefits and security of private cloud security. In this project, a private cloud is created using Tonido which is a free cloud server software. The private cloud was created in Acer Aspire e15 laptop. After that, the private cloud is enhanced by creating multiple Tonido servers in the same device to allow multiple users without an admin server. This ensures the security, confidentiality and integrity of the data stored in the private cloud. The private clouds created were tested by sharing specific files and then record the security of the private cloud. This also ensures the security of the files or folders shared in the private cloud so that only specific people allowed by the server user to access. The private cloud can also share publicly and privately using a share link configured by the private cloud server user. The multiple Tonido servers created also prevents unauthorized access into the private cloud.



## 7.3 Project contribution

The main contribution of this project is:

- Prevent unauthorized access in cloud computing system

- Prevent data breaches caused by misconfigured cloud security settings
- Create a private cloud that can store sensitive data securely
- Compare which cloud computing model is the most secured

## 7.4 Project limitation

The limitation of the project is as follows:

- The storage space for the private cloud is only 2GB for each private cloud server
- The cost is extremely high because the organization must purchase all of the resources

## 7.5 Future work

By focusing on the limitation of the project, the future works that can be done in is as follows:

- Increasing the storage space of the private cloud to more than 2GB
- Enhance the security to access the private cloud security with biometric authentication
- Create a notification when guest or other users view a shared folder

## 7.6 Conclusion

In conclusion, the research project has successfully achieved the objective. This project has created a private cloud model that can prevent the problem statement stated in this report. This research project increased the security, confidentiality and integrity of the private cloud created. This project is also able to provide benefits in providing information and data for other researchers in the future

## REFERENCES

Ashish Singh, A., & Chatterjee, K. (n.d.). Cloud security issues and challenges: A survey.

Azeez, N. A., & Vyver, C. V. d. (2018). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis.

Derbeko, P., Dolev, S., Gudes, E., & Shantanu Sharma, S. (2016). Security and privacy aspects in MapReduce on clouds: A survey.

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms.

Kumar, R., & Rinkaj Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey.

Mthunzi, S. N., Benkhelifa, E., Tomasz Bosakowski, T., Guegan, C. G., & Mahmoud Barhamgi, M. (2019). Cloud computing security taxonomy: From an atomistic to a holistic view.

R, P., Santhosh, G. T., Ratchnayaraj, I. A. J., & E. Jemiline. (2020). The security in web application of cloud and IoT service.

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges.

Sharma, D. K., Chakravarthi, D. S., Shaikh, A. A., Ahmed, A. A. A., Jaiswal, S., & Naved, M. (2021). The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique.

AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., & Jaradat, A. (2021). Mobile cloud computing models security issues: A systematic review.

Swetha, M., & M. Latha. (2021). Security on mobile cloud computing using cipher text policy and attribute-based encryption scheme.

Dubey, K., & S.C. Sharma. (2020). An extended intelligent water drop approach for efficient VM allocation in secure cloud computing framework.

Cotroneo, D., De Simone, L., Liguori, P., & Natella, R. (2021). Enhancing the analysis of software failures in cloud computing systems with deep learning.

Mekawie, N., & Yehia, K. (2020). Challenges of Deploying Cloud Computing in eHealth.