**Secure VPN & Cloud Storage**

**Research Manual**



**Maciej Chudy / C00247467**

**Supervisor: Joseph Kehoe**

Table of Contents

[Introduction 3](#_Toc132668122)

[VPN 4](#_Toc132668123)

[What is a VPN? 4](#_Toc132668124)

[Why is it important? 4](#_Toc132668125)

[VPN Requirements 5](#_Toc132668126)

[VPN Options 6](#_Toc132668127)

[VPN Conclusion 6](#_Toc132668128)

[Cloud Document Management System 7](#_Toc132668129)

[What are Cloud Document Management Systems? 7](#_Toc132668130)

[CDMS Options 7](#_Toc132668131)

[Operating System 8](#_Toc132668132)

[What is an Operating System? 8](#_Toc132668133)

[Operating System Options 8](#_Toc132668134)

[Server Security 9](#_Toc132668135)

[Logical Security 9](#_Toc132668136)

[SSH 9](#_Toc132668137)

[FTP 9](#_Toc132668138)

[Version 9](#_Toc132668139)

[Disabling services and ports 10](#_Toc132668140)

[HTTPS over HTTP 10](#_Toc132668141)

[Encryption 10](#_Toc132668142)

[Physical Security 10](#_Toc132668143)

[Platform 11](#_Toc132668144)

[Platform Options 11](#_Toc132668145)

[Dedicated Server 11](#_Toc132668146)

[Raspberry Pi 12](#_Toc132668147)

[Virtual Server 12](#_Toc132668148)

[Platform Requirements 13](#_Toc132668149)

[Conclusion 13](#_Toc132668150)

[References 13](#_Toc132668151)

# Introduction

With the rise of cyber-attacks happening all over the world, how do you stay protected on the internet? The internet is massive and nearly everyone in the world has access to it, with that being said, a lot of those people don’t understand the security part of it and don’t understand how their information is used, what sort of information about them is used and kept and they don’t even know that a malicious person could easily find out where they live, work, what they search on a daily basis or how they use their computers just simply by looking at the data that is gathered from visiting websites.

A general user doesn’t understand the importance of the digital footprint that they leave and how their information and files they store on the internet are used by companies not only for them to make money but to also put you at very high risk to become a victim of a cyber-attack.

A great way to prevent a big part of this problem that could happen to you everyday is to invest in a VPN and a Cloud Document Management System to keep your information at least a little bit more private, unless you do it all yourself for a fraction of the cost?

This paper will cover my research on VPN’s and Cloud Storage that a person could set up by themselves and to get educated on how to do so to lessen their digital footprint and protect their files, information but most importantly themselves from any cyber-attacks.

# VPN

## What is a VPN?

A VPN or other known as a Virtual Private Network is a way of extending a private network across a public network (Virtual Private Network, n.d.). This allows for users to connect to a private network that could be across the world.

## Why is it important?

When using the internet, devices are constantly exchanging data with the other devices on the web without the user even realising it but most importantly, the user’s IP can become public on some websites which is a big security risk since a person with bad intent could find out a user’s location, browsing history, operating system information, device identifiers, a VPN is important because it hides the user’s IP address by assigning them a different IP address from its own network which than leaves no traces back to the original user which negates any security risks that were mentioned before.

VPNs are also important for people who work remotely, personally during my internship I worked remotely and every day I was connected to a VPN which allowed me to remotely access the private network of my company which had all the necessary files that I needed to complete my work for the day as well as keeping my device protected and any information that was transferred between my machine at home and the servers that were across the country. Without the VPN the entire company would be at stake and any confidential information that is being sent over through the internet could easily be stolen or even intercepted and changed by a malicious user which would be a massive security risk.

No one is safe on the internet, even if your internet service provider (ISP) claims you are protected, the chances are – you really are not or just protected to a certain extent hence a VPN is important to have even for people who don’t use computers daily. If you are a person who uses public Wi-Fi, your information is out there and at risk to anyone who could use it in a malicious way this also includes any other device like a mobile phone or even a handheld gaming console.

Ideally, you’d want to keep your devices and information always protected whether that be from malicious users or just to keep anonymity when browsing the web hence a VPN would be important for any user.

How does a VPN tie into this project? The VPN is a crucial part of this project, it will allow users to access the server and use the services without any issues by having a point-to-point connection between the server and the device.

Users will be able to connect directly to the server from realistically anywhere they’d like if they have an internet connection. Not only is this important for the users to have access but as well as any administrator will be able to connect remotely to the server and manage it from the comfort of their own home without any interruptions and no security risks.

## VPN Requirements

The VPN is one of the most important aspects of the project, there are a few requirements that need to be met for the server to function efficiently and securely.

Data Encryption is one of the most important requirements for the VPN, it is important that all the information that is being sent through the secure tunnel is encrypted even if it is public files. Most of the packets sent also include information about the user’s device and could sometimes have personal information that should be kept secure.

The VPN needs to be fast and responsive whether that be through the connection process or by loading services if it isn’t, it will then be very tedious to use and it could discourage people from not using the server deeming it useless.

The VPN will need strong authentication methods, whether that be two factor authentication or just a very strict password and username policy. The files and services that are going to be kept on the server are going to be confidential so no unauthorized user should have access to them.

A kill switch is going to be another important requirement on the VPN. A kill switch will disconnect your device from the Wi-Fi if there was to be some sort of outage whether it be on the server or client side, by disconnecting the user from the internet it will significantly reduce the likelihood that the data is intercepted then compromised.

Your IP address is at risk when not connected to any sort of VPN service, hence when connected to the VPN it must hide your IP address to protect your personal information when sending information online.(Kaspersky, n.d.)

## VPN Options

There are many options out there for open-source VPN’s that I could utilise for this project, but there are only a few that fulfil the criteria.

OpenVPN is the first option on the list, it was initially released in 2001, it uses secure point-to-point connections in routed or bridged configurations and remote access facilities and can be installed both on the client and server applications. OpenVPN uses the OpenSSL library to provide encryption of data and control channels and it also does all the authentication with pre-shared keys, certificate based. However, OpenVPN offers the free version to only two simultaneous connections to the VPN which would not be suitable for the project unless I chose to pay for the service. It is also widely available on multiple platforms like Linux, Windows, macOS, iOS and Android. (Wikipedia, n.d.)

WireGuard is another option for the VPN, it claims to be an extremely simple yet fast and modern VPN that utilises state-of-the-art cryptography. It was released in 2019 and unlike OpenVPN it is completely free, it is also used as a base foundation for other VPN’s that are mentioned in this list. WireGuard mainly uses the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24 and HKDF which are all different types of cryptography. It was first initially released for the Linux kernel but since then has now expanded to other platforms like Windows, macOS, iOS and Andriod which would be perfect for any users that use multiple different devices. WireGuard might be regarded as the most secure, easiest to use, and the simplest VPN solution in the industry. (Wireguard, n.d.)

Next on the list is PiVPN, this will turn your Raspberry Pi into a VPN server within minutes. PiVPN is a set of shell scripts developed to easily turn your Raspberry Pi into a VPN server using both WireGuard and OpenVPN. It was originally designed to run on the Raspberry Pi OS Lite, but it will also work on an Ubuntu or Debian server. It uses elliptic curve encryption keys up to 512 bit (PiVPN, n.d.)and it can also run with Pi-Hole which is mainly used as a DNS server that offers network-wide protection, it blocks in-app advertisements, improves network performance, and allows to monitor statistics.

## VPN Conclusion

The VPN or Virtual Private Network is the most important part of this project as it allows for everything to come together and work in this project. The most important of a VPN is security as the user will be using it to connect to the platform and if the VPN is not secure, then a lot of crucial information about the user and the server could be compromised, another part of the VPN that is just as important is the efficiency, if the VPN is not efficient it would tremendously slow down the speed at which the user loads websites and features on the server as well as the internet.

# Cloud Document Management System

## What are Cloud Document Management Systems?

Cloud Document Management Systems allow a user to do many things when connected to a server. They are a web-based data storing and managing app that are used as data servers. A CDMS will allow users that are connected to the VPN securely access their files that are stored on the server whether it be text files, videos, or photos from remotely anywhere if the user has an internet connection.

## CDMS Options

There are a few available open-source CDMS options that can be installed on a Linux, Ubuntu, or Debian distribution servers.

ownCloud is a CDM system that is fully open-source and free to use if you choose to configure and run it yourself, initially released in 2017. It will allow users to store their files and access them whenever they want as well as enables users to share and sync data and keep it safe at the same time, on all platforms. It provides an extra layer of authentication so each user will have their own separate file storage that they can also share with their peers to collaborate. (ownCloud, n.d.)

NextCloud is another CDMS option it is an Open-Source private cloud software which also offers apps like a calendar, contacts, mail, news, notes, bookmarks, and tasks to keep you on track. NextCloud also offers and easy to use user interfaces which comes with many functionalities like search, favourites, tags, and others so you can quickly access the files you need and edit them on the spot. NextCloud also offers a dedicated server hosting which is high customisable and set up depending on the clients’ needs. (Nextcloud, n.d.)

# Operating System

## What is an Operating System?

An operating system or OS for shot is the collection of software that directs a computer’s operations, controlling and scheduling the execution of other programs, and managing storage, input/output, and communication resources. (Dictionary.com, n.d.)

## Operating System Options

There are a few options for the operating system, but they need to match the right criteria and they are also dependant on the platform that the server will initially be running on.

Windows Server 2022 is the first operating system that could be used to host the VPN server alongside all the cloud applications. Windows Server’s development first started in 1993 and it offers a wide variety of different functionalities such as Active Directory and it can be used as a file server, it can host applications, virtual machines and containers and it also has integrated DNS and DHCP services. Windows Server offers advanced multilayer security by using industry standard AES-256 encryption. (Microsoft, n.d.)

Linux is an open-source Unix-like operating system based on the Linux Kernel. It was first released in 1991. It was originally developed for personal computers based on the Intel x86 architecture but has since been ported to more platforms than any operating system. Linux has also become a distribution for other Linux based operating systems such as Debian and Ubuntu. Overall, Linux is a bare-bones operating system and since it is open-source it allowed for the development of other operating systems that provide more functionality dependant on the user’s needs. (Linux, n.d.)

Ubuntu is a Linux distribution based on Debian, like Linux it is also completely open source. Ubuntu was first released in 2004 and since then has been regularly updated. (Ubuntu, n.d.)Ubuntu allows for the user to secure their open-source applications and is currently a very popular operating system for cloud computing with its support for OpenStack. Ubuntu offers a lot of security features out of the box such as disabled ports and full disk encryption. The Ubuntu operating system default configuration comes with certification from the Center for Internet Security (CIS). (ubuntu, n.d.)

Raspbian OS is an operating system that was created specifically for the Raspberry Pi based on the Debian distribution. The first build of the operating system was released in 2012 and it comes with over 35,000 Raspbian packages optimized for best performance on the Raspberry Pi. (raspbian, n.d.)

# Server Security

An important part of the project is to create a very secure server that only users with privileged access will be able to login and view the content of the server or even be able to view the physical server.

### Logical Security

### SSH

SSH or Secure Shell is an important part of server security, it is a network protocol that allows authorised users to connect to servers and execute commands without having to plug their machines directly into the server itself.

All connections made via SSH are automatically encrypted using industry standard encryption algorithms like AES and hashing protocols like SHA-2. (Altaqi, 2020)

SSH is currently the most secure way of accessing a server hence it will be a core security aspect that will be used on the VPN server once it is up and running.

### FTP

FTP or File Transfer Protocol allows for the transfer of computer files between a computer and a server. This is a protocol that was initially developed in 1971. An FTP client is still commonly being used to transfer files even though it is severely outdated and offers little to no security when transferring the files from your device to the server. The authentication process that is used with FTP may be vulnerable to a network sniffing attack which creates a big security risk to files and to any device on a network.

FTP should be disabled on most servers unless it is needed for the first initial configuration or needed for transport of important files, but other methods of file transfer are recommended.

### Version

The version that is running on a server depends on which operating system is installed, it is important to keep the server’s operating system running on the latest and stable version that is available.

Operating Systems can become vulnerable very quickly when outdated hence it is good practice to keep it up to date with the most stable release, this also means that even the most recent update to an operating system isn’t going to be the most secure as there nearly always will be some sort of exploit or vulnerability in the first few months of a new operating system version.

### Disabling services and ports

There are many ports and services that come pre-configured on any server or device. It is good practice to disable any unused services and ports that are never going to be used to reduce the risk of a data breach.

The server should have all the unused ports and services disabled in order to keep maximum security and reduce the risk of any attacks that could occur.

### HTTPS over HTTP

HTTPS or Hypertext Transfer Protocol Secure is an extension of HTTP or Hypertext Transfer Protocol, the “secure” part of HTTPS is TLS encryption other known as Transport Layer Security is a widely adopted security protocol designed for privacy and data security over the internet with the primary use being encryption of communications between web applications and server.

The server should have HTTP completely disabled as it is a big security risk even though all the data will be fully encrypted through other measures, HTTPS will still provide an extra layer of security when browsing through the server’s applications.

### Encryption

Encryption is the process of encoding a message so that I can be read only by the sender and the intended recipient. Encryption systems often use two keys, a public key, available to anyone, and a private key that allows only the recipient to decode the message. (Dictionary.com, n.d.)

Once a user visits a website or connects with another peer, their connection should be fully encrypted, any sort of activity on the internet should be encrypted not only to protect the website but most importantly the user.

## Physical Security

Physical security is just as important as logical security. There are a few aspects to physical security that are sometimes even more important than some of the logical security aspects.

The server room must be secure to the point that only personnel with authorised access are allowed in. Every access point should have alarms and should be monitored. Ideally, the room should not have any windows as they could pose as security risks to an individual with malicious intent.

The server room should also be equipped with monitoring cameras, fire alarms, fire extinguishers and a fire suppression system.

The server room should ideally be in a secluded area that is not available to the general public with full monitoring and 24/7 security.

# Platform

There are multiple platforms that the server could run on, each offering similar or different features, so it is important that the server is running on a platform offers scalability, security and all the features necessary for great execution of this project.

## Platform Options

### Dedicated Server

A dedicated server is essentially a computer that is only used for a specific purpose, for example, a DNS server, its only purpose is to provide DNS for the network. A regular person can own a dedicated server or rent one from a company that provides such service.

Dedicated servers are extremely flexible in terms of scalability, you could build your own dedicated server depending on your specific needs, meaning you could get to choose which components the server is made up, which also means that in the future if your server is getting outdated, slowing down and not powerful enough for your needs, you can upgrade it yourself or the company that is renting you the server can upgrade it for you.

This type of platform can be used for nearly anything, they can run websites, game servers, or even used as a regular day to day computer.

The downside of dedicated servers is that they are quite expensive not only to build yourself, rent but most importantly to run, they use a lot of power which in return would equate to high electricity bills.

Depending on the company and the hardware of the server you choose to rent, according to SERVERMANIA, the lowest price to rent a dedicated server comes out to $40 a month scaling upwards depending on the hardware. (Brinkman, 2023)

If you choose to buy a fully ready-to-go server, it could be anywhere from 500GBP to 750GBP up-front payment depending on the hardware not account for running costs which would include internet, cooling and electricity. (mtg, 2021)

### Raspberry Pi

The Raspberry Pi is essentially an extremely small factor computer that is low power and relatively cheap.

Pi’s are extremely versatile and can literally be used for anything you’d like it to do with enough effort, you are completely in control of the machine meaning that what you want it to do, it can do, from home automation to a gyroscope to running a website, with a Pi it is possible.

The downside of the Raspberry Pi is its components. Depending on the needs of a user, a Pi mightn’t be enough, you get them as they are, meaning there is a lack of scalability on this platform.

Another downside of the Raspberry Pi is that as of writing this research manual, there is a shortage of them, meaning that they are hard to come by and if found, they are at an inflated price point.

The 4GB Raspberry Pi 4 Model B, is priced at around 70 euro (Raspberry Pi 4 Model B, n.d.) which is quite cheap for such a capable machine, although because of the shortage, at this moment in time you cannot purchase a Pi from a retailer, but they are being prices in the range of 160 euro from the likes of Amazon or eBay sellers. (Raspberry Pi 4 Model B, n.d.)

### Virtual Server

A Virtual Server or VPS is an extremely powerful dedicated server that has been separated into partitions which are rented out to users, some may refer to it as a Cloud Server since you don’t physically interact with it.

A VPS offers a great amount of scalability, low costs and somewhat low power usage. A VPS can be upgraded by any chance by the company you are renting it from to whatever your needs may be, this allows you to have full customisation of your own server without having to deal with any of the upgrading which could take hours if you have your own or rented dedicated server.

Most VPS’s offer customer support services since you are renting from them so if you ever encounter any issues with your server, it can get resolved in a quick timely manner depending on your server provider.

The downside of VPS’s is the fact that you don’t always have full control of your server meaning, if your provider wanted to decide to shut down your server for no reason, they could do so which would leave you at a risk of file corruption and money loss if your server is as a business asset.

Linode is a highly reputable company that offers server hosting services, pricing for a VPS with its own dedicated CPU starts at just $36 a month for a 4GB RAM server up to $4,608 a month for a 512GB RAM server. (Linode, n.d.)

## Platform Requirements

For this project, the platform that would be most suitable is one that would have enough resources to run all the applications on the server such as the CDMS + more meaning that the server would need at least a minimum of 4GB of RAM and a minimum of 50GB of expandable storage.

The server must also be low-power and cost efficient so that anyone who would like to create their own version of this project or anything similar, they could easily do so without having to pay a fortune in setup and monthly bills.

The platform must also create a reliable foundation for a person to work from so they can encounter the least number of issues while attempting a project like this or a project of their own.

Finally, the server must be scalable on command, the server should be capable of upgrading in a timely manner if it is required to do so.

# Conclusion

This research manual covers a lot of useful information that would educate a general user in terms of topic such as, VPN, cloud document management systems, server security, operating systems and platforms. This paper did not answer questions on what a user should do when trying to keep their information private while browsing the internet, but it did give insight on things to keep in mind when creating your own web server, or any type of server at that point as well give an insight into technologies that general users might not have ever looked into to enhance their privacy like the VPN or creating your own server to store all your files instead of paying corporations with hope that they don’t use your information and files maliciously and to their advantage.

# References

(n.d.). Retrieved from Ubuntu: https://ubuntu.com/

Altaqi, W. (2020, September 10). *The What, Why & How of SSH Protocol*. Retrieved from KEYFACTOR: https://www.keyfactor.com/blog/ssh-protocol/

Brinkman, E. (2023, February 10). *How Much Does a Server Cost For a Small Business in 2023?* Retrieved from servermania: https://www.servermania.com/kb/articles/how-much-does-a-server-cost-for-a-small-business/

Dictionary.com. (n.d.). *Encryption*. Retrieved from Dictionary.com: https://www.dictionary.com/browse/encryption

Dictionary.com. (n.d.). *Operating System*. Retrieved from Dictionary.com: https://www.dictionary.com/browse/operating-system

Janssen, D. (2022, September). *What is a VPN? How Does it Work and Why Do You Need One?* Retrieved from vpnoverview: https://vpnoverview.com/vpn-information/what-is-a-vpn/

Linode. (n.d.). *Dedicated CPU Plans*. Retrieved from linode.com: https://www.linode.com/pricing/#compute-dedicated

*Linux*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Linux

Microsoft. (n.d.). *Windows Server*. Retrieved from Microsoft: https://www.microsoft.com/en-ie/windows-server

mtg. (2021, April 23). *How much does a server cost for small & medium businesses (UK)*. Retrieved from manxtechgroup: How much does a server cost for small & medium businesses (UK)

Nextcloud. (n.d.). *About Us*. Retrieved from Nextcloud: https://nextcloud.com/about/

ownCloud. (n.d.). *About Us*. Retrieved from ownCloud: https://owncloud.com

*Raspberry Pi 4 Model B*. (n.d.). Retrieved from thePiHut: https://thepihut.com/products/raspberry-pi-4-model-b?variant=20064052740158&src=raspberrypi

*Raspberry Pi 4 Model B*. (n.d.). Retrieved from amazon.co.uk: https://www.amazon.co.uk/Raspberry-Pi-Model-4GB/dp/B09TTNF8BT?th=1

raspbian. (n.d.). Retrieved from raspbian: https://www.raspbian.org/

ubuntu. (n.d.). *Certifications & Hardening*. Retrieved from ubuntu: https://ubuntu.com/security/certifications

*Virtual Private Network*. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Virtual\_private\_network