SECURITY ISSUES IN CLOUD COMPUTING

BY

Rehnuma Tasnim
ID: 191-15-12770

Afrin Akter Mim
ID: 191-15-12862
AND
Salman Hasan Mim
ID: 191-15-12655

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University

Co-Supervised By

Md. Sanzidul Islam
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
JANUARY 2023

APPROVAL

This Project titled **"Security Issues In Cloud Computing"**, submitted by **Rehnuma Tasnim, Afrin Akter Mim,** and **Salman Hasan Mim** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 07 January, 2023.

BOARD OF EXAMINERS

Dr. Touhid Bhuiyan — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Subhenur Latif — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Mohammad Monirul Islam — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

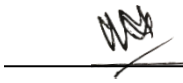
26-01-23

Dr. Dewan Md Farid — **External Examiner**
Professor
Department of Computer Science and Engineering
United International University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Dr. Md. Ismail Jabiullah, Professor, Department of CSE and** co-supervision of **Md. Sanzidul Islam**, **Lecturer**, **Department of CSE, Daffodil International University**. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree.

Supervised by:



Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University

Co-Supervised by:

Md. Sanzidul Islam
Lecturer
Department of CSE
Daffodil International University

Submitted by:

Rehnuma Tasnim
ID: -191-15-12770
Department of CSE
Daffodil International University

Afrin Akter Mim
ID: -191-15-12862
Department of CSE
Daffodil International University

Salman Hasan Mim
ID: -191-15-12655
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year Thesis successfully.

We really grateful and wish our profound to our supervisors **Professor Dr. Md. Ismail Jabiullah and Md. Sanzidul Islam, Lecturer, Department of CSE, Daffodil International University**, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of Network based research to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Touhid Bhuiyan, Professor,** and **Head, Department of CSE, Daffodil International University, Dhaka.** For his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

The cloud is one of the most significant technologies nowadays. For the vast majority of our activities, this cloud computing technology acts as the cornerstone. Our endeavor was divided into three different parts. Studying the offers of the various cloud suppliers is necessary to fully understand the services or advantages we can experience from using the cloud. Then, we build an on-premises network architecture to get further networking knowledge. Researching numerous cloud security flaws and potential fixes will be our next priority. People will be able to comprehend the numerous services that different cloud providers offer. Our network design is adaptable to any organization's needs. Our research may be utilized to learn about numerous issues with cloud security and potential remedies.

TABLE OF CONTENTS

LIST OF TABLES:

LIST OF FIGURES:

CHAPTER 1
INTRODUCTION

1.1 Introduction

The term "cloud" has many meanings depending on who you ask; software engineers, system administrators, and even database administrators all have their own ideas on what it entails. The "cloud" describes a pool of customizable services that end users may tap into through an Internet connection. Cloud services from companies like Microsoft, Amazon, Google, and others may cost users money depending on their membership and use. There are several providers of various Cloud services, such as those for messaging, social computing, storage, customer relationship management, identity management, content management, and so on. Cooperative use of available resources is essential to cloud computing. By using cloud computing, application software may be used with these linked devices. The term "cloud" may also be used interchangeably with "cloud computing." Services like data storage are only one example of the many that may be accessed through cloud computing. By pooling available resources, cloud computing ensures reliability and cost-effectiveness. On the basis of these two approaches, cloud computing might be classified as either public or private. The implementation and distribution models for cloud computing services. This is a typical format for a backup file. You may use the same document for several jobs of different types. To put it another way, cloud computing simplifies things by letting you do things you couldn't before with a regular PC. Cloud computing boosts responsiveness in another way: by making resources more easily accessible. Cloud computing services are often broken down into three categories: infrastructure, platform, and application (SaaS). Clients often use cloud services on an as-needed basis, and this is typically on an hourly basis. The cloud's pay-as-you-go model has made it such that customers may use their services whenever they choose, and the provider handles all maintenance and upkeep. The usage of Cloud Computing has been exploited by some of the most basic security threats. Since botnets are used to spread spam and malware, they pose a security risk. In 2010, the United

States Secret Service looked into 761 data breaches, and more than 63% of them occurred at companies with 100 employees or less. Even more so, Symantec Corp., a provider of security technologies, found that over 73% of small and medium-sized firms had been compromised by a cyber-attack in a survey of more than 2,000 organizations in 2011. One of the best features of cloud computing is the pay-as-you-go model of computing as a resource. With this strategy, businesses and nonprofits that want substantial processing capacity may get it without spending a fortune on new computer systems and networking components. Scalability and increased flexibility at a cheap cost are two further advantages of cloud computing. A recent paradigm shift in the evolution of distributed systems is cloud computing. The cloud architecture is abstracted so that the user doesn't need any special expertise or training to utilize it. The most popular business applications are now hosted online and may be accessed from any web browser.

1.2 Objectives

One of the most important technologies nowadays is the cloud. This cloud computing technology serves as the foundation for most of our work. We separated our effort into three distinct segments. To comprehend the services or benefits we may have from using the cloud, we must study the various cloud suppliers' offerings. To learn more about networking, we then construct an on-premises network architecture. Our next task will be to research various cloud security vulnerabilities and possible solutions.

• People will be capable of understanding the various services offered by various cloud providers.
• Any organization can adapt our network architecture for its organization.
• Our work can be used to learn about various cloud security challenges and potential solutions.

1.3 Motivation

Biologically speaking, we have an innate predisposition to actively seek out and respond to threats. However, this may serve as a powerful inspiration for some. The term "network security" refers to a collection of technologies aimed at stopping unauthorized users from accessing and spreading malicious code throughout an organization's network. The main goal of network security is to avoid these potential problems: Abuse of the system without permission. Alterations to the usual operation of the network, such as interruptions, slowdowns, or other forms of interference. Abuse of the Internet in contravention of the Principles for the Ethical and Lawful Treatment of Data (SPG 601.07). Whether you're based in Chicago or Tampa, the widespread increase in cybercrime is a major problem for companies anywhere in the United States and worldwide. Florida is one of the hardest-hit states in the United States, with year-to-date ransomware incidents increasing by 185%, according to recent estimates. In today's world, however, ransomware is the only real danger facing companies. Companies might lose thousands of dollars due to cybercriminals' innovative methods of infiltrating or destroying susceptible networks. There are five essential components of a safe and secure network. Identity: One of the most important aspects of any network is its ability to positively identify its users, hosts, applications, services, and resources. Kerberos, password management programs, and authentication protocols like RADIUS and TACACS+ make it possible to verify the identity of a user. Perimeter security: Network applications, data, and services may be protected against unauthorized users and unwanted data with the help of perimeter security. Data privacy: Data privacy refers to the precautions taken to prevent unauthorized parties from seeing or changing data that has been requested by a legitimate user. When it comes to securing Virtual Private Networks, tunneling, encryption, and protocols like IPSec are crucial (VPNs). Security monitoring: Testing and monitoring your security measures on a regular basis is also essential. Being proactive allows you to spot problem areas and make necessary modifications. You will be prepared for a genuine security incident. Policy management: You'll need policy management if your network ever becomes too big or too complicated

to administer. As the network expands, you'll require centralized policy-management technologies that use directory services. Enhancing the usability and performance of your network's security solutions, these tools develop, distribute, enforce, and audit the security policy using browser interfaces. How you handle security issues is crucial to your cloud security strategy. To improve your reaction time during detection, investigation, and recovery, practice incident response using simulations and automated tools. To specify how to design and secure cloud-based activities and operations, such as identity and access management, techniques and controls to secure apps and data, and ways to achieve and maintain visibility into compliance, a cloud security architecture is developed. Although many businesses still hold to the false belief that on-premise and hardware-based security provides a higher level of safety, the reality is exactly the contrary. The advantages of cloud security versus on-premise security are made abundantly clear by the benefits of cloud computing. Select the most reliable cloud security service to protect your cloud based data.

1.5 Related Work

The cloud is where distributed systems are heading now. Thanks to the abstraction provided by clouds, users don't need to worry about the underlying infrastructure. Cloud service providers host and make available popular web-based business applications that may be accessed from any internet-connected device with a web browser. [2]. The findings of this study provide a thorough illustration of the efforts made from the perspective of next-generation cellular networking and the open research areas that must be explored to extract the maximum benefit from the combination of telecommunications and cloud computing. [3] This article takes a macroeconomic perspective on the cloud computing industry, looking at a variety of service providers. It calculates the costs associated with service provision under different scenarios. DropBox, Box, and SugarSync are examined in depth, along with a few lesser-known personal cloud services, in this work (see [4]). Key features of personal cloud storage services were

tested for efficiency, with special attention paid to the methods by which data was transferred. [6] Various definitions, properties, and technologies of Cloud computing were shown by the research community. They have shown many prototypical Cloud computing environments. This article discusses [7] the benefits and drawbacks of using cloud computing, cloud storage systems, and infrastructure built with web services like Amazon Web Services. [8]. The findings of this paper's comparison show that the characteristics of different cloud storage systems are a major factor in the selection procedure. [10] They brought attention to ongoing improvements to a decentralized computing and networking infrastructure for ocean research that is diverse. [13] This article is to examine the Windows Azure technologies developed by Microsoft and the commonly used servers. [14] This article details the plan for a state-of-the-art network at a university, complete with Internet of Things devices and common networking hardware. They use Cisco Packet Tracer 7.0 to create a three-tiered hierarchical framework with several functions. It uses Micro Controller Units (MCUs) programmed in Python to connect and manage IoT devices. After an IoT device establishes a connection to an IOE server, the IOE service may be activated. With its four Ethernet ports and "Home gateway" SSID, the home gateway facilitates the connection of various wireless access points. Establishing a safe wireless network at home is as simple as configuring your gateway to use WEP/WPA-PSW WPAL. [18] This article provides a summary of four significant routing protocols (RIP, EIGRP, IGRP, and OSPF) based on several factors such as transmission cost, latency for queuing, and other considerations (RIP, EIGRP, IGRP, and OSPF). These factors all contribute to OSPF's superior performance. [19] In this article, we'll discuss how to establish a campus network to provide sufficient service while keeping administration expenses low. The use of a hierarchical design was necessary to accomplish this. We used many features of Cisco Packet Tracer to design this local area network (LAN) layout. They use a certain range of IP addresses and are partitioned into several subnets, with some of those subnets being kept for possible future use or scalability. They also use a wide variety of IOE devices, each of which has a unique encoding scheme to connect to the network. [22] The fundamentals of the Cisco technology platform, in particular routing and switching, are

more abstract and difficult to witness compared to real hardware and simulator software, making it difficult for students to learn. The study compared physical labs to virtual ones and analyzed the features of several simulator software packages before recommending one as a solution to the issue at hand. Finally, it provided a brief description of how three distinct lab strategies developed over time in Routing & Switching Technology courses have been affected by simulator software. [25]

CHAPTER 2

OVERVIEW OF CLOUD COMPUTING

2.1 Network Layers

In networking, layering refers to the practice of subdividing the process of message transmission into progressively lower levels of abstraction. Each division is responsible for a certain aspect of the overall communication process. The TCP/IP paradigm describes how these protocols work together to transmit data across the Internet. You must take into account the following four levels: i. Application Layer: The first layer, the application layer, is responsible for encoding and decoding the message so that it can be read by both the sender and the receiver. The client initiates communication by sending a command to the server, and the server responds by assigning the client a port number. After that, the client initiates a connection with the server by sending an initial connection request, and the server responds with an acknowledgment (ACK) once it has received the request. At this point, the client has established a connection with the server and can either download files from the server or upload them. ii. Transport Layer: The second layer, known as the transport layer, is in charge of chopping up the data transfer into manageable pieces (packets). There are a certain amount of packets in total, and each packet has a unique number. This data is used by the receiver to reassemble the packets in the proper sequence. The receiver may also check for any lost data bytes. iii. Network Layer: Third, the network layer, which includes the sender's and receiver's IP addresses. The network will be able to trace the message's origin and destination. In the OSI model of computer networks, the network layer is located at the third level. Its primary job is to move data packets through a network from its origin to its final destination. Both the sending and receiving hosts are necessary for its completion. The data link layer is responsible for taking packets from the transport layer and encapsulating them in datagrams before passing them on to the physical layer for transmission to their final destinations. The packet is removed from the datagram and sent to the appropriate transport layer once the datagram reaches its destination. iv. Data Link Layer: The fourth layer of network architecture is the data connection layer, which facilitates the

transmission of data between individual network nodes and between other networks. Each link is the communication channel between two neighboring nodes, and each link must be traversed by the datagram as it travels from its source to its destination. Datagrams in a Data Link Layer may be processed by a variety of link layer protocols along a given route. Ethernet, for instance, handles the datagram on the first connection, whereas PPP does it on the second. By using a layered approach, not only can standards be created, but they can also be modified to accommodate future technology and software. As an example, several apps use the same transport, network, and link layers but each has its own application layer. The mode of communication itself stays the same; what changes is the program's encoding of the message. The transition from IPv4 to IPv6 addressing has the same effect on just the network layer; all other levels continue to function normally. Because of this, progress may be done without requiring a radical rethinking of current modes of interaction.

2.2 Cloud Computing Delivery Model

The use of software as a service models is rising quickly. Software as a service (SaaS) is a model of delivering software, often from a third-party provider, via the Internet, with a focus on facilitating user interaction. Plugins are necessary, although SaaS apps may be accessed straight from a browser without any prior downloading or installation. When using a cloud service, users are granted access to the provider's cloud platform for application deployment. SaaS eliminates the burden of managing software installations and updates across a network. This design makes it simple for businesses to enhance their support and maintenance capabilities, since third-party providers may take care of the applications, runtime, data, middleware, operating system, virtualization, servers, storage, and networking. The fundamental advantage of SaaS is that it does not need any initial software or hardware purchases. i. Infrastructure as a Service: Infrastructure as a Service allows for the monitoring and management of remote center infrastructures, including computing (virtualized or bare metal), storage, and networking. Users may buy IaaS based on their use, similar to conventional utilities. Users are responsible for managing

applications, data, runtime, and middleware while using IaaS. Still managed by providers include virtualization, servers, storage, and networking. In addition to virtualization, IaaS companies also provide databases, message queues, and other services. ii. Platform as a Service: Platform as a service (PaaS) is a type of cloud computing services that enables customers to design, run, and manage applications without having to set up and maintain the requisite infrastructure. The cloud service provider will take care of lower-level infrastructure, network topology, and security concerns, so one need not bother about these. Using this technology, third-party vendors may manage the operating system, virtualization, and the PaaS software itself. Developers oversee application administration. PaaS-enabled apps have access to cloud characteristics such as scalability, multitenancy, support for SaaS, and high availability. This strategy is useful for organizations because it reduces the amount of code necessary, automates business activities, and facilitates the conversion of applications to the hybrid model.

2.3 Cloud Computing Deployment Model

i. **Public clouds:** Public clouds include sharing cloud services via an open network. The model faithfully represents real-world cloud hosting. This vendor offers a wide range of cloud-based services to its clientele. There is no way for customers to have any say in the placement of infrastructure. There may be very little or no structural difference between public and private clouds, except for the degree of security guaranteed by cloud hosting organizations for the different services delivered to public cloud members. Organizations in need of load management might benefit from using public clouds. Lowering costs in both setup and ongoing maintenance make the public cloud approach worthwhile.

ii. **Private Cloud:** An organization's internal IT department manages the firewall protecting a private cloud, which is another kind of cloud computing platform. With a private cloud, only authorized users may

access the company's data, giving the company more peace of mind. These real machines, which may be located anywhere, provide private cloud services that tap into a limited set of resources. If a company has needs that are often changing, crucial administrative chores, and a need for 100% uptime, the private cloud is the best option. Private clouds don't need to adhere to the same stringent standards of security and bandwidth availability as their public cloud counterparts.

iii. **Hybrid Cloud:** Integration is at the heart of the Hybrid Cloud computing model. Depending on the context, this might mean any of the following configurations of two or more cloud servers: Since hybrid clouds may cross provider borders and isolation, it is difficult to classify them as either public, private, or community clouds. You may expand your cloud service's storage and processing power by combining it with other cloud packages and tailoring them to your needs. Resources in a hybrid cloud may be handled by an organization's own staff or by an external vendor. Workloads may move freely between the public cloud and the private cloud as a result of this compatibility.

2.4 Major Services And Cost Factor

loud computing delivers network, computer, and storage capabilities that are userfriendly and easily accessible over the internet.

i. **Network service:** Connecting your network's resources via a third-party service provider is what we call "cloud networking service." Each cloud computing service has its own networking infrastructure, which is configured and supported in a different way. All other networking providers were ignored in favor of Amazon, Microsoft Azure, and Digital Ocean. First and foremost, we are aware of DDoS protection, IPv4 and IPv6 support, virtualization

networks, content delivery networks, domain name system (DNS), private connections, and load balancing are the fundamental building blocks of networking services. The goal of load balancing in computing is to maximize processing efficiency by distributing a group of tasks over a pool of available resources. In essence, its purpose is to improve users' response times. A load balancer is a device that monitors incoming network traffic from clients and then forwards routing requests to predetermined endpoints. It keeps an eye on the right place to make sure the resources go where they need to go. Following is a breakdown of the many load-balancing tools available. Sometimes, people may refer to their IP (Internet Protocol) addresses as their "unique addresses." Its primary goal is to recognize a gadget. The difference between IPv4 and IPv6's footprints is striking. IPv6 addresses are 128 bits long, but IPv4 addresses are just 32 bits long. This trio of cloud providers offers IPv4 service. Amazon and Microsoft Azure both supported IPv6, however Digital Ocean did not. Via the use of virtual networks, devices in different geographical locations may access the same resources as those connected through a traditional physical network. Because of this feature, the virtualization method is possible. The content delivery network feature distributes data across a network using dispersed groups of computers that are all connected to one or more central servers. It is often used for the rapid distribution of content to users in a variety of locations through servers connected to a worldwide network. Domain Name System (DNS) is a hierarchical distributed database that allows IP addresses and other data to be stored and retrieved using names. DNS services are offered by all three of these companies: Amazon, Azure, and Digital Ocean.

ii. **Compute service:** Electronic or non-electronic data and information transmission, storage, maintenance, organization, presentation, generation, processing, and analysis using information technology and computer systems (including software, application service provider services, hosted computing services, information technology and telecommunication hardware, and other

equipment). In this post, we will examine the top three cloud service providers, including Amazon Web Services, Microsoft Azure, and Digital Ocean. Each of these businesses offers a unique set of computer services to its clientele. As a result, we'll be using one service from each of these cloud computing companies. Amazon uses AWS Lamda, Microsoft uses Azure VM, and Digital Ocean uses Kubernetes.

iii. **Storage service:** Traditional network storage and hosted storage are important for the development of cloud storage. The advantage of cloud storage is the ability to access data from any location. Cloud storage services may store everything from a single file to a large enterprise's inventory. Customers will pay the cloud storage provider depending on the amount and manner in which they deliver data. The cloud storage client uploads the data to the data servers of any cloud storage provider. The availability of redundant copies of client data on all or opposite data servers of cloud storage providers promises that the customer's data is preserved even if anything goes wrong. Most systems store identical data on a server with several power supplies. Due to the growing proliferation of data and the need to keep it more secure and for a longer amount of time, companies must integrate how they handle and use information from the moment it is generated until it is destroyed. We are now able to store all of our data on the Internet. Over the Internet, other firms supply and manage this off-site storage. Cloud Storage signifies a big storage pool with three defining characteristics: access through the Web Services API over an unstable network connection, instant availability of vast quantities of storage, and pay-per-use pricing. It promotes quick scaling. Cloud storage is a cloud computing service. Amazon Web Services, Azure, and Digital Ocean all give a number of storage solutions, but it is unclear which one is optimum for your requirements. Amazon S3 (Simple Storage Service), Amazon EBS (Elastic Block Store), and Amazon S3 Glacier are the most popular AWS storage choices. Azure storage is Disk Storage, Blob Storage, File Storage, and Queue Storage. In addition, Digital Ocean storage provides both Volumes

Block Storage and Space Object Storage. We're here to provide an overview of storage, including what each service is built for, how they vary, and how to utilize each one.

iv. **Pricing structure of vCPU**: We look at pricing kinds and price discrepancies for various virtual CPU types for these vendors in this table.

TABLE 2.4.1: A COMPARISON TABLE ON PRICING TYPE

	Amazon	**Azure**	**Digital Ocean**
Pricing Type	Pay-as-you-go, On-demand	Pay as you go, on-demand per second billing	Pay as you go pricing.

Table 2.4.2: A Comparison table on basic virtual machine cost

Virtual CPU	**Amazon**	**Azure**	**Digital Ocean**
1 vCPU	8.50$	7.59$	5$
2 vCPU	15.23$	15.11$	15$
4vCPU	60.91$	60.74$	40$
8 vCPU	121.50$	121.18$	80$

CHAPTER 3
SECURITY ISSUES & POSSIBLE NETWORKING SOLUTION IN CLOUD COMPUTING

3.1 Cloud Computing Vulnerabilities, Threats And Attacks

As well as a wide range of useful services, cloud service models expose sensitive data, increasing the dangers associated with using cloud computing. Infrastructural as a Service (IaaS), found at the cloud's foundation, delivers the most potent features of the cloud's other layers. IaaS also makes it easier for hackers to launch resource-intensive assaults, such brute-force cracking. Since IaaS allows for several virtual computers, it provides the perfect setting for attacks that need a huge number of separate attacking instances. Another potential security issue with cloud models is data loss. To a greater or lesser extent, data in cloud models is vulnerable to access by both internal and external hackers. Workers inside the company might readily get access to sensitive information, either on purpose or by mistake. Databases in these settings might be compromised by external hackers via session hijacking and network channel eavesdropping. Cloud servers are vulnerable to virus and Trojan horse attacks [6]. In order to create a system with stronger security procedures to safeguard cloud computing environments, it is crucial to first identify the potential cloud threats that might compromise such settings.

3.1.1 Compromised Credentials And Broken Authentication:

Organizations struggle with identity management when attempting to issue rights commensurate with the user's job function. When a user's job role changes or they leave the company, they occasionally fail to revoke access. The Anthem data breach exposed over 80 million customer details due to stolen login passwords. Anthem had neglected to implement multifactor authentication, so once the attackers had access to the credentials, it was game over. Numerous developers

have committed the error of embedding credentials and cryptographic keys in source code and storing them in public repositories.

3.1.2 Exploited System Vulnerabilities:

With the emergence of multitenancy in cloud computing, vulnerabilities in the system and exploitable defects in applications have become a greater concern. Close proximity between organizations that share memory, databases, and resources creates additional attack surfaces. Comparatively to other IT investments, the expenses associated with addressing system risks are modest. The cost of implementing IT procedures to identify and fix vulnerabilities is negligible compared to the potential loss.

3.1.3 Data Breaches:

Cloud settings suffer many of the same vulnerabilities as conventional corporate networks, but because a great deal of data is kept on cloud servers, cloud service providers have become an appealing target. The degree of the harm is often proportional to the sensitivity of the exposed data. Data breaches involving government information and trade secrets may be more catastrophic than breaches involving personal financial information. A corporation that suffers a data breach may be exposed to legal action. The expenses associated with breach investigations and consumer notification might be substantial. Indirect impacts such as brand harm and revenue loss may have a lasting influence on an organization's future.

3.1.4 Permanent Data Loss:

In the past, hackers have wiped data permanently from the cloud to hurt organizations, and cloud data centers are as susceptible to natural catastrophes as any other facility. For increased security, cloud service providers may suggest splitting applications and data over various zones. Important are adequate data backup and disaster recovery procedures. With the adoption of cloud settings, daily data backup and off-site storage are crucial. The responsibility for avoiding data loss is shared between the cloud service provider and the data suppliers. A client may encrypt data before uploading it to the cloud; however, the encryption key must be protected with care. If the key is lost, the data will be gone as well. Sometimes, compliance regulations stipulate how long firms must keep audit records and other documents. The loss of such sensitive information may have severe implications.

3.1.5 Dos Attacks: Disruption of service attacks have been occurring for a while, but recently acquired attention due to cloud computing, since they often have a bearing on accessibility. It's possible that systems may be unresponsive or will time out. Large amounts of processing time are lost during these DoS assaults, which may be charged to the consumer. While distributed denial of service attacks (DDoS) are frequent, asymmetric and application-level DoS assaults that exploit Web server and database vulnerabilities should also be taken into account. Cloud service providers are more prepared to deal with denial-of-service assaults than end users. The most important thing here is for administrators to have ready access to the resources they'll need to counter the assault, and that can only happen if they have a strategy in place ahead of time.

3.2 Essential Elements Of Network Security

The four most important parts of a secure network are firewalls, intrusion prevention systems, network access control, and security information and event management. DLP (data loss prevention), AV (antivirus), WASP (web application firewall), ESP (email protocol security), and many more round out the list. Now that almost all data and applications are online, it is more important than ever to ensure that networks are secure against intrusion. If hackers get access to your company's network, it might be the end for your company's existence. A company's vulnerability to hacking and data theft may be reduced by installing a reliable network security solution. That's why it's so important to strengthen the perimeter of your network. When advanced network security solutions are put into place, a wide variety of dangers are neutralized. There are six main parts to any reliable network security system, and they are as follows:

i. **Firewall in a Network:** When it comes to preventing unauthorized access to your company's internal network from the wider internet, firewalls play a vital role. It keeps tabs on data traveling to and from your network and uses that information to make decisions about what to let through and what to shut

down. An example of such a rule would be to deny access to any and all IP addresses that have not been previously approved as safe, but still permit traffic from known, trusted sources. In order to safeguard networks against widespread dangers, most commercially available firewalls ship with a preconfigured blacklist of suspect IP addresses. Administrators have the option of whitelisting or blacklisting certain domains when setting up security policies for the network. Hardening network security by adjusting firewall settings beyond factory defaults is recommended. Kaspersky or Sophos would work well in that circumstance. To help you easily avoid, identify, and remediate attacks, Sophos endpoint protection combines real-time threat intelligence from SophosLabs with tried-and-true technologies like malicious traffic detection. A user's access policies for the web, applications and devices may travel with them. Kaspersky Endpoint Security protects macOS machines against malware and other online dangers. Protecting the computer's file system in real-time, File Threat Protection monitors for and assesses any attempts to open files on the system. However, there are a few problems: although we have control over Kaspersky, the Sophos interface doesn't let us make any adjustments to the security settings.

ii. **Intrusion prevention system (IPS):** An intrusion prevention system (IPS) is a network device that proactively checks data transmissions for threats. Intrusion prevention systems (IPS) are located within the network and monitor packet payloads for signs of policy violations, malware attacks, and other irregular activity, as opposed to firewalls, which sit on the network's perimeter and determine whether or not to let traffic through. When looking for threats to a network, intrusion prevention systems typically use one of two main detection methodologies. The first approach is signature-based detection, which searches through the most recent threat intelligence databases to find known vulnerabilities and cyberattacks. The alternative is anomaly-based detection, which is used to identify novel risks. The finest IPS

systems can fine-tune their security measures in response to monitored KPIs like throughput, latency, and packet loss. Once an IPS has identified a threat pattern or signature, it will take rapid action to eliminate the threat. Disconnecting the connection, dropping any malicious packets, and blacklisting the source IP are all options. Additionally, the IPS will send out notifications to system administrators through email and/or text message whenever a possible security violation is detected.

iii. **Advanced threat protection**: In order to detect and counteract the growing sophistication of malware assaults that are evading conventional defenses, advanced threat prevention systems use a wide variety of methods. Heuristic and code analysis, a method that delves into the nitty-gritty of a file or program that may be malicious, is the first line of defense. Heuristic analysis works by comparing the code to the patterns of recognized malware. Ransomware is malicious software that encrypts a victim's data without their knowledge or consent, whereas cryptojacking malware hijacks a victim's computer to mine bitcoin. For the most part, contemporary anti-virus software will immediately label a program as malicious if it contains any code that even remotely matches that used in today's most common cyberattacks. Advanced threat prevention also uses sandboxing, which is another method. To do this, you must launch your data or application inside of a virtual machine that has no connection to the real world or your company's network. Next, APT may use heuristics and machine learning to analyze the file's behavior and decide whether it poses a security risk to your company. If malicious software is confirmed to exist, APT will eliminate it and add new details about the attack to databases of threat information, making future scans less time-consuming and more accurate.

iv. **Network access control (NAC):** Network access control (NAC) is a system that combines company-wide regulations and network administrator tools to stop unwanted people and devices from connecting to a business's internal

network. Users within your organization may be given their own secure logins and accounts thanks to NAC. Users may be sorted into groups according to their specific jobs, allowing for the creation of role-based permissions that specify what each group is allowed to do and access inside the company's internal network. Alternatively, NAC may place visitors on a different network with restricted access to prevent them from gaining access to any confidential data. Through the use of NAC software, you may add company-approved gadgets to your system and let the network know exactly which ones should be allowed access. To further guarantee that only low-risk devices are able to access the network, you may also limit access depending on the operating system the device is using and the presence or absence of suitable security software.

v. **Web Filtering:** In order to prevent users from accessing inappropriate content, software called a "web filter" may be installed on their computer. The majority of online filtering software will use up-to-date security intelligence databases to establish a site's quality and reputation, but administrators may also create their own standards on which websites to ban. This is essential for lowering the probability that workers may accidentally visit malicious websites like phony software shops and P2P file-sharing networks. Web filtering also helps organizations boost productivity by blocking access to time-wasting sites like social networking, video streaming, and gaming services.

vi. **Security information and event management (SIEM):** SIEM software allows for full insight into all network activity for network managers. The company's comprehensive security framework—which includes firewalls, IPS, advanced threat prevention systems, network access controls, and more—provides the necessary log data for this purpose. Following this, the program generates a security report detailing probable malware assaults and assessments of unusual network activity. When administrators have all the

facts, they may swiftly respond to threats by limiting user access, isolating networks, and blocking malicious payloads. SIEM software also provides administrators with fine-grained insights on network traffic and signatures, allowing them to make more educated choices about how to enhance network security and reduce exposure to threats. You need to fill out your defenses for devices, apps, and even people in addition to these network security components to have a solid cybersecurity architecture. After gathering this information, administrators may swiftly respond to threats by limiting user access, isolating networks, and blocking malicious payloads. SIEM software also provides administrators with fine-grained insights on network traffic and signatures, which aids them in making educated choices to enhance network security and reduce vulnerability to threats. If you want an expert opinion on how to protect your network, give us a call right now.

vii. **Human Threats:** When it comes to safety, physical protection is paramount. If you don't have a safe and secure physical location, nothing else matters. Verizon found that human error was at blame for 82% of data breaches in their 2022 Data Breaches Investigations Report. Employee mistakes that either directly discloses information (such as through misconfiguring databases) or provide cybercriminals access to an organization's systems are included in this category. Companies confront a significant security risk from human mistakes, but you wouldn't know it from the lack of investment in reducing the likelihood of this happening. Especially under duress and pressure, humans are fallible in their actions. One of the trickiest parts of security to de-risk is, unfortunately, human mistake. In addition to spending money on technologies like DLP, businesses need to invest in people and procedures to support their technological solutions. In order to show where problems arise, security awareness training and simulated phishing might be used.

CHAPTER 4

METHODOLOGY

4.1 ARCHITECTURE FOR ON-PREMISES ORGANIZATION

We are using Cisco packet tracer to design the network infrastructure. The three learning concepts of active learning, social learning, and contextual learning form the basis of Packet Tracer. As a result, it aims to make it easier to produce interactive, collaborative, customized technologies and design a premium quality architecture.

This network architecture will be very helpful for University or College campus, corporate office, mill-industry and many kinds of small & big companies. I think this architecture will be very useful for any organization and by using IoT devices, hopefully this will save our time, be more secure and make sure to protect our privacy and also reduce unnecessary access from outsiders of the organization. It is more secure because all the IoT devices and routers are set up at an advanced level of configuration and all the switch ports and servers are set up in a secure way, so that no one can break it easily.

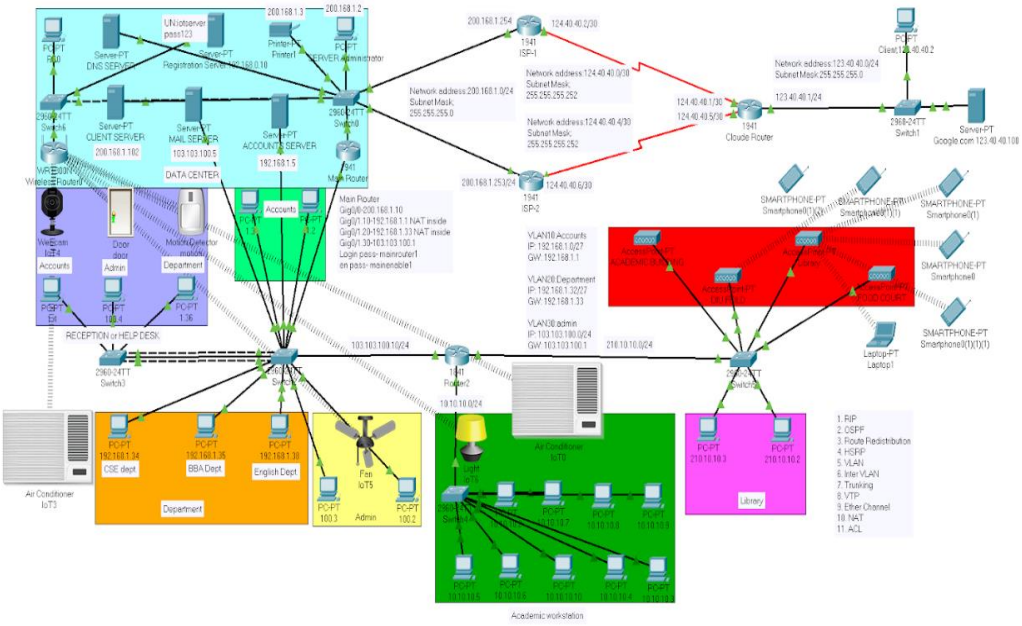


Figure 4.1: Architecture for any on-premises organization

4.1.2 BROWSING FROM CLIENT'S PC

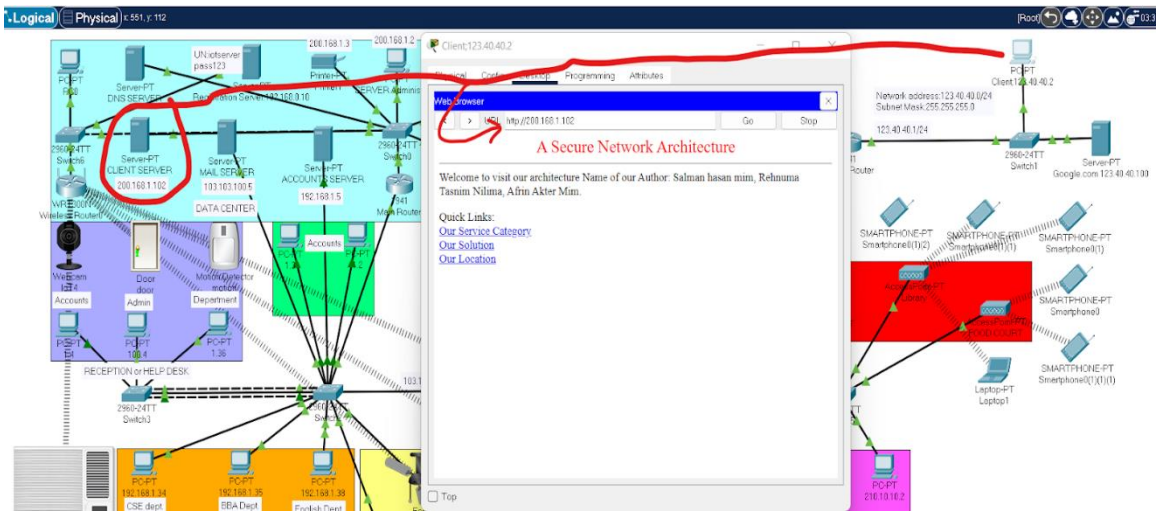


Figure 4.1.2: Browsing client/Web server from the client's pc

4.1.3 PING TESTING ACCOUNTS PC TO DEPARTMENT, ADMIN AND ACCOUNTS SERVER

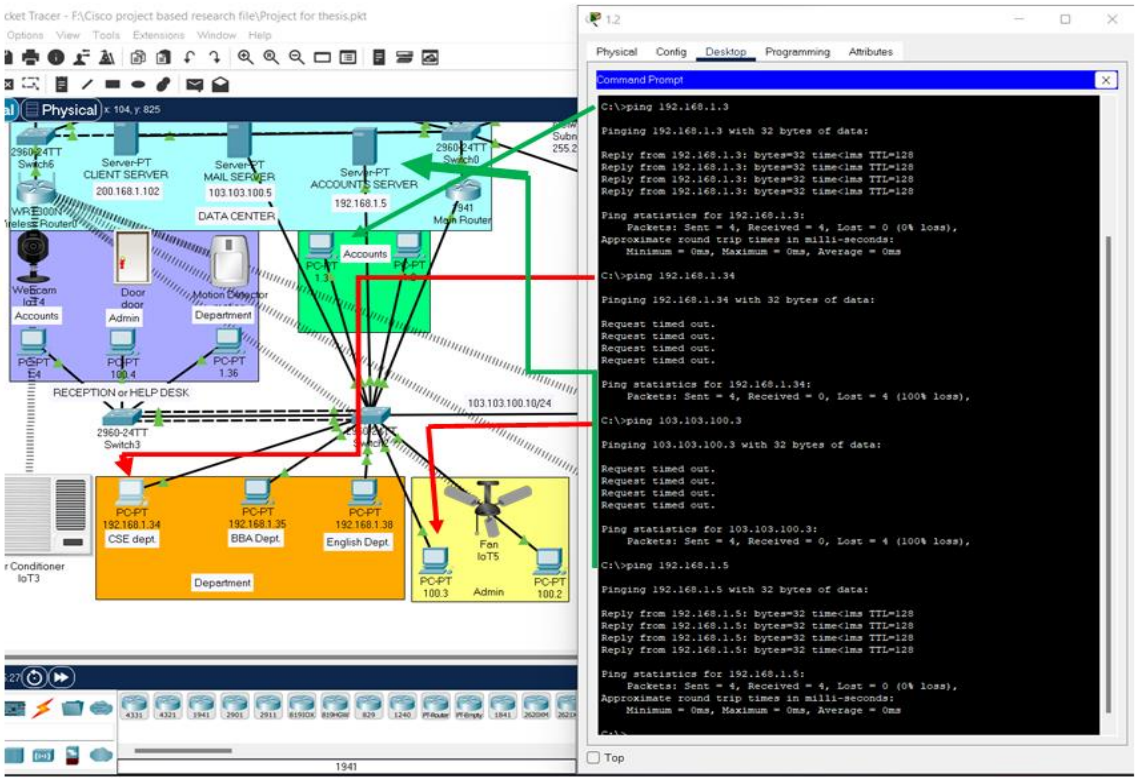


Figure 4.1.3: Ping testing from Accounts PC to Department, Admin and Accounts server

4.1.4 MOTION DETECTOR

Motion detector not detected that's why door light is Red (off).

Motion detector detected obstacle that's why door light is Green(ON)

Figure 4.1.4: Motion detector testing

4.2 CISCO COMPONENTS

TABLE 4.2: DEVICE USED FOR THIS ARCHITECTURE

NO.	DEVICE	FUNCTION
1	Router- 1941	Core connection between ISP1, ISP2 & Office
2	Router-1841	Office network
3	Switch-2960	ISP1 & ISP2 to Office Connection and used to distribute lower layer for access.
4	Switch-3560	Used for Inter vlan.
5	Server-PT: DNS server and DHCP server	Access to visit outsider of the office network.

6	Server-PT: Mail, Accounts, IoT server	Can’t access outsider of the network and control smart thing registered on it.
7	Personal Computer	Connect to access layer in the internet.
8	Motion Detector	Connect in the Home Gateway.
9	Webcam	Capture the movement in the Organization.
10	Air Conditioner	Used to ventilate on some condition.
11	Light	Provide light.
12	Fan	It’s also used to ventilate.
13	Door	Provide cellular system coverage for different user by using motion detector.

4.3 Distributed IP address

TABLE 4.3: USABLE IP ADDRESS FOR THIS ARCHITECTURE

Class	Network Address	Subnet Mask	First IP	Last IP	Host	Type
A	123.40.40.0/24	255.255.255.0	123.40.40.1	123.40.40.254	254	Public
A	124.40.40.0/30	255.255.255.252	124.40.40.1	124.40.40.2	2	Public
A	124.40.40.4/30	255.255.255.252	124.40.40.5	124.40.40.6	2	Public
C	200.168.1.0/24	255.255.255.0	200.168.1.1	200.168.1.254	254	Public
C	192.168.1.32/27	255.255.255.224	192.168.1.33	192.168.1.62	30	Private
C	192.168.1.0/27	255.255.255.224	192.168.1.1	192.168.1.30	30	Private
A	103.103.100.0/24	255.255.255.0	103.103.100.1	103.103.100.254	254	Public
A	10.10.10.0/24	255.255.255.0	10.10.10.1	10.10.10.254	254	Private
C	210.10.10.0/24	255.255.255.0	210.10.10.1	210.10.10.254	254	Public

4.4 USABLE CONFIGURATION AND SETUP

To implement a network infrastructure on Cisco packet tracer, here is given the usable configuration for this architecture:

- The Cisco three-layer network architecture. Cisco recommends a hierarchical network architecture with three levels, or "layers," called the "Core," "Distribution," and "Access." Designing networks according to Cisco's Three Layer Model.
- Use RIPv2 and OSPF routing protocol. (We know that EIGRP offers the best balance between speed, scalability and ease of management. But RIPv2, OSPF support Routing Protocol Authentication.)
- Subnetting.
- Switch port security configure.
- Vlan.
- Inter Vlan.
- Route distribution.
- Hot Standby Router Protocol-HSRP.
- Trunking.
- Access control list (ACLs).
- Server Configuration.
- NAT and PAT

4.5 DEVICE CONFIGURATION

After configuration is done the device gets an IP address dynamically.

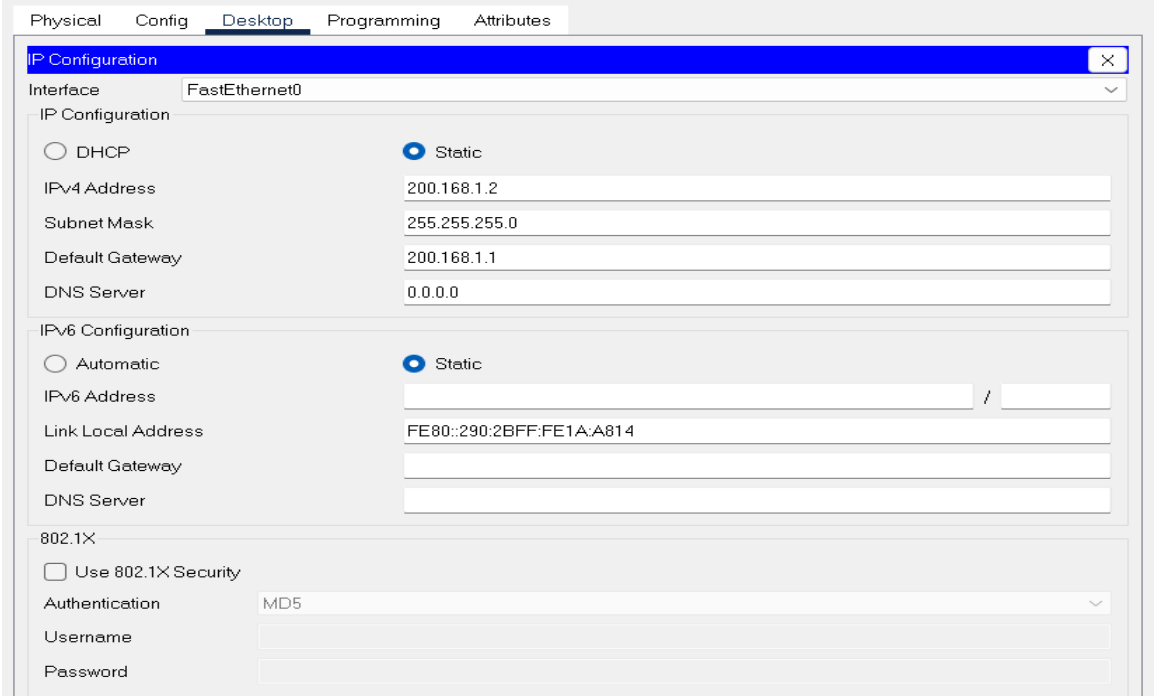


Figure 4.5.1: Server administrator pc configuration.

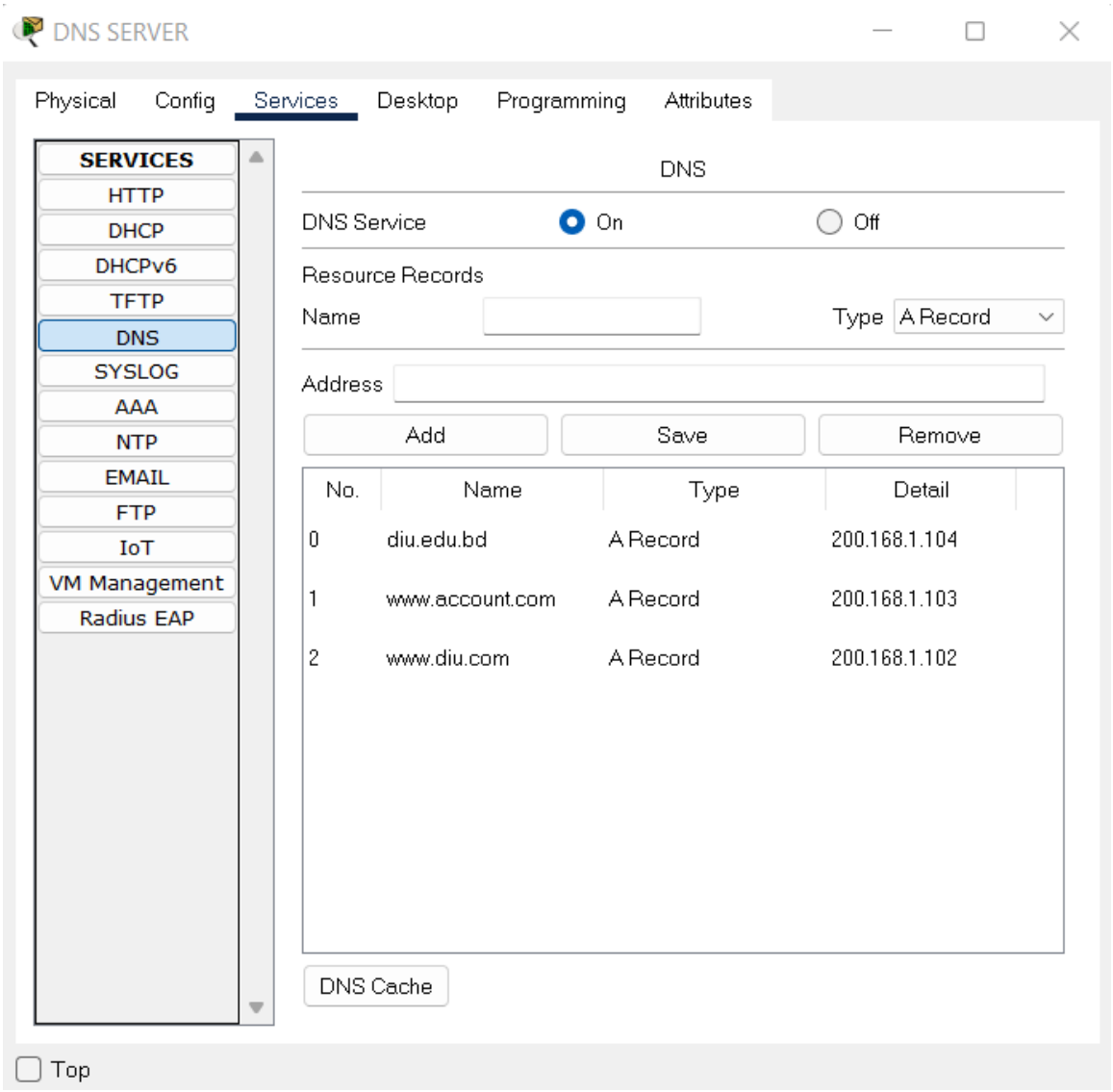


Figure 4.5.2: DNS Server setup and configuration.

When the DNS server configuration is done, then set the IoT server, mail server, registration server, file server and also can set up many types of server that are needed for the organization in the data center. In the IoT server, here we create the client name as Office and set the IP address. Then each of the IoT devices configure with individual Username and password manually.

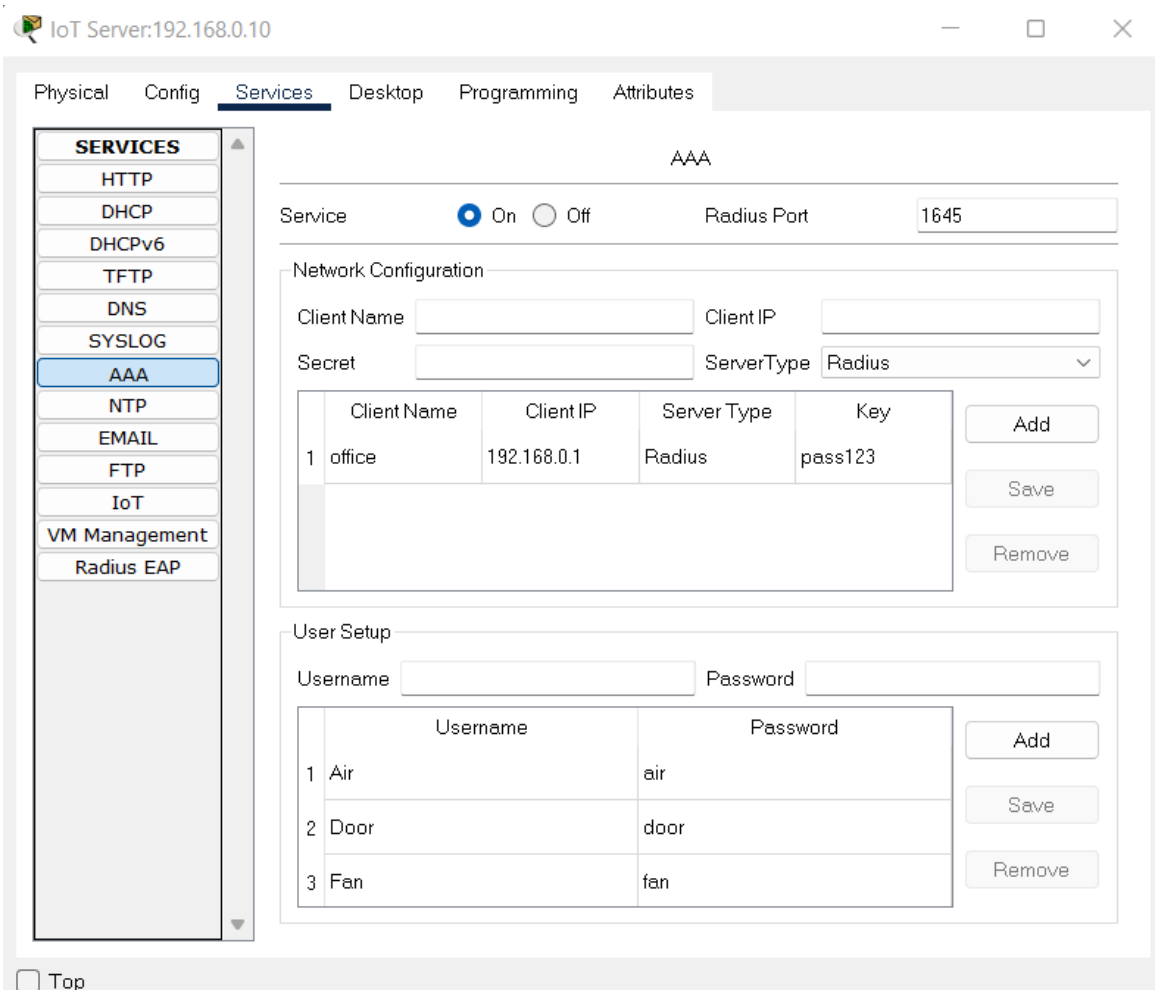


Figure 4.5.3: Configure IoT server

After completing the IoT server configuration then here we use a wireless router to connect the IoT devices.

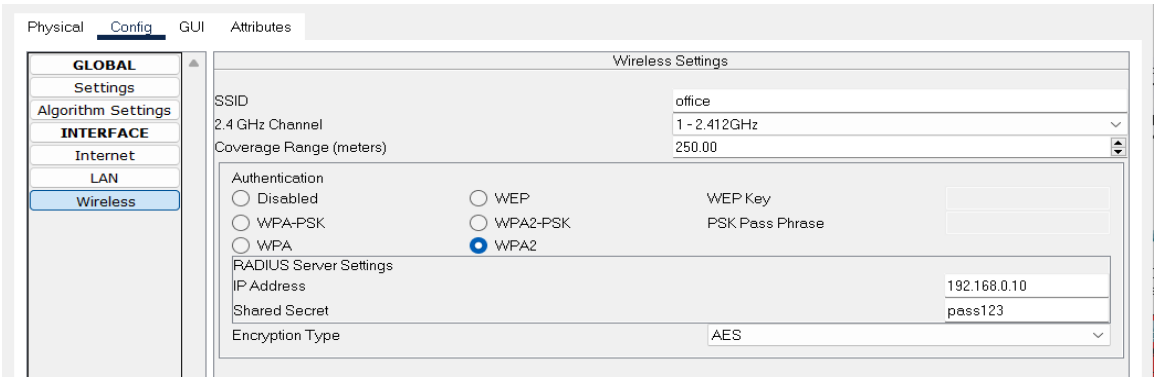


Figure 4.5.4: Configure wireless router for connecting the IoT device.

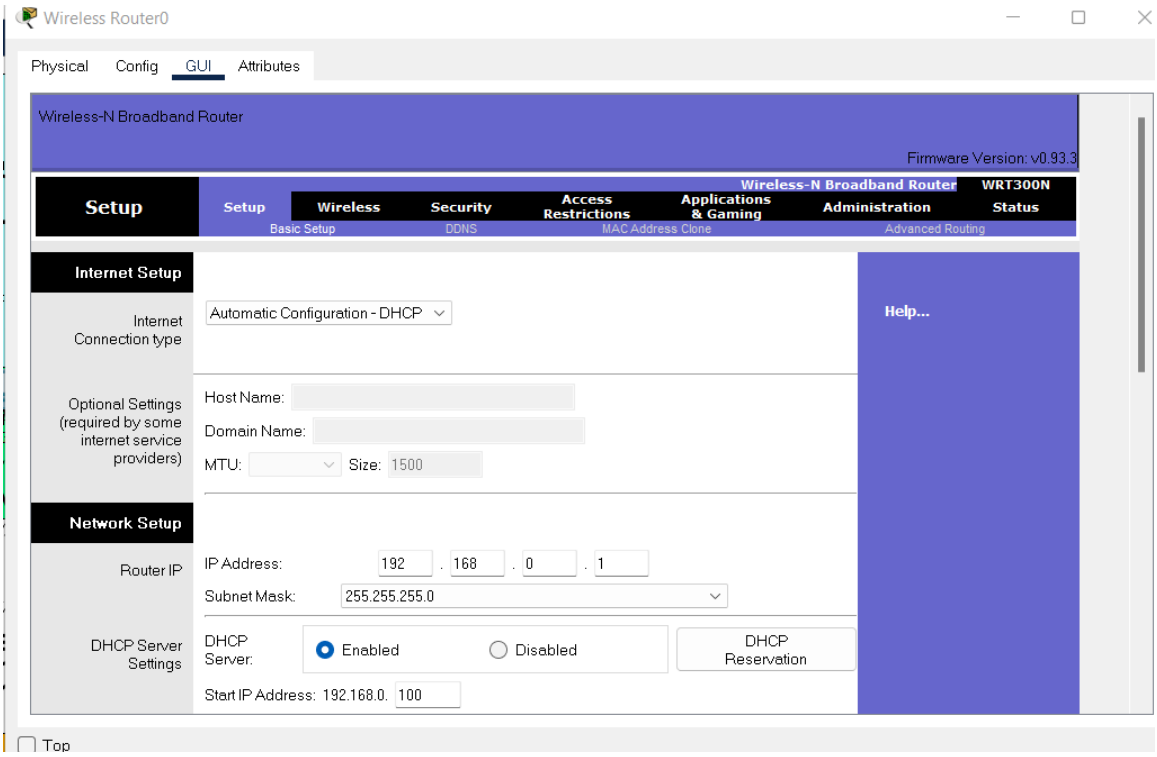


Figure 4.5.5: Configure wireless router in GUI mode for connecting the IoT device.

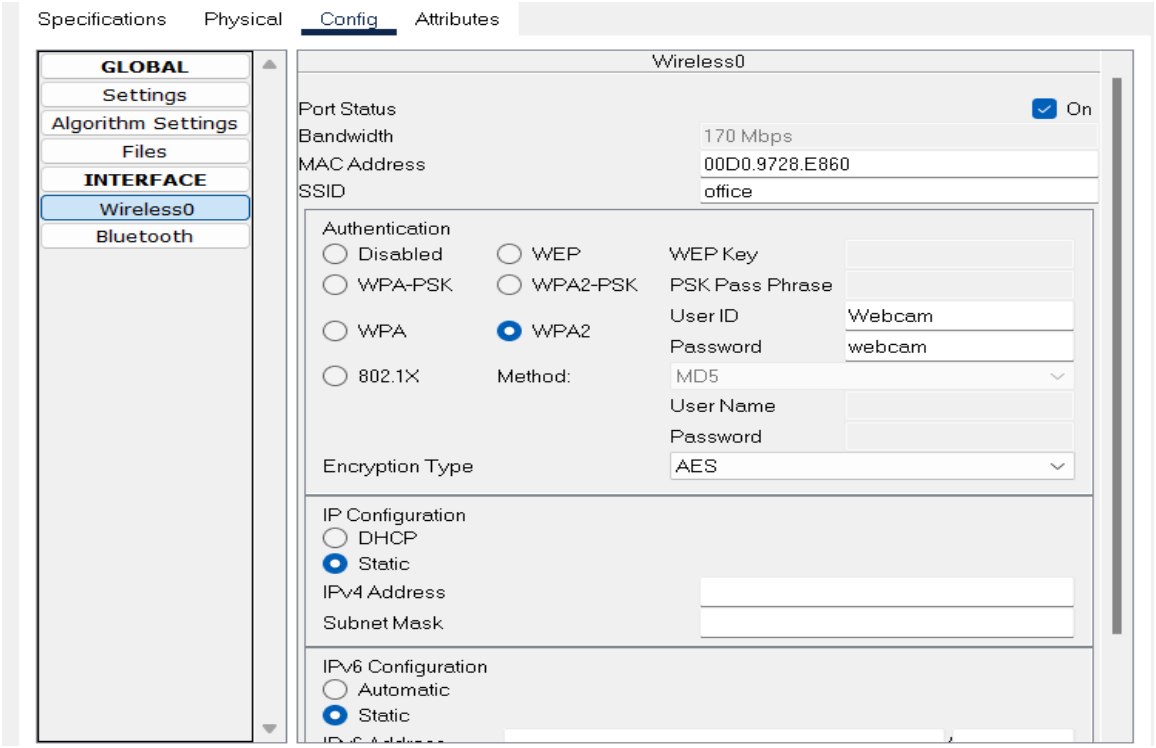


Figure 4.5.6: Configure IoT device with wireless router.

4.5.1 ROUTE DISTRIBUTION

It enables the advertising of routes from one routing protocol in another. It sits in the middle, between OSPF and RIPV2.

4.5.2 HOT STANDBY ROUTER PROTOCOL-HSRP

It ensures that in the event of a first-hop router failure, user traffic recovers seamlessly and instantly.

4.5.3 TRUNKING

A network trunk is a dedicated communications path between two locations, capable of transmitting many signals at once. It is located in two core switches and here we use model 2960-24TT layer 3 type switch.

4.5.4 VLAN AND INTER-VLAN

We use VLAN for distributed three secure sections which are Department, Accounts and admin panel in switch2 and switch3 devices. In the same switch, we also configured Inter-VLAN to assure better security. Inter-VLAN is mainly used to assure the switch spoofing attacks and double tagging attacks.

CHAPTER 5

ANALYSIS AND RESULT

5.1 ANALYSIS BASED ON DIFFERENT SERVICES CLOUD VENDORS

Nowadays we are all moving into cloud computing services to gain better performance because they assure more scalability, flexibility and redundancy for end users. But the security and privacy issues may concern these users. In cloud computing, security and privacy are important elements since a client's data and business logic must be trusted to cloud servers owned and controlled by cloud providers rather than by the customer. So all the cloud providers make sure to provide their services in a secure way to protect their customers' valuable information and data. As a result, the protection of security and privacy are advantages to both cloud service providers and users. By migrating to the cloud, businesses are forced to decide between the comfort of having data and applications housed safely on dedicated, on-premise servers and the purchase price, scalability, and simplicity of using public cloud resources from a provider like AWS. But on-premises infrastructure is genuinely more secure than cloud technology from most debate continues.

DigitalOcean exclusively provides IaaS, whereas Amazon and Azure offer IaaS, PaaS, and SaaS. (IaaS). When it comes to large, scalable applications, AWS and Azure shine, while developers and tiny apps will find more success on Digital Ocean. Users that need to rapidly deploy a powerful, but compact, instance are its primary demographic. Even still, when comparing the efficiency of virtual machines (VMs) on the two systems, Amazon lags behind its scrappier rival. One supplier may be very good at a number of different tasks. When compared to the other three cloud providers, however, Digital Ocean's VPS Performance is higher on every metric we measured: network speed, CPU consumption, web server capacity, rate of CPU-intensive operations, and Sequential read/write speeds. Putting it bluntly, "Digital Ocean is not a real competition to Amazon

and Azure," However, the continuing pricing battle between Amazon, Microsoft Azure, and Digital Ocean is as fierce as ever. If you believe you will be sending out a lot of data, it's best to go with a company that provides a large allocation rather than one that charges you by the gigabyte. The absence of Interzone data transmission emphasizes this point. Unfortunately, none of the three cloud service providers provides a clear explanation of the various subscription options and their associated costs (though Microsoft is a bit better than Amazon and Digital Ocean in this regard). And although the two companies' cloud services may differ in a variety of ways, Amazon's information page seems positively esoteric when compared to Digital Ocean's no-nonsense approach.

5.2 DIAGRAM

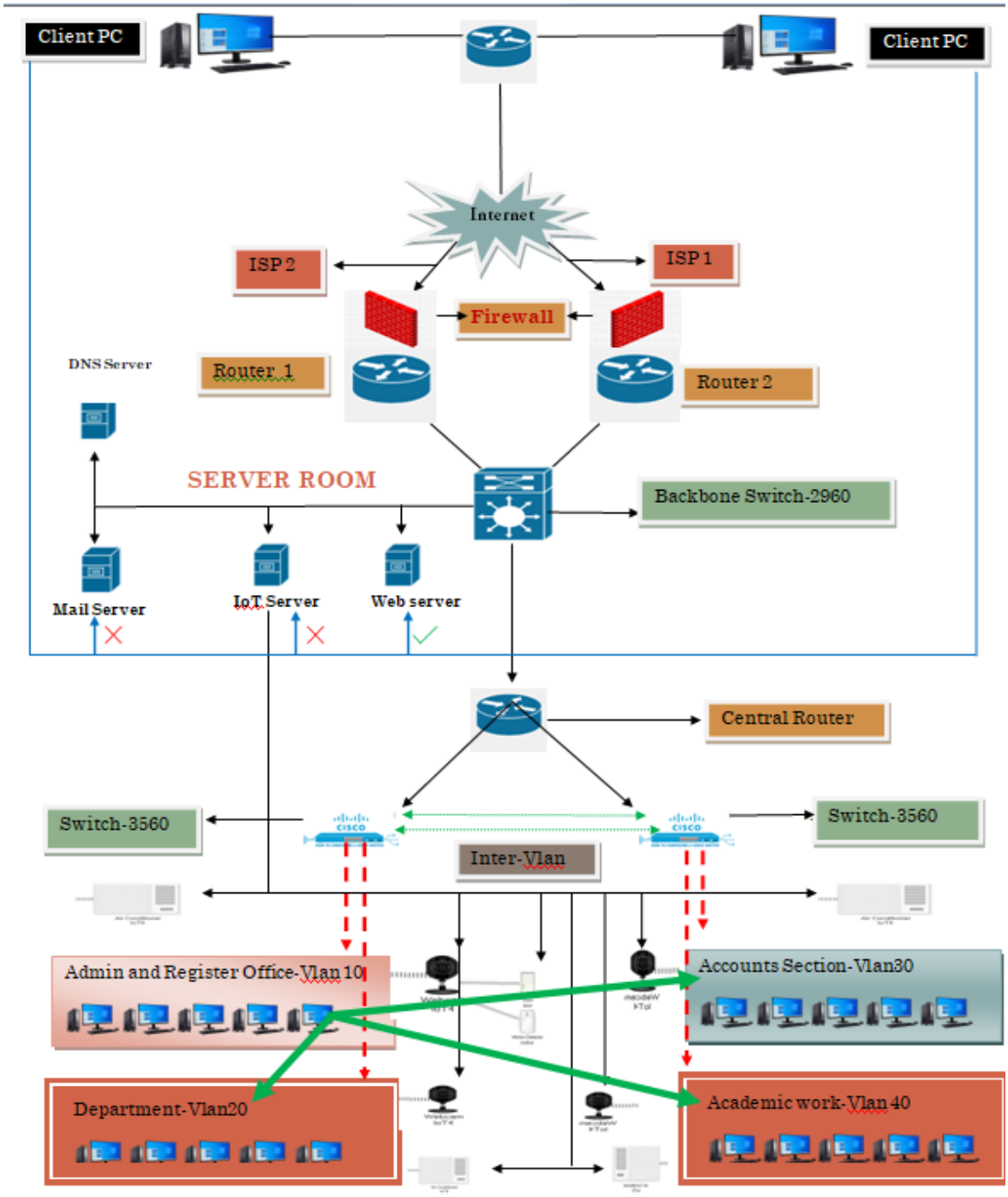


Figure 5.2: Proposal Diagram

5.3 RISK RATING CALCULATION BASED ON ARCHITECTURE

TABLE 5.3.1 RISK APPETITE AND RISK TOLERANCE

No.	Threat-sources	Risk Scenarios	Risk Appetite (Frequency per year)	Risk Tolerance
1.	Core Application	Software Unavailability	5	± 10%
		Unauthorized access	4	±20%
		Hardware Failure	2	±10%
2.	Information	Theft	1	± 15%
3.	Database	System failure	2	± 10%
		Server Failure/Overload	30	± 50%
		Malicious code injected by an insider or outsider	1	± 10%
4.	Human Error	Disclosure of Password	15	± 20%
5.	Cyber Attacks	Malware	40	± 20%
		Denial of Service (DoS)	20	± 10%
		Phishing	50	± 50%

TABLE 5.3.2: RISK FREQUENCY BASED ON RISK SCENARIOS ON ASSETS IF A VULNERABILITY IS PRESENT OR NOT

No.	Assets	Risk Scenarios	Risk Frequency Evaluation Details/Paragraph	Vulnerabilities	Risk Frequency rating
1.	Core Application	Software Unavailability	Possibility of software unavailability is very low due to regular basis testing, proper monitoring, and keeping the system up to date.	No	0.1
		Unauthorized access	The chance of theft by an insider or outsider is extremely minimal because all settings are isolated and well-monitored.	No	0.1
		Hardware Failure	Since all of the hardware resources is well maintained, hardware failure is regarded as being low.	No	0.5
2.	Information	Theft	Possibility of theft by insiders or outsiders is very low due to proper monitoring and all environments being separated.	No	0.1

3.	Database	Server Failure	Server down is categorized as medium-risk due to attackers making many queries to the server, which caused it to go down several times until MN online bookshop took action to fix it.	No	.5
		Database System failure	As a result of all settings being protected and carefully monitored, the chances of a database system failure is extremely low.	No	0.1
		Malicious code injected by insider or outsider	The chance of injecting malicious by an insider or outsider is extremely minimal because all settings are isolated and well monitored.	No	0.1
4.	Human Error	Disclosure of Password	Sometimes, workers will purposefully or accidentally disclose authentication information with an untrusted party.	Yes	0.5
5.	Cyber Attacks	Malware	A malware attack is a common cyberattack where malware executes	No	1

	unauthorized actions on the victim's system.		
Denial of Service (DoS)	Threats against SSH, which is frequently used by attackers to create new botnets for DDoS attacks, have constantly decreased.	No	.5
Phishing	It happens when an attacker poses as a reliable source in an email, IM, or text message in order to trick a victim into opening the message.	Yes	1

TABLE: 5.3.3 IMPACT SCALE

Note: Likelihood X Impact = level of risk

Overall Risk Rating Table:

No.	Assets	Risk Scenarios	Risk Frequency rating F	Consequences	g Overall Risk rating
1.	Core Application	Software Unavailability	.1	100	10
		Unauthorized access	.1	50	5
		Hardware Failure	.1	50	5
2.	Information	Theft	.1	50	5
3.	Database	Server Failure	.5	10	5

		Database System failure	.1	10	1
		Malicious code inject by insider or outsider	0.1	10	5
4.	Human Error	Disclosure of Password	0.5	50	25
5.	Cyber Attacks	Malware	.1	100	10
		Denial of Service (DoS)	.5	100	50
		Phishing	.5	50	25

Overall Risk Rating Calculation 146÷ 500 x 100 = 29.2 %

The result is **29.2%.** So, it can say that the result is fair. Our architecture is in a good position. But it can be more enriched.

CHAPTER 6

CONCLUSION

6.1 CONTRIBUTION

An overview of the cloud features offered by top service providers is presented in this research. We contrast the most well-known cloud services providers, such as Digital Ocean, Azure, and Amazon. The numerous differences between these providers in terms of various qualities are explained in this text. The main services offered by different cloud providers, such as storage, computing, and network services, are the subject of this research. Then, in order to learn more about networking, we construct an on-premises network design. Our next focus will be to investigate several cloud security issues and viable solutions. The many services that various cloud providers provide will be clear to people. Any organization's demands may be accommodated by our network architecture. You may use our study to learn about various problems with cloud security and potential solutions.

6.3 FUTURE WORK

In the future, we should do some security analysis for these project-related vulnerabilities and two routing protocols RIPv2 and OSPF which are used in this network project architecture. In our project, we have just evaluated a few key configurations to secure any organization's security. We switched the topic to network security issues that are frequently seen in today's cloud computing after reading a ton of papers and tutorials. Security and network architecture are virtually as essential as access to clean water, food, and shelter. The network will be scalable, performance and security will be improved, and the network will be simple to maintain if we stick to the hierarchical network design. Organizations can transition to using the cloud more safely if they are aware of the vulnerabilities that exist in cloud computing. Because cloud computing uses numerous technologies, it also carries over its security problems.

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A.S., Stoica, I., & Zaharia, M.A. (2009). Above the Clouds: A Berkeley View of Cloud Computing. Science, 53, 07-013.Bang, Sohyun, DongAhn Yoo, Soo-Jin Kim, Soyun Jhang, Seoae Cho, and Heebal Kim. "Establishment and evaluation of prediction model for multiple disease classification based on gut microbial data." *Scientific reports* 9, no. 1 (2019): 1-9.

[2] Das, Piyali & Mitra, Rupendra. (2016). A survey on cloud computing and networking in the next generation. 10.1201/b20012-56.Muhammad, L. J., Md Milon Islam, Sani Sharif Usman, and Safial Islam Ayon. "Predictive data mining models for novel coronavirus (COVID-19) infected patients' recovery." *SN Computer Science* 1, no. 4 (2020): 1-7.

[3] Zenuni, Xhemal & Ajdari, Jaumin & Ismaili, Florie & Raufi, Bujar. (2014). Cloud storage providers: A comparison review and evaluation. 883. 272-277. 10.1145/2659532.2659609. Shamrat, FM Javed Mehedi, Md Abu Raihan, AKM Sazzadur Rahman, Imran Mahmud, and Rozina Akter. "An analysis on breast disease prediction using machine learning approaches." *International Journal of Scientific & Technology Research* 9, no. 02 (2020): 2450-2455.

[4] Islam, Noman & Islam, Zeeshan. (2017). An economic perspective on major cloud computing providers Zeeshan Islam. ITB Journal of Information and Communication Technology Priya, M. Banu, P. Laura Juliet, and P. R. Tamilselvi. "Performance analysis of liver disease prediction using machine learning algorithms." *International Research Journal of Engineering and Technology (IRJET)* 5, no. 1 (2018): 206-211.

[5] https://aws.amazon.com/lambda/?nc2=h_ql_prod_fs_lbd International Journal on Cybernetics & Informatics (IJCI) Vol. 11, No.4, August 2022 178 Rahman, AKM Sazzadur, et al. "A comparative study on liver disease prediction using supervised machine learning algorithms." *International Journal of Scientific & Technology Research* 8.11 (2019): 419-422.

[6] Gracia-Tinedo, Raúl & Sánchez-Artigas, Marc & Moreno-Martínez, Adrián & Cotes Gonzalez, Cristian & López, Pedro. (2013). Actively Measuring Personal Cloud Storage. IEEE International Conference on Cloud Computing, CLOUD. To appear. 10.1109/CLOUD.2013.25.Candás, Juan Luis Carús, Víctor Peláez, Gloria López, Miguel Ángel Fernández, Eduardo Alvarez, and Gabriel Díaz. "An automatic data mining method to detect abnormal human behaviour using physical activity measurements." *Pervasive and Mobile Computing* 15 (2014): 228-241.

[7] S.Nagaprasad, & A.VinayaBabu, & K.Madhukar, & Verghese, D.Marlene & V.Mallaiah, &A.Sreelatha,. (2010). Reviewing some platforms in cloud computing. International Journal of

Engineering and Technology. 2 Chaurasia, Vikas, and Saurabh Pal. "Data mining approach to detect heart diseases." *International Journal of Advanced Computer Science and Information Technology (IJACSIT)* Vol 2 (2014): 56-6.

[8] Bandaru, Avinash. (2020). AMAZON WEB SERVICES Ibrahim, Ibrahim, and Adnan Abdulazeez. "The role of machine learning algorithms for diagnosing diseases." *Journal of Applied Science and Technology Trends* 2, no. 01 (2021): 10-19.

[9] https://www.digitalocean.com/?refcode=e8a7842ff717

[10] https://azure.microsoft.com/en-us/services/ddos-protection/#overview

[11] https://www.digitalocean.com/resources/cloud-performance-report

[12] https://www.upguard.com/blog/digitalocean-vs-aws

[13] Patrikalakis, Nicholas & Abrams, Stephen & Bellingham, James & Cho, Wonjoon & Mihanetzis, Kostantinos & Robinson, Allan & Schmidt, Henrik & Wariyapola, Pubudu. (2000). The Digital Ocean.. 45-54. 10.1109/CGI.2000.852319

[14] Kharade, S., & Kharade, K. (2017). A Comparative Study of Traditional Server and Azure Server. Journal of Advances in Science and Technology, 13(1), 329–331

[15] https://www.geeksforgeeks.org/aws-lambda-copy-object-among-s3-based-on-events/

[16] Chnar Mustafa Mohammed & Subhi R.M Zeebaree, 2021. "Sufficient Comparison Among Cloud Computing Services: IaaS, PaaS, and SaaS: A Review," International Journal of Science and Business, IJSAB International, vol. 5(2), pages 17-30

[17] https://www.cybersecurity-insiders.com/portfolio/2022-cloud-security-report-isc2/

[18] https://www.bunnyshell.com/blog/aws-google-cloud-azure-digitalocean-vps-performance

[19] Rakheja, Pankaj & kaur, Prabhjot & gupta, Anjali & Sharma, Aditi. (2012). Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network. International Journal of Computer Applications. 48. 6-11. 10.5120/7446-0401.

[20] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[21] I. S. Jacobs and C. P. Bean, “Fine particles, thin films, and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado, and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[22] K. Elissa, “Title of paper if known,” unpublished.

[23] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[24] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[25] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[26] Security Problems in Campus Network and Its Solutions, 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam1,2Department of Computer Science, NIT Agartala, India, 3National Informatics Centre, India

[27] Cisco White Paper, “Designing a Campus Network for High Availability,”http://www.cisco.com/application/pdf/e /us/guest/netsol/ns432/c 649/cdccont 0900aecd801a8a2d.pdf.

[28] “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL4 Manual/security-guide/ch-sgs-ov.html.

[29] CCNA Exploration 4.0 LAN Switching and Wireless, Cisco Networking Academy, Cisco Systems, Inc 2007

[30] CCNA Security 1.0, Implementing Network Security, Cisco Systems, Inc 2009.

[31] Tasnim, Rehnuma & Mim, Afrin & Mim, Salman Hasan & Jabiullah, Md. Ismail. (2022). A Comparative Study On Three Selective Cloud Providers.

APPENDIX

We had to solve various difficult problems in order to finish this assignment. Our biggest challenge was gathering resources and locating the right equipment for our architecture. For the purpose of constructing this network design, we looked at the structure of the network at our own institution. Finding the challenges and solutions related to cloud security is a concern for us since it is a new and difficult technology. Overcoming all of these problems was difficult for us because we are new to the field.

PLAGIARISM REPORT: